

Artificial intelligence Internet of Things: A new paradigm of distributed sensor networks

International Journal of Distributed
Sensor Networks
2022, Vol. 18(3)
© The Author(s) 2022
DOI: 10.1177/15501477211062835
journals.sagepub.com/home/dsn
 SAGE

Kah Phooi Seng^{1,*} , Li Minn Ang² and Ericmoore Ngharamike³

Abstract

The advances and convergence in sensor, information processing, and communication technologies have shaped the Internet of Things of today. The rapid increase of data and service requirements brings new challenges for Internet of Things. Emerging technologies and intelligent techniques can play a compelling role in prompting the development of intelligent architectures and services in Internet of Things to form the artificial intelligence Internet of Things. In this article, we give an introduction and review recent developments of artificial intelligence Internet of Things, the various artificial intelligence Internet of Things computational frameworks and highlight the challenges and opportunities for effective deployment of artificial intelligence Internet of Things technology to address complex problems for various applications. This article surveys the recent developments and discusses the convergence of artificial intelligence and Internet of Things from four aspects: (1) architectures, techniques, and hardware platforms for artificial intelligence Internet of Things; (2) sensors, devices, and energy approaches for artificial intelligence Internet of Things; (3) communication and networking for artificial intelligence Internet of Things; and (4) applications for artificial intelligence Internet of Things. The article also discusses the combination of smart sensors, edge computing, and software-defined networks as enabling technologies for the artificial intelligence Internet of Things.

Keywords

Internet of Things, artificial intelligence, deep learning, embedded analytics, distributed sensor networks

Date received: 18 April 2021; accepted: 26 October 2021

Handling Editor: Peio Lopez Iturri

Introduction

In recent years, we have witnessed the development and proliferation of billions of mobile and Internet of Things (IoT) devices. This rapid increase in IoT sensors, things, objects, and resources puts a demanding strain on existing IoT and distributed sensor network infrastructures. Emerging technologies and intelligent techniques can play a compelling role in addressing these new requirements. The result is a new interdisciplinary field and paradigm termed as the artificial intelligence Internet of Things (AIoT).¹ The AIoT is beginning to receive a significant amount of interest from the research communities and industries. The widespread acceptance and penetration of artificial

intelligence (AI) technology have resulted in more AIoT applications to emerge. These AIoT applications have the characteristics of being computationally

¹School of AI and Advanced Computing, Xian Jiaotong Liverpool University, Suzhou, China

²School of Engineering and Science, University of Sunshine Coast, Sunshine Coast, QLD, Australia

³Computer Science Department, Federal University, Oye-Ekiti, Nigeria

*This author is now affiliated to School of Computer Science, Queensland University of Technology, Brisbane, Australia

Corresponding author:

Kah Phooi Seng, School of AI and Advanced Computing, Xian Jiaotong Liverpool University, Suzhou, China.
Email: kahphooi.seng@qut.edu.au



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work

without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

demanding to execute machine-learning or deep learning algorithms and meet the real-time processing constraints. However, IoT devices are resource constrained (computation, storage, and communications), and this increases the design and deployment challenges to fulfill the quality-of-service (QoS) requirements for the AIIoT and its related applications.

In this article, we analyze the convergence of AI throughout the IIoT architecture to form the AIIoT with a focus on four aspects: (1) architectures, techniques, and hardware platforms for AIIoT; (2) sensors, devices, and energy approaches for AIIoT; (3) communication and networking for AIIoT; and (4) applications for AIIoT. The first aspect is related to the combination of AI and edge computing as key enabling technologies for the AIIoT. The other remaining three aspects seeks to apply and embed AI and machine-learning techniques toward the design and implementation of the various IIoT layers and structure. Figure 1 shows the overview concept of the AIIoT and the general layer structure for an AIIoT which consists of three layers: (1) sensing and device layer; (2) communication and network layer; and (3) application layer. The AIIoT aims to embed AI and machine-learning techniques into the sensing, communication, and application layers to achieve high-performing IIoT infrastructures.

In the sensing and device layer, the AIIoT paradigm can take advantage of recently developed edge computing architectures² and machine-learning approaches, such as active learning (AL),³ transfer learning (TL),⁴ and federated learning (FL).⁵ AL techniques can deal with the time-varying and unpredictable data over the IIoT network. TL utilizes pre-trained models developed at the edge servers to deliver accurate results. FL can provide the necessary privacy at the edge server for the processing information. In the communication and network layer, the AIIoT paradigm can take advantage of newly emerging communication technologies and networks, such as software-defined networking (SDN) and 5G/6G cellular communications.

A critical factor for the AIIoT paradigm is the security within the IIoT network. The heterogeneity of IIoT devices and massive scale of IIoT networks make it highly vulnerable to attack in several ways, as the likelihood of detecting an IIoT device that has not been properly secured or that has a weak security measure is very high. With the deployment of IIoT on 5G networks which provide high speed, low latency, and large bandwidth, it is easier, in the case of network security breach, for hackers to steal and download information, such as customer information and personal information, at a faster rate.⁶ Traditional security schemes are not efficient in solving security issues of IIoT network especially emerging security threats. AI tools have been integrated with IIoT (AIIoT) to offer more effective and efficient security solutions for IIoT networks.

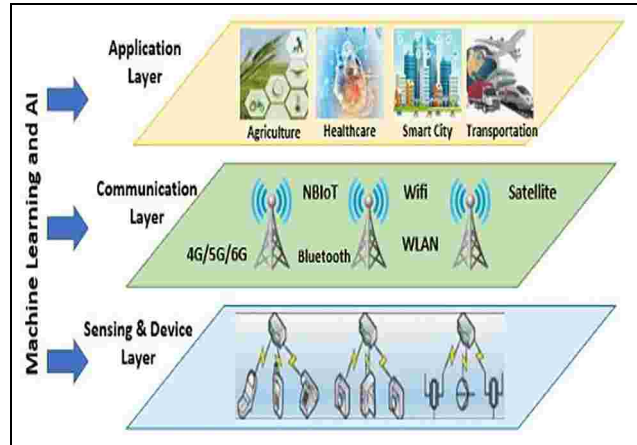


Figure 1. AIIoT architecture and layers.

In the application layer, the potential for the AIIoT is very high. It can be applied to make urban environments and vehicles smart. In smart homes, home appliances such as smart TVs, lights, thermostats, refrigerator, coffee makers, and so on are equipped with sensors and intelligence to learn a user's habits. The intelligence developed can be used to offer automated home support for daily task, minimize energy usage, and so on. Many organizations apply AIIoT to assist in managing energy, lighting, and access in the office building. Sensors placed in the office can detect the number of staff present per time and make necessary adjustment to lighting and temperature to enhance energy efficiency. Sensors also use face recognition to determine what personnel to grant access into certain areas of the office environment.⁷ The introduction of AIIoT and edge computing for intelligent driving allows the vehicle to offload tasks to the server closer to the vehicle side, creating a new paradigm for task offloading and resource allocation.

The survey work has used relevant papers which were searched from databases and other sources including IEEE Xplore, ScienceDirect, Scopus, and Google Scholar. We gave priority to papers which have been published more recently (from 2015 onwards). In performing the search, we used keywords, such as "Artificial Intelligence," "Internet of Things," and "Distributed Sensor Networks" using a combination of AND/OR operators to find the papers which were relevant toward the area of AIIoT. The studies also utilized two major contexts which were the problem context and the solution context to locate the various studies which focused on techniques, methods, and applications for AIIoT.

The remainder of the paper is organized into five sections. The sections are mostly structured to follow the different layers in the AIIoT as shown in Figure 1. Section "The convergence of architectures, techniques, and platforms for AIIoT" gives discussions on the convergence of architectures, techniques, and hardware

Table 1. Summary and discussions for AIoT—a new paradigm of distributed sensor networks.

Area	Sub-area	Focus of work
Convergence of architectures, techniques and platforms for AIoT	Edge, fog, and MEC architectures for AIoT	Resource-efficient AIoT edge computing (ThriftyEdge), ⁸ AIoT and UAV-mounted MEC, ⁹ cooperative edge computing in AIoT devices (ICE), ^{10,11} acceleration of CNNs on AIoT edge devices (AWARE-CNN), ¹² accelerating AIoT inference, ^{13–15} other works ^{16,17}
	Novel machine-learning and training techniques for AIoT	Deep learning for AIoT, ^{18,19} transfer learning for AIoT (FATL), ²⁰ federated learning for AIoT, ^{20–22} game theory for AIoT scheduling ²³
Convergence of sensors, devices, and energy approaches for AIoT	Scalable sensing, computation, and management for AIoT	AIoT sensing and deep reinforcement learning (DRL), ²⁴ AIoT and compressive sensing, ²⁵ AIoT and decentralized blockchain management ²⁶
	Wireless power transfer (WPT) and energy-harvesting approaches for AIoT	AIoT and energy-harvesting devices, ²⁷ AIoT and WPT on-device learning (WPEG) ²⁸
Convergence of communication and networking for AIoT	Frameworks for AI-enabled IoT networks	AIoT and contention-based random access, ²⁹ AIoT and over-the-air computation (AirComp), ³⁰ AIoT and WLAN, ³¹ AIoT and non-orthogonal multiple access (NOMA), ³² AIoT and multi-hop ad hoc network ³³
	AI-enabled IoT and cellular networks	AIoT and 5G cellular technologies, ³⁴ AIoT and 6G cellular technologies ³⁵
Convergence of applications for AIoT	Software-defined networking (SDN) for AIoT	SDN-AIoT and channel assignment, ³⁶ SDN-AIoT and QoE, ³⁷ SDN-AIoT intrusion detection system (NIDS), ^{38,39} SDN-AIoT and endogenous trusted network (ETN) ⁴⁰
	AIoT and MEC data streams	AIoT and MEC caching, ⁴¹ AIoT and DRL MEC resource sharing, ⁴² AIoT and MEC VR streaming ⁴³
	Energy, smart grids, and AIoT	AIoT and energy prediction, ^{44,45} AIoT and microgrid energy dispatch, ⁴⁶ AIoT and energy edge management, ⁴⁷ AIoT and blockchain architecture for natural gas ⁴⁸
	Industry, smart buildings, and AIoT	AIoT and smart building management, ⁴⁹ AIoT and thermal modeling, ⁵⁰ AIoT and fire evacuation ⁵¹
	Vehicles, smart transportation, and AIoT	AIoT and blockchain for intelligent driving edge systems, ⁵² AIoT and Safety-as-a Services infrastructure ⁵³
	Biomedical, smart health, and AIoT	AIoT and assisted health systems, ⁵⁴ AIoT and stress classification system ⁵⁵
	Environmental, smart agriculture, and AIoT	AIoT for disease detection (RiceTalk), ⁵⁶ AIoT for environmental monitoring, ⁵⁷ AIoT for farms (PigTalk) ⁵⁸
	Education, smart entertainment, and AIoT	AIoT and intelligent learning environments, ^{59–61} AIoT for smart entertainment ^{62,63}
	Robotics and computer vision in AIoT	AIoT drones for smart surveillance, ⁶⁴ AIoT robots for disaster management, ⁶⁵ AIoT virtual emotion detection system (CONTVERB), ⁶⁶ AIoT for intelligent parking management ⁶⁷
	Security in AIoT	AIoT security for smart cities, ⁶⁸ AIoT and intrusion detection, ^{69,70} AIoT and trust recommendation, ⁷¹ other works on security in AIoT ^{72–77}

platforms for AIoT. The discussions here include edge, fog, MEC, and cloud architectures for AIoT deployment. Section “The convergence of sensors, devices, and energy approaches for AIoT” gives discussions on the convergence of sensors, devices, and energy approaches for the AIoT. Section “The convergence of communication and networking for AIoT” gives discussions on the convergence of communication and

networking for the AIoT. Section “The convergence of applications for AIoT” gives discussions on the convergence of various applications for the AIoT. Section “Conclusion” concludes the article with some concluding comments and remarks. Table 1 shows a summary and discussions for the AIoT—a new paradigm of distributed sensor networks, to also serve as a concise summary for the article.

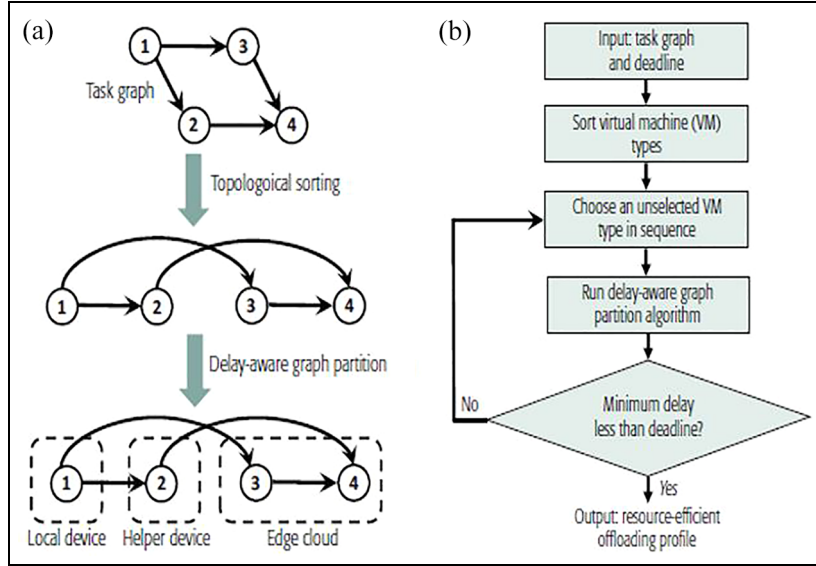


Figure 2. Task graph and flow chart for ThriftyEdge:⁸ (a) task graph for topological sorting and (b) flow chart for computation offloading.

The convergence of architectures, techniques, and platforms for AIoT

This section discusses the convergence of architectures, techniques, and platforms for AIoT from two aspects: (1) edge, fog, and mobile-edge computing (MEC) architectures for AIoT and (2) novel machine-learning and training techniques for AIoT. A summary of the representative studies discussed in this section can be found in Table 1.

Edge, fog, and MEC architectures for AIoT

Chen et al.⁸ proposed an approach for resource-efficient edge computing in AIoT termed as ThriftyEdge. In this work, they proposed a device-centric approach and a resource-efficient edge computing scheme to minimize the cloud resource utilization and be able to satisfy its QoS requirement. Their approach is based on a novel mechanism which consists of an efficient topology sorting-based task graph partition algorithm. An optimal virtual machine selection method is also proposed to minimize the IoT device edge resource occupancy and meet its QoS requirement. The virtual machine types are ranked and then selected based on the ranking to utilize the graph partition algorithm. Figure 2(a) shows the task graph for topological sorting and partitioning, and Figure 2(b) shows the flow chart of computation offloading profile.

Fragkos et al.⁹ proposed an AI-MEC framework by exploiting the computing capabilities of a unmanned aerial vehicle (UAV)-mounted MEC server for the IoT applications. In this work, the authors formulated

optimal offloading strategies to the UAV MEC servers based on a game-theoretic model. The pure Nash equilibrium (PNE) strategies were determined following the theory of submodular games. Their experimental results demonstrated the operational characteristics and performance of the models. Gong et al.¹⁰ proposed another approach to perform cooperative edge computing in AIoT devices termed as ICE (intelligent cooperative edge). In their approach, the AI computations are re-designed from the cloud to be distributed and operate on edge devices. Their distribution approach utilized lightweight pipelines for cloud compression and edge reconstruction. The authors' prototype and their evaluation showed that their approach could enable a useful combination of AI and edge computing.

Sanchez et al.¹² proposed an approach for the real-time acceleration of convolutional neural networks (CNNs) on edge devices termed as AWARE-CNN. Their approach utilized reconfigurability features of field-programmable gate array (FPGA) devices to construct application-specific AIoT architectures to guarantee the latency-aware execution for IoT data. Figure 3 shows the architecture of AWARE-CNN from a high-level view to its microarchitecture. Figure 3(a) shows an overview of AWARE-CNN which creates a translation from the high-level logical description of CNNs to an application-specific dataflow execution engine. Figure 3(b) shows the logical execution of cross-layer parallelism in AWARE-CNN. Figure 3(c) shows the microarchitecture where each layer is mapped to a pipeline stage containing a buffer-sized tile.

A current limitation of DL systems in IoT environments is the efficient assignment of compute tasks.

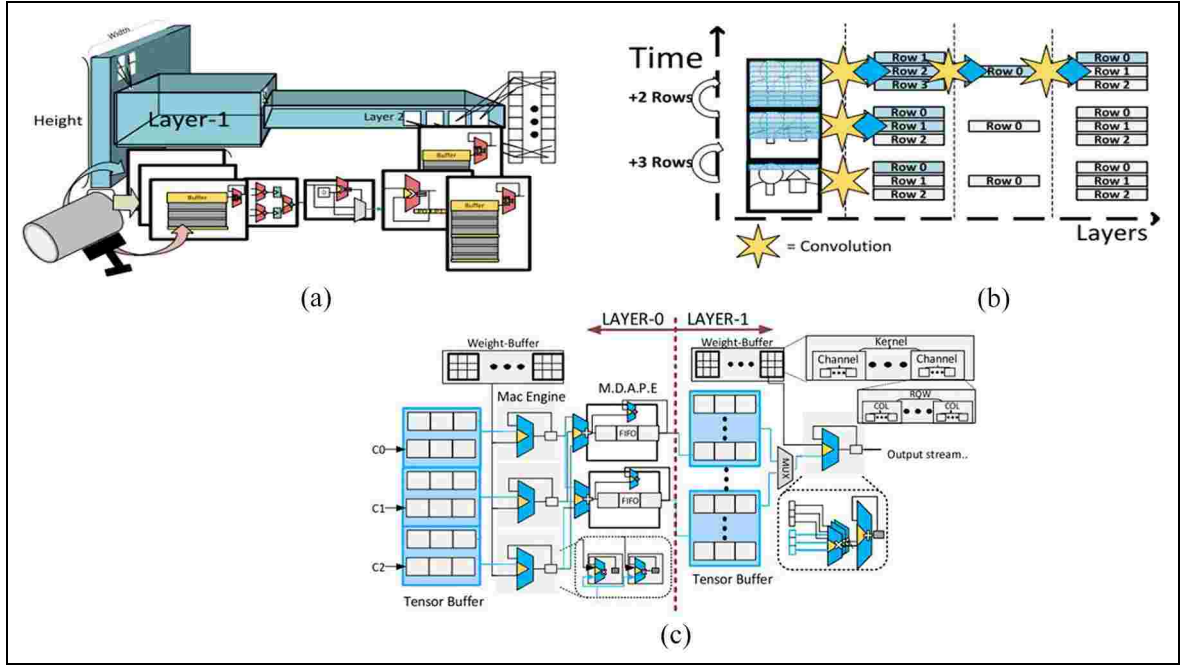


Figure 3. AWARE-CNN acceleration on edge devices:¹² (a) overview of AWARE-CNN, (b) cross-layer parallelism in AWARE-CNN, and (c) microarchitecture in AWARE-CNN.

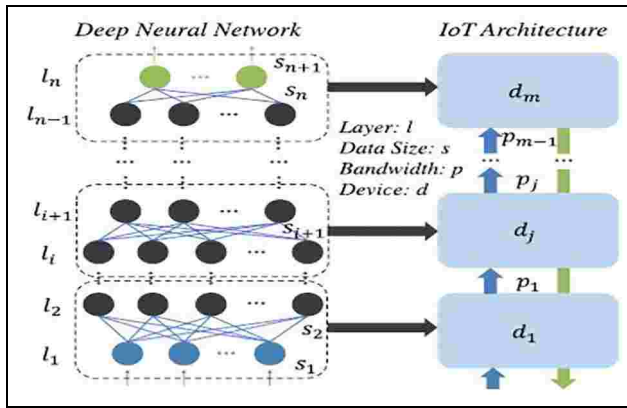


Figure 4. AAIoT inference computation on edge devices.¹³

Zhou et al.¹³ proposed an approach for allocating the inference computation among the IoT devices termed as AAIoT (accelerating artificial intelligence Internet of Things). Figure 4 shows the proposed AAIoT approach. In their approach, the first device collects the data, performs the computation for the first layer, and delivers the results to the next device. This process is carried on for the different devices, and the final result is communicated back to the first device. The operations of each layer depend on the results of the previous layer.

He et al.¹⁴ proposed an approach to reduce the end-to-end inference delay for DL implementation in multiple deep neural network (DNN) partitions. In this

work, the authors used a mixed-integer nonlinear programming approach and divided the problem into two subproblems: (1) a computing resource allocation (CRA) problem with fixed partitions and (2) a DNN partition deployment (DPD) problem. The authors then proposed to solve the CRA problem based on a Markov approximation algorithm and proposed a low-complexity DPD algorithm to solve the DPD problem to achieve a near-optimal solution. The computational complexity for cooperative multiaccess edge computing can increase significantly when there is large number of users which leads to delays in decision-making. Shi et al.¹¹ proposed an approach for deep reinforcement learning (DRL) for the task placement problem to enable servers to reduce the average service delay for cooperative multiaccess edge computing. Their approach utilized a mean-field game-guided DRL approach to address the task placement problem.

Liu et al.¹⁶ considered another challenge for edge computing in mobile wireless sensor networks (WSNs) with disjoint connectivity. In their work, the authors proposed a rendezvous selection strategy for data collection in disjoint WSNs with mobile edge nodes and optimize the path length and network connectivity. Their approach utilized the ant colony optimization (ACO) algorithm to give two advantages: (1) simplifying the path construction and computational cost and (2) reducing the search space and increasing the convergence speed. Yang et al.¹⁵ proposed an approach for energy-efficient execution of deep learning inferences

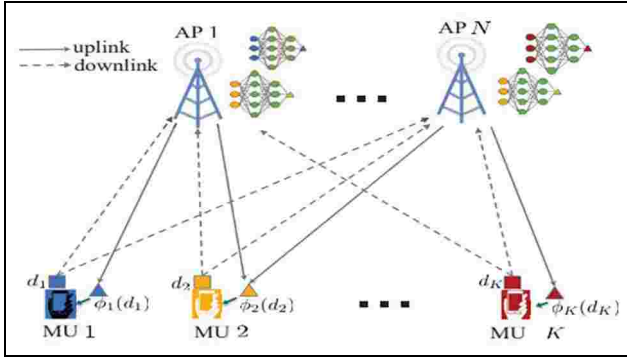


Figure 5. System model of edge inference for DNNs.¹⁵

tasks for deployment on mobile edge devices. Figure 5 shows the system model of edge inference for DNNs. In this work, the authors proposed to minimize the sum of computation and transmission power consumption under probabilistic QoS constraints. The authors developed a reweighted power minimization approach by iteratively solving a regularized reweighted l_1 .

Yang et al.¹⁷ proposed an Edge-Based IoT Platform for AI (EBI-PAI) by integrating SDN and serverless technology into QoE-aware edge computing to address the issues of resource scheduling and service definition in AIoT. Figure 6 shows the system architecture for the EBI-PAI which consists of three layers: (1) control layer; (2) mapping layer; and (3) edge layer. The authors investigated the QoE-aware server deployment problem to optimize the architecture performances

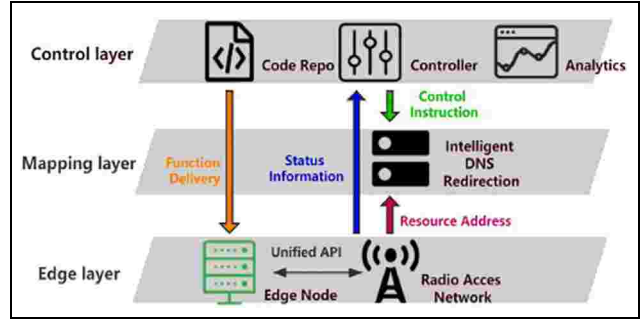


Figure 6. Edge-based AIoT (EBI-PAI) architecture.¹⁷

during incremental deployment. They formulated the deployment problem, proved its complexity, and designed heuristic algorithms with near-optimal performance (greedy minimum dominating set algorithms (GDSAs) and greedy cover for QoE-Aware (GCQA)). Their work was validated with a case study with real user demands.

Novel machine-learning and training techniques for AIoT

A desirable goal is to accelerate the training process of machine and deep learning approaches on the AIoT network. Liu et al.¹⁸ proposed a hierarchical training framework termed as HierTrain which has the capability to efficiently deploy DNN training tasks on the mobile-edge-cloud computing (MECC) model. Figure 7 shows the system overview of the HierTrain framework

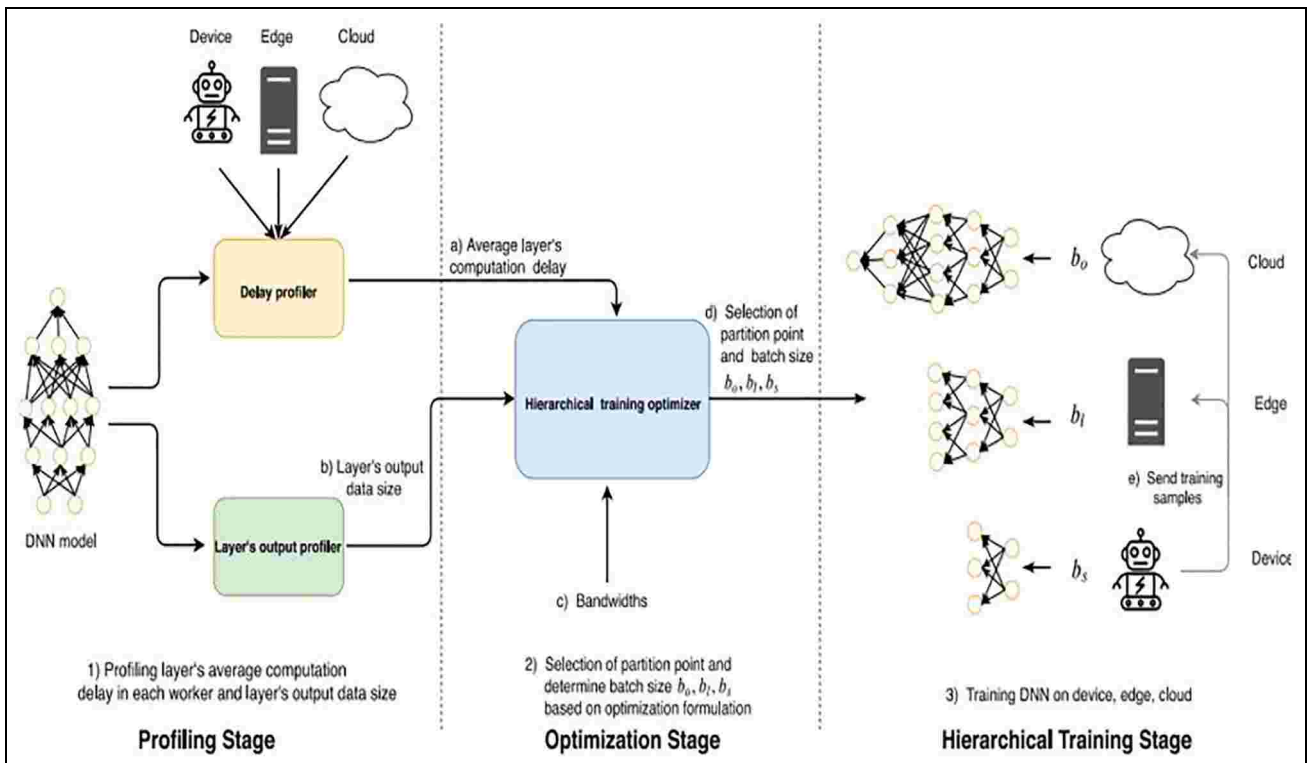


Figure 7. HierTrain AIoT training and deployment over MECC.¹⁸

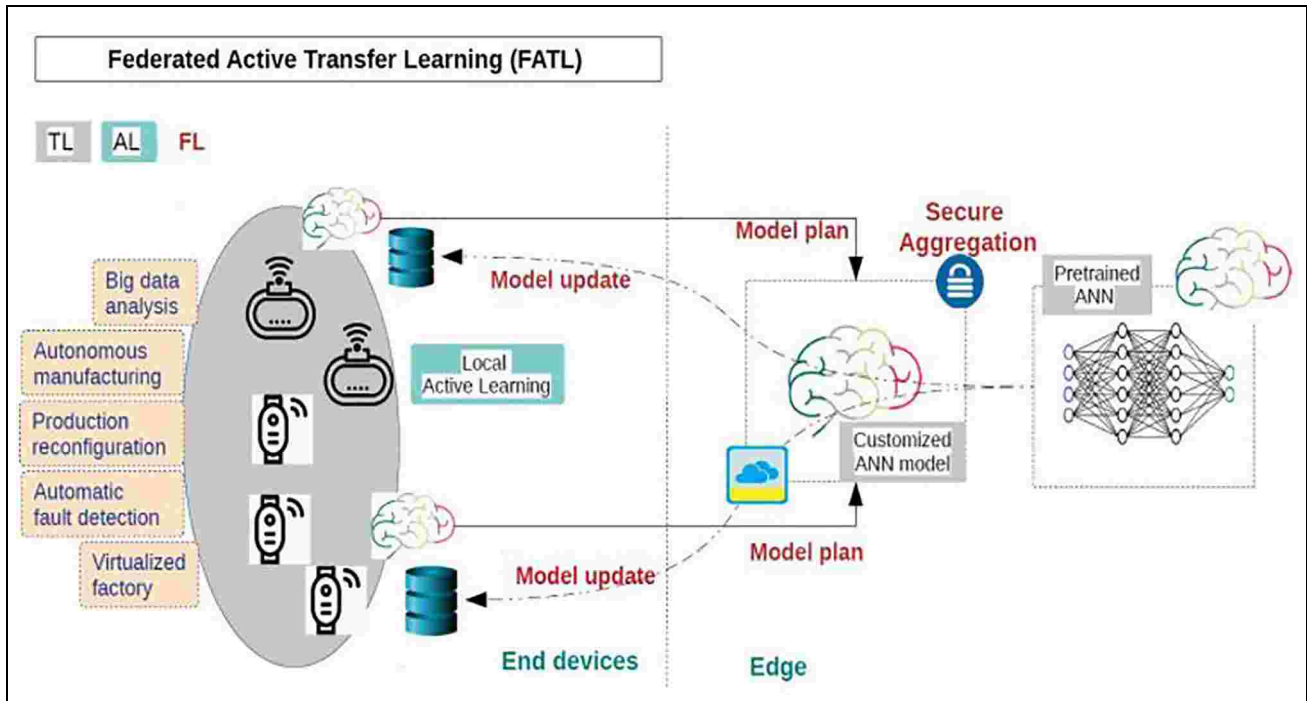


Figure 8. FATL architecture for IIoT applications.²⁰

which consists of three stages: (1) profiling stage—profiling the execution time for different layers on the device, edge and cloud; (2) optimization stage—selecting the optimal partition model and determining the training samples for the edge device, edge server, and cloud server; and (3) hierarchical training stage—sending the partitioned samples to the edge and cloud servers. Their work was implemented and deployed on a hardware prototype over the three levels. Their results showed that HierTrain could achieve an increase of 6.9 times performance speedup compared to the cloud-based approach.

Foukalas and Tziouvaras²⁰ proposed a combined FATL (federated active transfer learning) model for industrial IoT (IIoT) applications. Figure 8 shows the architecture of the proposed FATL for IIoT. Their proposed architecture had the objective to increase the learning speed and reduce the amount of labeled data during learning iterations for training on the IIoT devices. The authors utilized various machine-learning techniques to achieve these benefits. TL using a pre-trained artificial neural network (ANN) and FL were used for the edge IIoT architecture and scheduling for multiple devices, whereas AL was deployed on the IIoT end devices. Their experimental and simulation results showed that the proposed FATL architecture gave high accuracy and allowed scaling for a number of IIoT devices.

Another usage of FL was proposed by Wang et al.²¹ toward the problem for cooperative edge caching for

IIoT. In this work, the authors proposed an approach termed as FADE (Federated Deep Reinforcement Edge). The FADE approach enabled base stations to learn a shared predictive model by utilizing the first-round training parameters as the initial input for the training process. Their experimental results showed that their approach gave a reduction in performance loss and average delay, and improved the cache hit rate efficiency. Zhou et al.²² proposed an approach for coordinating edge and cloud architectures for the optimization and cost efficiency of FL. In this work, the authors utilized Lyapunov optimization theory and developed an optimization framework for load balancing, data scheduling, and accuracy tuning for the dynamically arriving training data samples. The authors showed that their approach had the advantages for reducing both the computation and communication cost.

Chiang et al.¹⁹ proposed an approach for co-task processing in multiaccess edge computing systems. The authors proposed an approach termed as DDL (deep dual learning) where the learner updates primal and dual variables based on randomly perturbed samples. Other than machine-learning approaches, algorithms from other fields, such as game theory, could also provide useful algorithms for IIoT architectures. IIoT fog nodes have the characteristics of having low resource capabilities. An important challenge is to match the IIoT services to fog node resources while guaranteeing the minimal delay for IIoT services and efficient resource

utilization. Arisdakessian et al.²³ proposed a multicriteria intelligent IoT-fog scheduling approach using game theory. Their approach proposed to design the preference list functions for the IoT and fog layers for ranking based on the criteria for latency and resource utilization.

The evolvement of edge, fog, and MEC architectures will play an important role in future research for the development of the AIoT to fully realize its potential and advantages for real-world deployments and applications. The following gives some aspects and main interests for researching and future trends on the convergence of architectures, techniques, and platforms for AIoT:

- A critical requirement would be the development of platforms and architectures that will support and coordinate the usage of distributed machine-learning algorithms and techniques throughout the AIoT ecosystem. Some illustrative examples are the work by Teerapittayanon et al.,⁷⁸ who proposed an approach for implementing distributed DNNs over cloud and edge devices and the work by Savaglio et al.⁷⁹ who proposed an approach for distributed data mining on edge devices;
- A second trend and focus would be the development of AIoT architectures, techniques, and platforms which are robust and secure to hostile, adversarial, and imposter attacks. An interesting research direction would be to utilize blockchain technologies to protect against cloned or counterfeit edge nodes or devices and demand proof of authenticity;⁸⁰
- A third focus would be the development of techniques and mechanisms for privacy-preserving data collection and mining within the AIoT. This is specifically important for AIoT containing heterogeneous nodes and devices.

The convergence of sensors, devices, and energy approaches for AIoT

The convergence of IoT and AI for the AIoT needs to be supported by different types of sensors, devices, and sensing approaches based on AI and other approaches. A review of AI-based sensors and deployment of AI-based sensors for the next-generation IoT applications can be found in Mukhopadhyay et al.'s study⁸¹ This section discusses the convergence of sensors, devices, and sensing approaches for the AIoT from two critical aspects: (1) scalable sensing, computation, and management for AIoT and (2) wireless power transfer (WPT) and energy-harvesting approaches for AIoT.

Scalable sensing, computation, and management for AIoT

The scalability for IoT sensing, computation, and management is an important issue to be addressed due to the geographically and rapidly increasing number of IoT devices. The advantages of the AIoT paradigm where the sensing and computation can be offloaded to the IoT devices is expected to offer users with higher quality of experience (QoE). However, the current computation offloading with QoE approaches using machine-learning and deep learning approaches may have issues of instability and slow convergence. Lu et al.²⁴ proposed an approach for offloading computation by utilizing DRL. The authors proposed an algorithm based on double-dueling deterministic policy gradients (D3PG) to address the instability and convergence issues for DRL while offering users better QoE. Their QoE approach has the capability to incorporate multiple factors and elements into the model: (1) computational and transmission latencies; (2) computational and transmission energy consumption; and (3) success rate for tasks.

Compressive sensing (CS) techniques gives a potential way to address the energy efficiency issue in AIoT sensor nodes. However, this approach is limited by the overhead of signal reconstruction constraints in the sensor node and the analysis in the remote server. Wang et al.²⁵ proposed a compressive sensing architecture utilizing deep learning for implantable neural decoding. The objective of their work was to improve the wireless transmission efficiency and reduce the overheads. The authors proposed a two-stage classification procedure: (1) coarse-grained screening module and (2) fine-grained analysis module. The screening module performed the front-end classification task and transmits the compressed data to a remote server for the fine-grained analysis.

Xu et al.²⁶ proposed an approach utilizing a blockchain-enabled edge computing platform termed as Edgence for the management of decentralized IoT applications. Figure 9(a) shows the decentralized Edgence architecture which is deployed on edge clouds of MEC. The Edgence platform consists of several master nodes. A master node contains a full node of the blockchain and a collateral. In this work, the authors proposed using a three-stage validation process: (1) script validation; (2) smart contract validation; and (3) master node validation. Figure 9(b) shows the decentralized AI training under the management of Edgence which used feed-propagation and back propagation for updating the AI models. The initial layers are trained using the data sets of mobile users at the edge clouds, whereas the latter layers are trained at the remote cloud center.

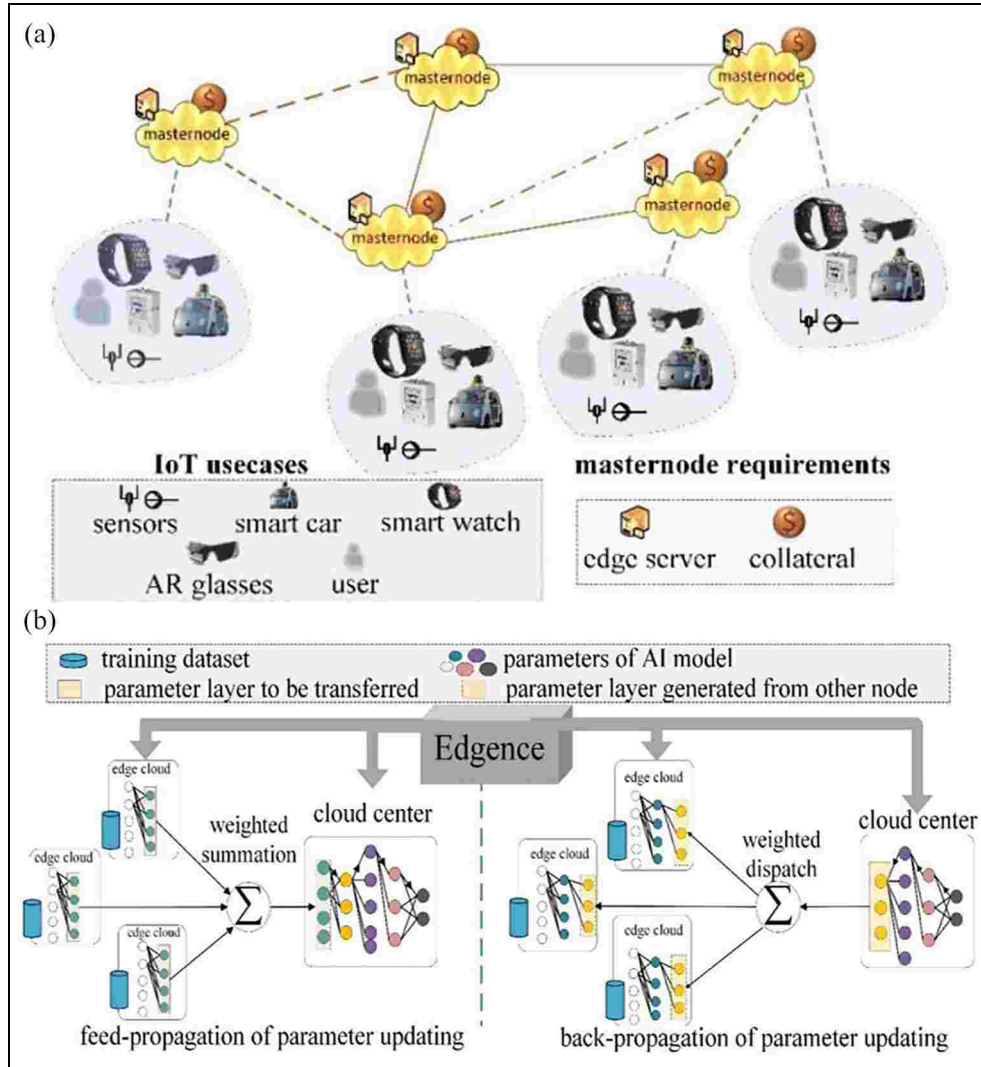


Figure 9. Decentralized Edgedge AI architecture and training:²⁶ (a) decentralized Edgedge platform architecture and (b) decentralized Edgedge AI models training.

WPT and energy-harvesting approaches for AIoT

There are several challenges which remain to be addressed to enable the practical deployments of WPT technologies in AIoT, such as ensuring security requirements to overcome selfish and untrusted devices and providing monetization incentives for charging services. Zhang et al.²⁷ proposed an approach for offloading time-varying computation task loads and requirements for deployment in MEC and energy-harvesting IoT devices. The authors approach utilized hybrid-DRL techniques consisting of: (1) hybrid decision-based actor-critic learning (Hybrid-AC)—an improved actor-critic architecture where the actor outputs continuous actions corresponding to every server, and the critic evaluates the continuous actions and outputs the discrete action of server selection and (2) multidevice

hybrid-AC (MD-Hybrid-AC)—constructs a centralized critic to output server selections which considers the continuous action policies of all devices.

Wu et al.²⁸ proposed a novel approach which integrates WPT and battery-constrained on-device learning techniques termed as WPEG (Wirelessly Powered Edge intelligence). Figure 10(a) shows the framework of the proposed WPEG nodes. Each node has the responsibility to manage the edge devices and WPT nodes within its coverage. In this work, the authors also proposed a permissioned blockchain approach to establish a secure point-to-point (P2P) energy trading for edge intelligence. Figure 10(b) shows the permissioned blockchain structure in the WPEG. The authors further proposed a two-stage Stackelberg game model to achieve the optimization for transmission power and incentive strategies.

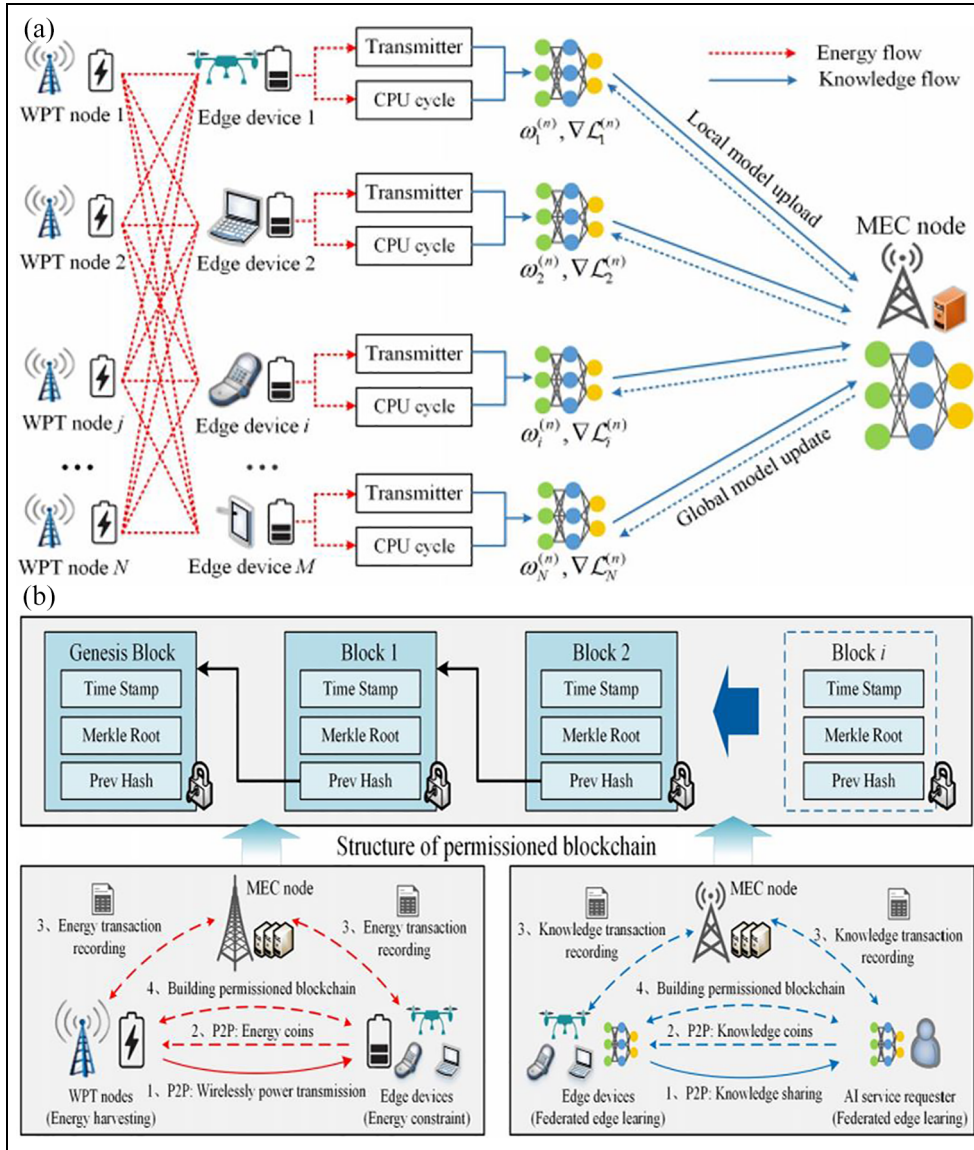


Figure 10. Framework and blockchain structure for WPEG:²⁸ (a) framework of proposed WPEG nodes and (b) permissioned blockchain structure in WPEG.

The following gives some aspects and main interests for researching and future trends on the convergence of sensors, devices, and energy approaches for AIoT:

- A potential solution for scalable sensing to cover large-scale areas and environments, such as smart cities would be to exploit mobile, opportunistic, and/or vehicular crowdsensing technologies and/or the internet of vehicles (IoV) for deployment of the AIoT sensors. Ang et al.⁸² discuss the applications, architecture, and challenges for IoV sensing and deployment in smart cities;

- The need for highly efficient energy management, harvesting, and WPT techniques remains another critical requirement for the continuing development of the AIoT. Ijamaru et al.⁸³ discuss the utilization of mobile collectors for opportunistic IoT sensing with WPT. Security aspects for WPT are going to become more significant and are opportunities for more research. Encryption techniques for WPT are required so that only the authorized receptors can acquire the transmitted energy and unauthorized receptors are prevented from illegally accessing the transmitted energy.

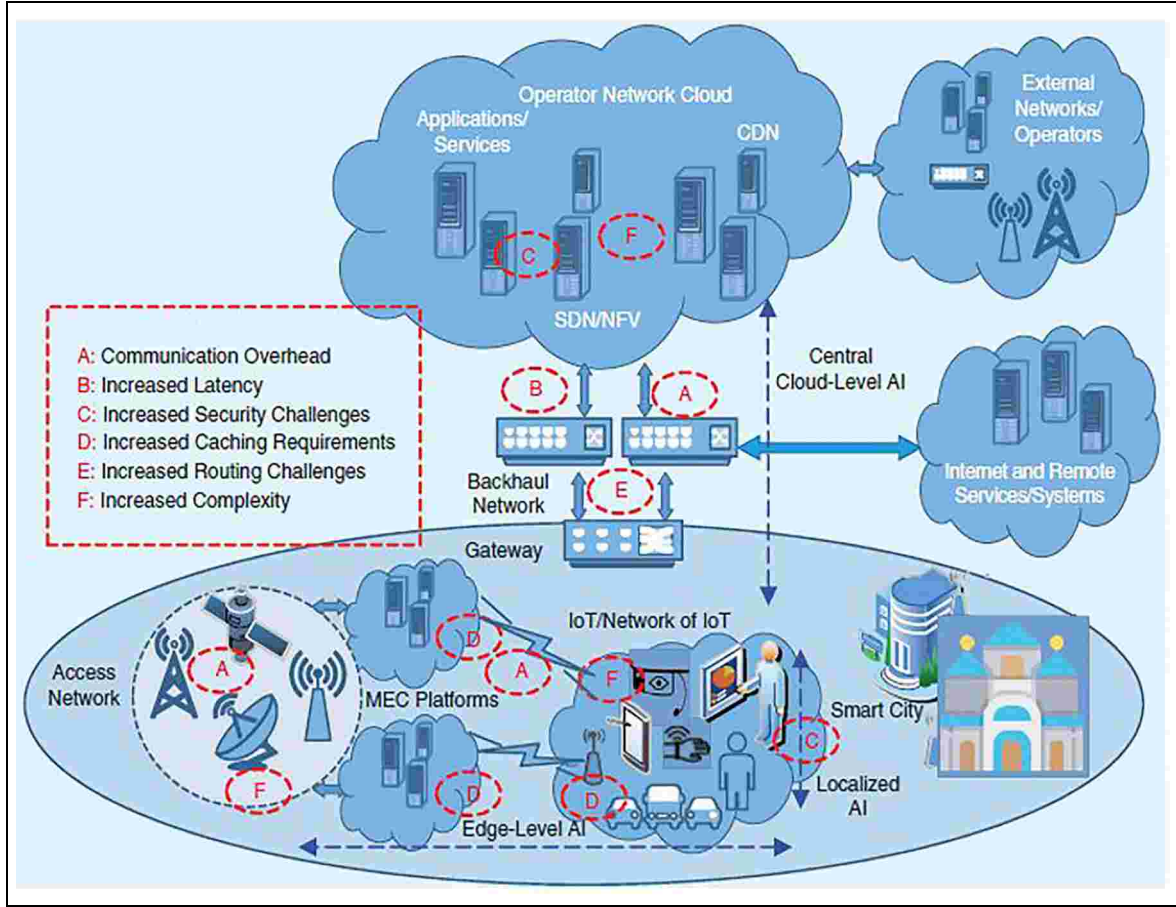


Figure 11. Network architecture showing AI in the IoT.⁸⁴

The convergence of communication and networking for AIoT

There are several advantages and challenges to converge AI in the network layer for routing, scheduling, and enhancing the QoS. Ijaz et al.⁸⁴ discussed some challenges of AI in wireless networks for IoT (as shown in Figure 11). Their article focused on the communication aspects for IoT and proposed a generic network architecture showing a few key areas of AI in the IoT: (1) software-defined network; (2) network function virtualization (NFV); (3) multiaccess edge computing; and (4) content delivery network (CDN). They discussed some challenges for the above areas. These included challenges for latency-critical IoT, challenges in routing and network traffic control, challenges in caching, and so on. This section discusses the convergence of AIoT in communication and networking from four aspects: (1) frameworks for AI-enabled IoT networks; (2) AI-enabled IoT and cellular networks; (3) SDN for AIoT; and (4) AIoT and MEC computing.

Frameworks for AI-enabled IoT networks

Song et al.²⁹ proposed an approach for centralized and distributed AI-enabled IoT networks. In this work, the authors discussed the challenges of contention-based random access and proposed some AI approaches in centralized IoT networks. The authors proposed to utilize DRL techniques for the online training process of the deep Q-network (DQN). Two neural networks (NNs) are used, namely an evaluated NN and a target NN for the DRL. For distributed IoT networks, the authors pointed out some key technical challenges of spectrum access and spectrum sensing. The work also proposed a DQN-based spectrum access strategy for intelligent spectrum access. Yang et al.³⁰ proposed an over-the-air computation approach termed as AirComp for a communication-efficient federated machine-learning architecture. Figure 12 shows the AirComp architecture and communication process of federated machine learning in intelligent IoT. The global and local models are iteratively updated through a number of communication rounds until the consensus of the

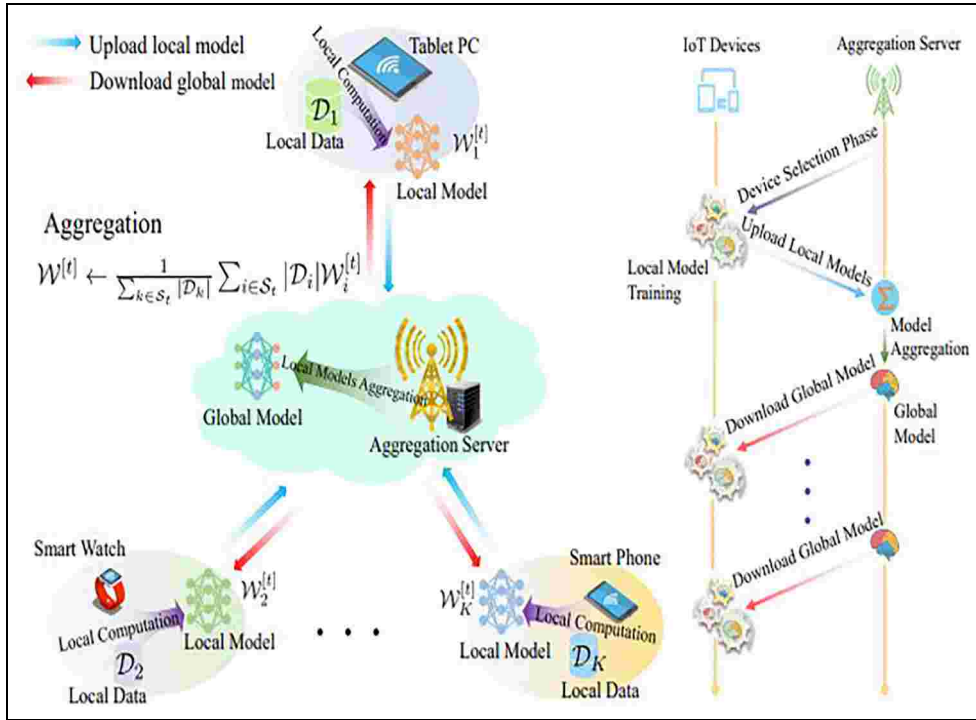


Figure 12. AirComp architecture and communication in AIoT.³⁰

global model is reached. As shown in the figure, three steps are performed for each learning round: (1) device selection; (2) local model upload; and (3) global model download. The AirComp approach achieved this by using the superposition property of a multiaccess channel to achieve fast local aggregation for federated machine learning.

Ramírez et al.³¹ proposed a WLAN and AIoT architecture for resource allocation and sharing among the devices in the IoT. The design of this architecture is for the IoT-WLAN. Figure 13 shows the AIoT-WLAN architecture. The proposal is based on an IoT network with centralized management architecture and AI control agent. Their proposed approach utilizes three control agents for the different environments. The AI control agents are located inside the smart things, in the centralized gateway administration, and in the cloud platform. The AI agents are responsible for learning the machine-to-machine (M2M) relations. Each smart thing connects to the network using the MQTT protocol.

Non-orthogonal multiple access (NOMA) schemes have a high potential for massive machine-type communication (mMTC) framework because it allows multiple users and devices to share resource blocks. Emir et al.³² proposed a deep learning-aided multi-user detection approach termed DeepMuD for uplink grant-free NOMA IoT networks to utilize the massive machine-type communication. Figure 14 shows the proposed DeepMuD model. In the proposed model, the authors

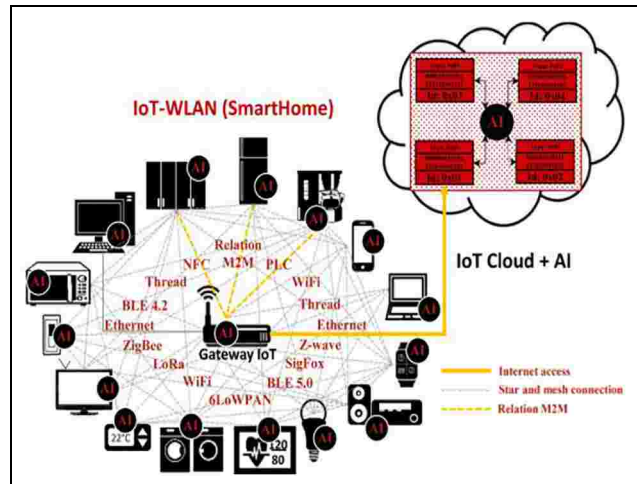


Figure 13. AIoT-WLAN architecture.³¹

used a model-driven deep learning technique called offline-trained LSTM-based network to perform the multi-user detection. Their work showed that the proposed approach could outperform conventional detectors (even with perfect channel state information (CSI)). Their experimental results showed that the same performance was obtained for increasing number of users with a 10-dB decrease in power consumption.

Kwon et al.³³ proposed a distributed approach to design a multi-hop ad hoc IoT network as shown in

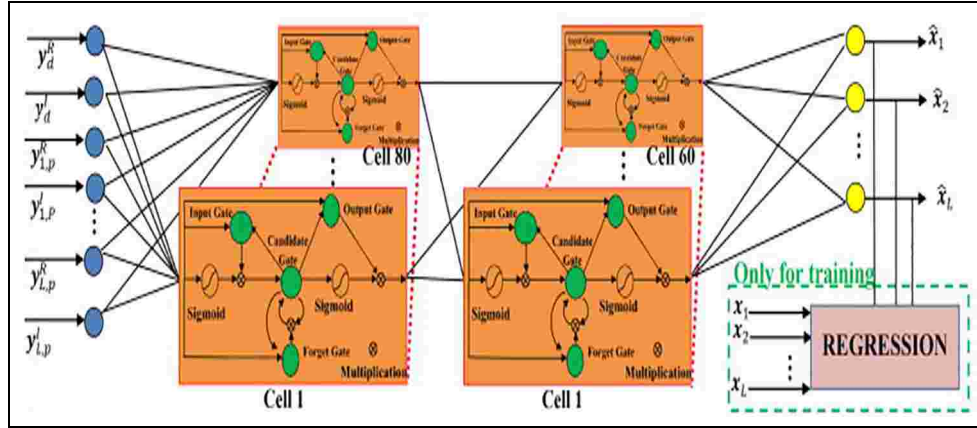


Figure 14. Non-orthogonal multiple access (NOMA) AIoT.³²

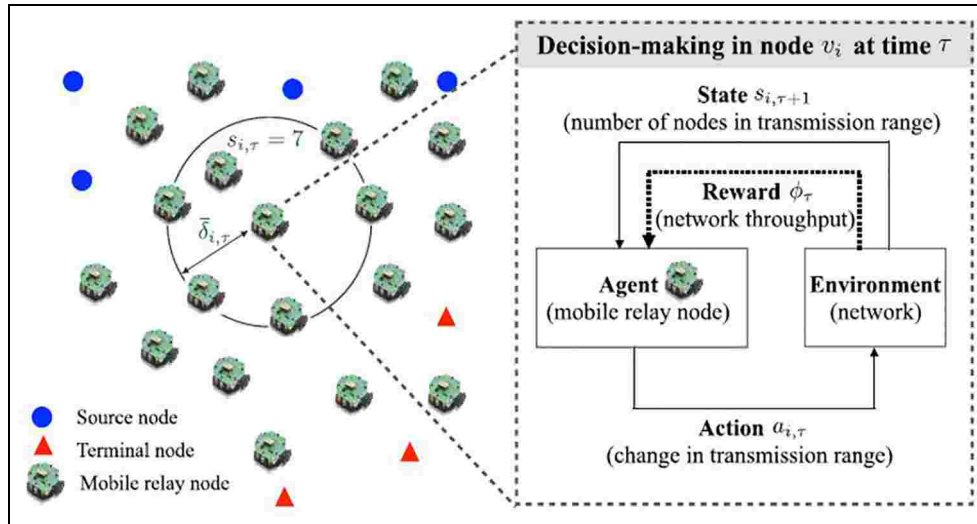


Figure 15. Distributed AIoT multi-hop ad hoc network.³³

Figure 15. In this work, the authors formulated a decision-making process based on an MDP framework which considers the trade-off between network throughput and individual transmission power consumption. A DRL algorithm using a double deep Q-network (DDQN) was deployed for decision-making at the relay nodes. Each node owns a DDQN to build its own policy e.g. transmission range, etc. The learning process for their system enables individual relay nodes to make decisions using a minimal amount of information.

AI-enabled IoT and cellular networks

The development of cellular network technologies such as 5G and 6G provides the potential to deploy complex sensors in the AIoT and to optimize the

communication channels. Wang et al.³⁴ proposed an architecture for 5G intelligent Internet of Things (5G I-IoT) which consist of three major components: (1) processing center; (2) object processor; and (3) sensing regions. Figure 16(a) shows the architecture of the 5G I-IoT, and Figure 16(b) shows the details of the processing center component. The processing center in the cloud includes the intelligent computing module and execution module to process data automatically with intelligent algorithms. DL algorithms are used to design the intelligent computing module.

Zhang et al.³⁵ discussed their model of the AIoT with 6G cellular technologies. Figure 17 shows their AIoT model with 6G technologies which includes three aspects: (1) mobile ultra-broadband—terabits per second wireless transmissions; (2) super IoT—supplemented by symbiotic radio and satellite-assisted IoT

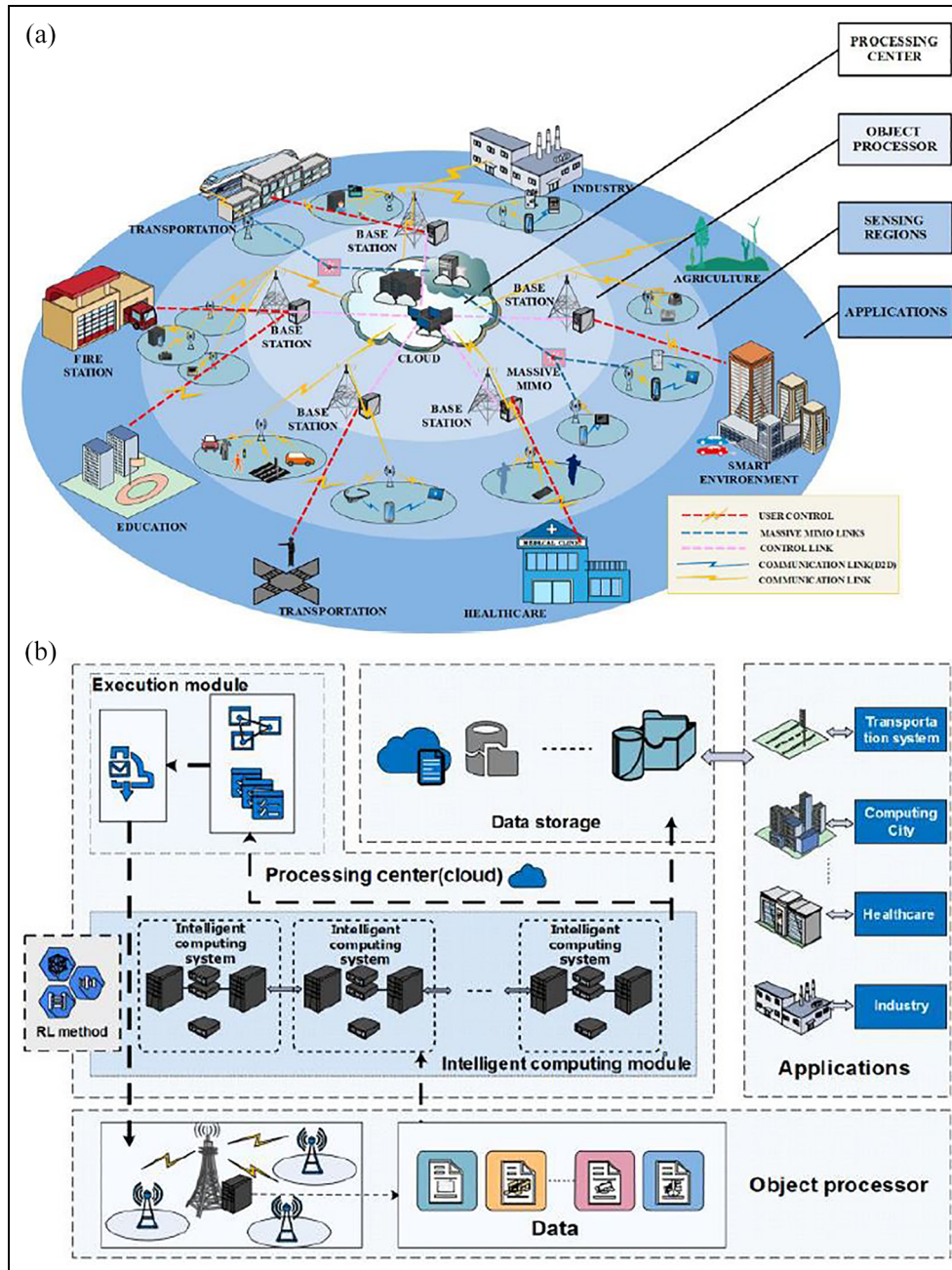


Figure 16. 5G I-IoT architecture and processing center:³⁴ (a) architecture overview and (b) processing center component.

communications to support a wider coverage and larger number of connected IoT devices; and (3) AI—advanced machine-learning focused on deep learning and reinforcement learning.

Software-defined networking for AIoT

In recent years, software-defined networks has emerged as a potential solution to provide cost-effective and flexible IoT services. The SDN-IoT can optimize network resources which may be underutilized to deliver the IoT

data. Tang et al.³⁶ proposed an approach for SDN-IoT which exploits partially overlapping channel assignment (POCA) in the SDN-IoT. In this work, the authors first investigated and showed that the conventional fixed POCA algorithms are not viable for the highly dynamic large-scale SDN-IoT. Figure 18 shows the wireless SDN-IoT with a heterogeneous structure and the problem with the fixed POCA. The authors proposed a DL-based intelligent POCA for the wireless SDN-IoT where the IoT data traffic dynamically changes. Their approach utilized two DL learning strategies for the

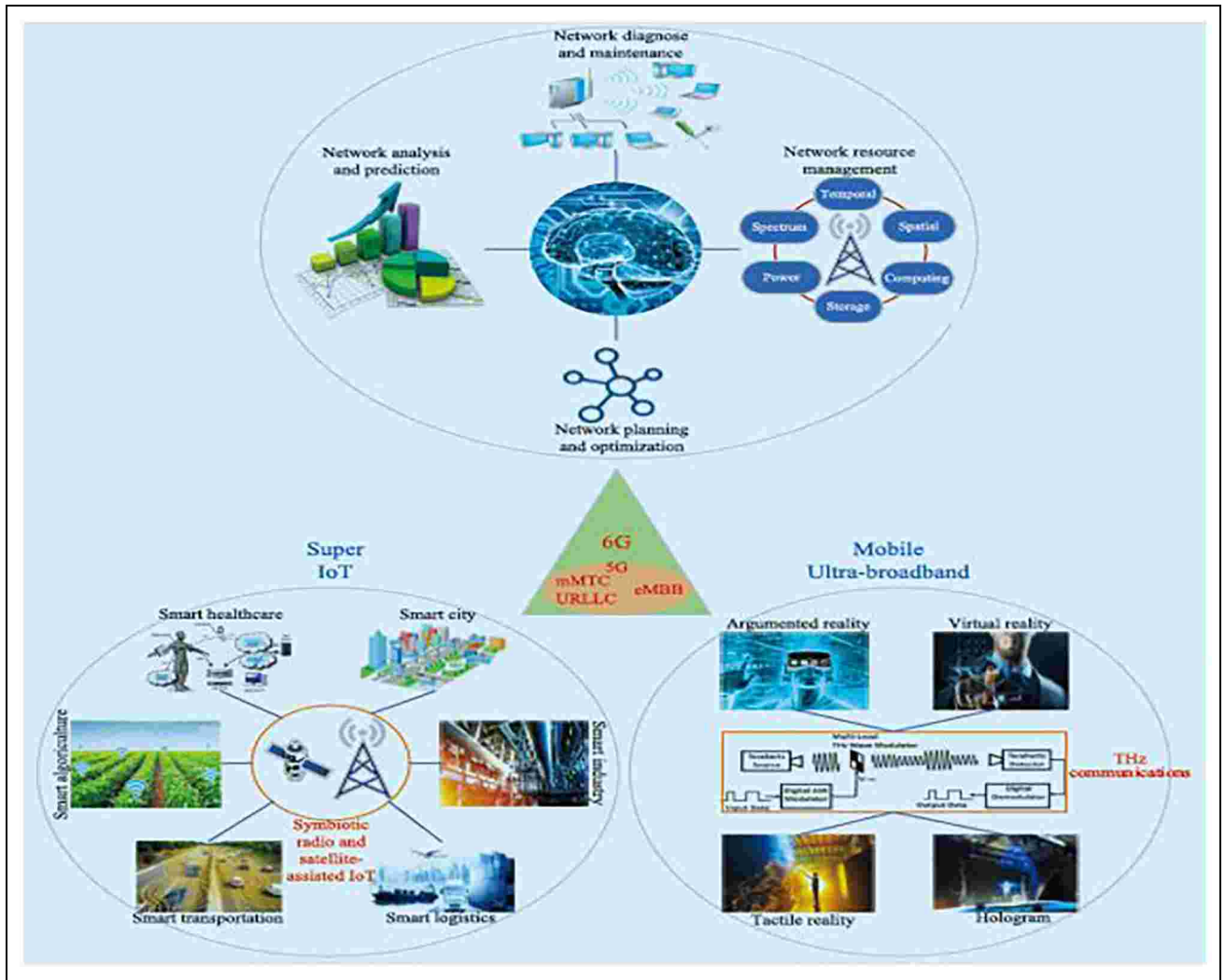


Figure 17. AIoT model with 6G cellular technologies.³⁵

prediction of IoT traffic load and to adaptively assign the POCs.

QoE for different services is an important factor for the AIoT. He et al.³⁷ proposed QoE models to evaluate the qualities of the IoT for both network and users. In this work, the authors focused on optimization of cache capacity among content-centric computing nodes and the transmission rates under a constrained total network cost. Figure 19 shows the cache resource allocation for content-centric IoT. The authors formulated the QoE as a cache resource allocation problem under the different transmission rate to acquire the best QoE. Their approach used DRL to adaptively improve the QoE.

Wu and Zhang³⁸ proposed a collaborative and intelligent network-based intrusion detection system (NIDS) architecture termed as SeArch for SDN-based cloud IoT networks. Figure 20(a) shows the proposed

SeArch NIDS architecture, and Figure 20(b) shows the NIDS node graph. The architecture consists of three layers: (1) edge-IDS; (2) f-IDS; and (3) cloud-IDS. These IDSs utilized DL and ML algorithms. For detection engines in the SeArch architecture, machine-learning algorithms were used (e.g. SVM for Edge-IDS, SOM for Fog-IDS, and Stacked autoencoder for Cloud-IDS).

Li et al.³⁹ proposed an intrusion detection approach by utilizing an AI SDN-IoT architecture. Figure 21 shows the proposed AI SDN-IoT architecture. The authors utilized different types of AI algorithms to perform the feature selection and flow classification tasks. These algorithms were (1) improved Bat algorithm with swarm division and differential mutation and (2) improved random forest. The improved Bat algorithm with swarm division and differential mutation was used to select the typical features. The algorithm splits the

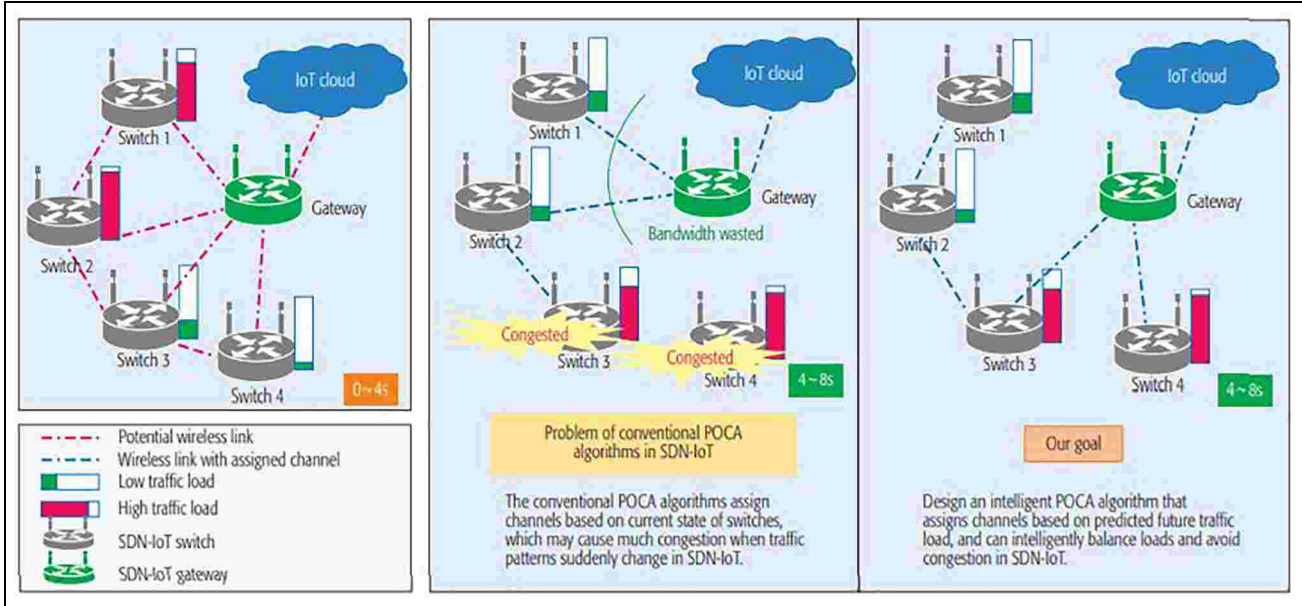


Figure 18. Wireless SDN-IoT.³⁶

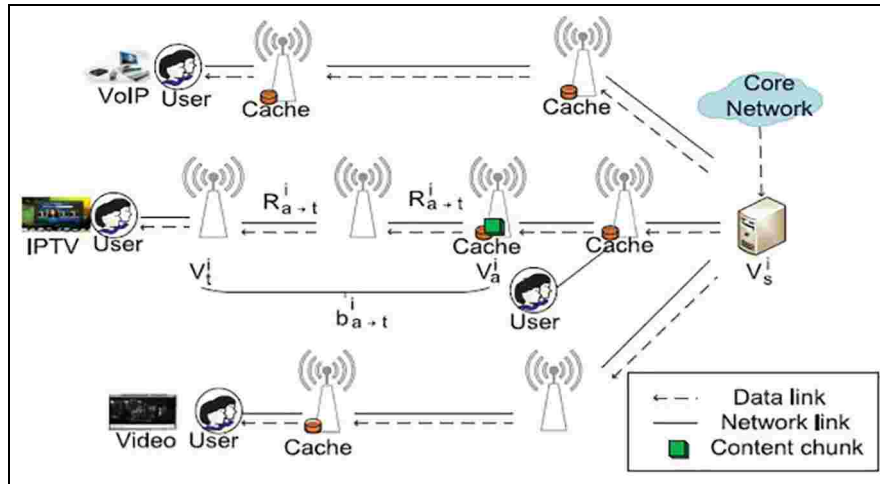


Figure 19. Cache resource allocation for content centric IoT.³⁷

swarm into several subgroups. Each subgroup is then used to learn among the different populations efficiently.

Guo et al.⁴⁰ proposed an approach for an endogenous trusted network (ETN) to support virtual network operations, resource allocation, and provide shared services. In this work, the authors utilized blockchain technology together with SDN and NFV to achieve the trusted sharing of network resources. Figure 22 shows an overview of the proposed ETN framework. The ETN consists of five layers: (1) terminal device layer; (2) network layer; (3) blockchain layer; (4) platform layer; and (5) application layer. Their blockchain

approach is used to achieve trust between resource requesters and resource providers in a distributed network.

AIoT and MEC data streams

MEC is a promising technology to improve QoE in AIoT networks. Jiang et al.⁴¹ proposed an approach termed as Crowd-MECS which used a crowdsourcing framework for mobile edge caching and sharing. Figure 23 shows the Crowd-MECS architecture. The two edge devices (in green) which denote a mobile edge device and a fixed edge device store the cache

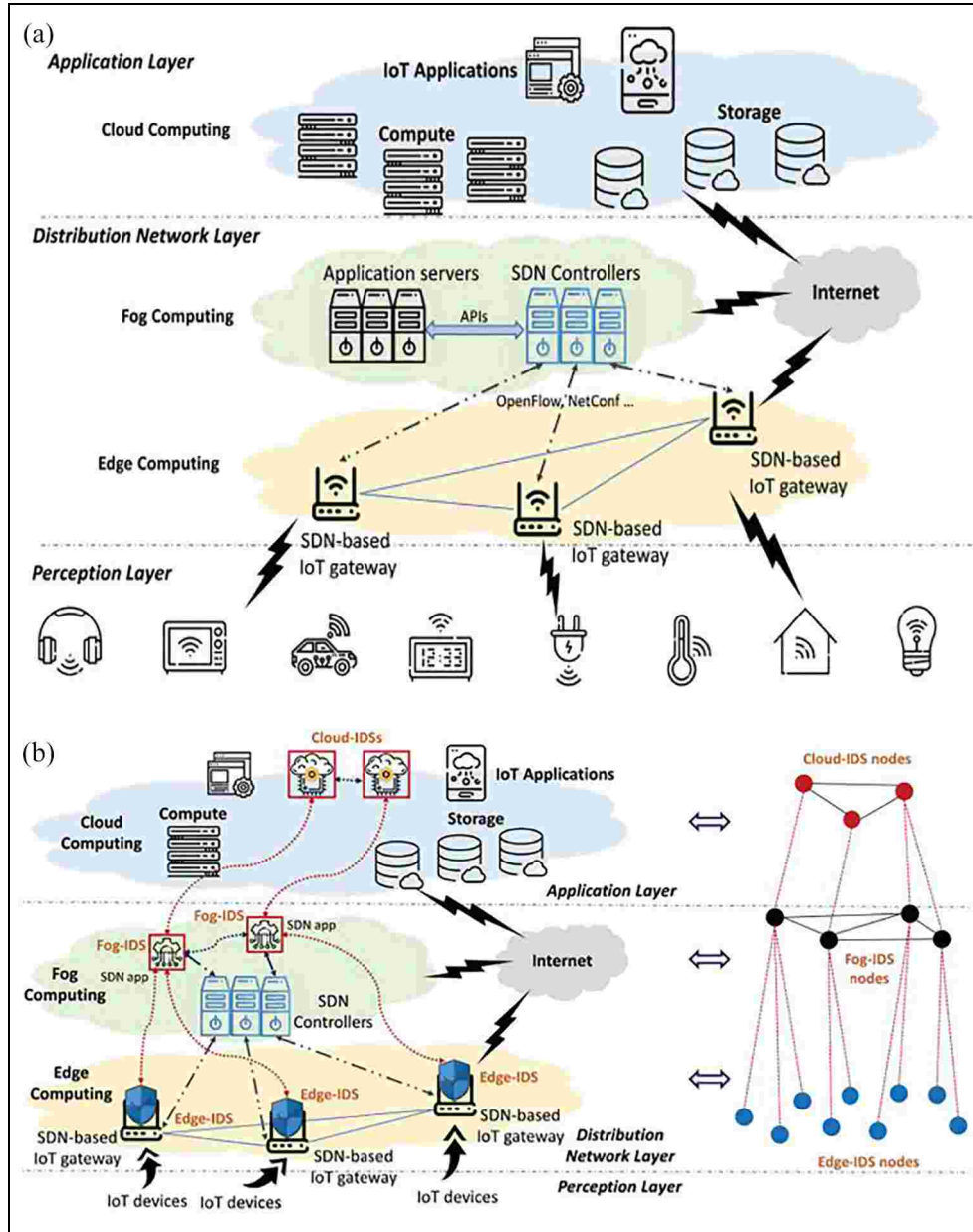


Figure 20. SeArch NIDS architecture and node graph:³⁸ (a) SeArch NIDS architecture and (b) NIDS node graph.

contents. These cached contents are shared with the red edge devices. Incentives are offered to the green edge devices for the content caching.

Other works for AIoT and MEC can be found in Jiang et al.⁴² and Du et al.'s studies.⁴³ Jiang et al.⁴² proposed a resource-scheduling approach based on DRL for large-scale MEC networks. In this work, the authors proposed a DRL approach to minimize the sum of weighted task latency for all IoT users by optimization of the task offloading decision, transmission power, and resource allocation in the large-scale MEC system. Du et al.⁴³ proposed a DRL approach for optimization of the energy consumption for immersive VR video streaming over terahertz wireless networks. In this work, the authors utilized DRL

to learn the optimal viewport rendering offloading and transmit power control policies and proposed an actor-critic (A3C)-based joint optimization algorithm.

The following gives some aspects and main interests for researching and future trends on the convergence of communication and networking for AIoT:

- The future will see the development of large-scale (e.g. citywide) IoT and AIoT networks. In these scenarios, interoperability is an important consideration in view of the rapid advances in new technologies such as 5G and 6G. The challenges for interconnection of multiple IoT networks which are owned by different organizations/

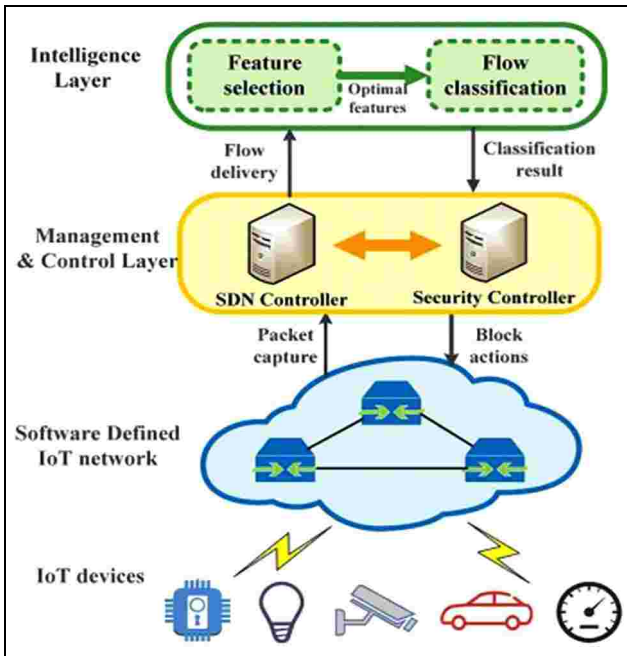


Figure 21. AI-based SD-IoT architecture.³⁹

stakeholders and/or developed using different communication networks/protocols and heterogeneous technologies remain an important issue to be satisfactorily resolved. SDN and NFV are interesting research directions and solutions to resolve the interoperability issues in IoT and AIoT networks;

- There is a growing importance to build trust into the communication networks for IoT. A growing trend in this regard is the replacement of centralized IoT trust architectures with decentralized architectures. An interesting research direction would be to utilize distributed ledger technologies (DLTs) for trust development and protection in IoT networks. Danzi et al.⁸⁵ give a discussion of the challenges for the integration of IoT networks and DLT.

The convergence of applications for AIoT

The convergence of AI and IoT enable the utilization of AI tools to introduce intelligence and decision-making capability into diverse IoT applications and systems.

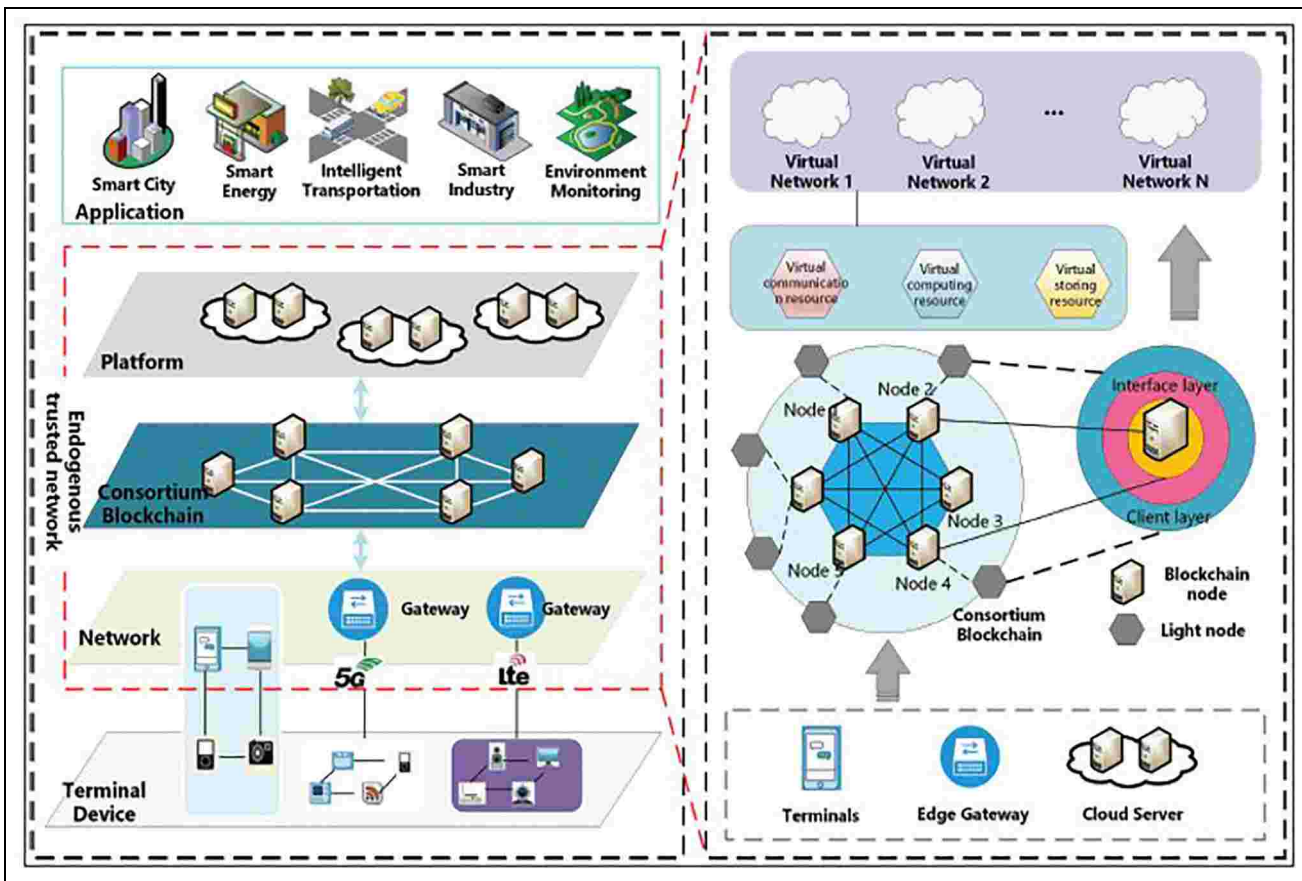


Figure 22. Endogenous trusted network (ETN) AIoT.⁴⁰

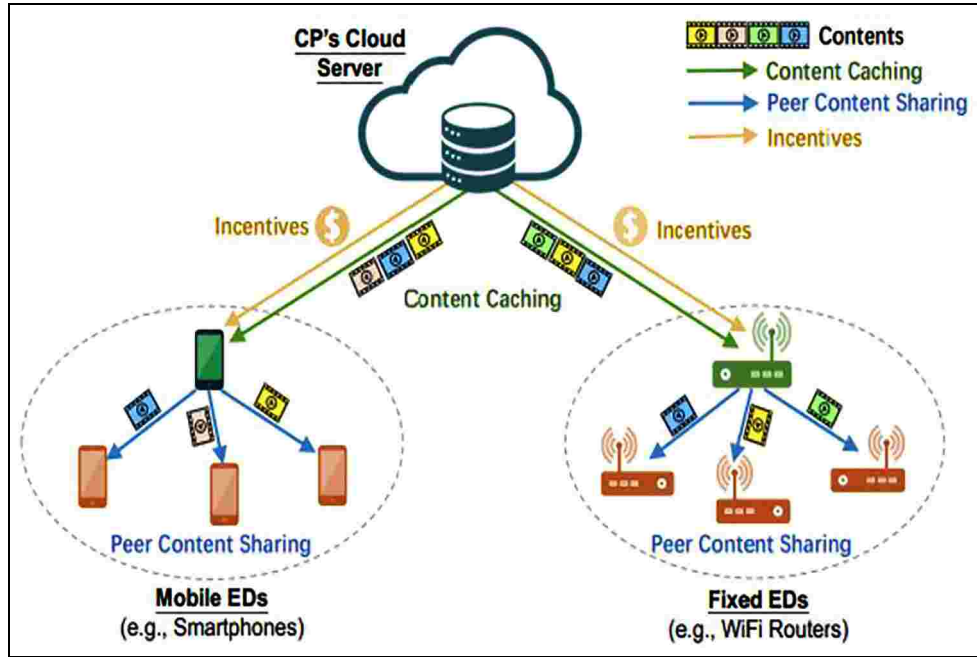


Figure 23. Crowd-MECS architecture.⁴¹

This convergence is helping to solve multiple IoT problems that have slowed its global adoption. The AIoT focuses on providing fast services, helping to unleash the potentials of utilize data in a better and faster way.⁸⁶ For example, in transportation applications, vehicles can be equipped with camera, GPS, radars, and sonar sensors to gather and analyze data to determine the condition of roads, pedestrian behavior, and so on and make decisions in response to such situations. Transportation companies have deployed AIoT to monitor and manage their fleets. Data gathered by the fleets is analyzed to manage fuel cost, track maintenance, and identify driver's unsafe behaviors. This section discusses the convergence of AIoT applications from eight aspects: (1) energy, smart grids, and AIoT; (2) industry, smart buildings, and AIoT; (3) vehicles, smart transportation, and AIoT; (4) education, smart entertainment, and AIoT; (5) biomedical, smart health, and AIoT; (6) environmental, smart agriculture, and AIoT; (7) robotics and computer vision in AIoT; and (8) security in AIoT. A summary of the representative studies which are discussed in this section can be found in Table 1.

Energy, smart grids, and AIoT

Researchers have deployed the AIoT in multiple ways to help energy producers optimize their equipment for better service delivery and to help users efficiently manage energy to minimize cost.⁸⁷ Puri et al.⁴⁴ developed an AIoT system that generates electrical energy from different sensors which can be used in industrial areas

and household appliances. The authors utilized different sensors, such as piezoelectric sensor, which generates energy from stress caused by human body weight, body heat to electric converter which generates energy from heat generated by movement of human body, and solar panel which generates energy from the sunlight. The authors built and validated the data collected from the sensors with two AI models (ANN and ANFIS) to perform the prediction of generated power output. The authors showed that their system could produce accurate results in predicting the power generated from renewable resources.

Lei et al.⁴⁶ proposed a DRL-based energy dispatch approach for IoT microgrids (MGs). The authors formulated and solved a finite-horizon partial observable Markov decision process (POMDP) model by learning from past data to identify uncertainties in future renewable power generation and electricity consumption, which is the focus of the authors. To address the instability challenges of DRL algorithms and the distinctive features of finite-horizon models, the authors designed two novel DRL algorithms. The first is a finite-horizon deep deterministic policy gradient (FH-DDPG) for finite-horizon MDP based on DDPG. The authors conducted experiments applying the idea of time-dependent actor to the proposed algorithm against the baseline DDPG. The results showed that the proposed FH-DDPG performed better than the baseline DDPG in providing stability to energy management problem. The second algorithm is a finite-horizon recurrent deterministic policy gradient (FH-RDPG) to solve the partial observable problem. This algorithm

was evaluated against RDPG. The result showed that the FH-RDPG algorithm performed better than baseline RDPG algorithm in a POMDP domain.

Liu et al.⁴⁷ proposed an IoT-based system for managing energy on edge computing devices using DRL. Their proposed architecture for the system consists of three major components: (1) energy device; (2) energy edge server; and (3) energy cloud server. The energy device is any entity in the network that requires and can supply energy. The energy edge server is a server deployed either at the network gateway or base station. The energy cloud server is connected to the energy management central controller with the responsibility of providing real-time analysis, maintaining record of devices connected to the network and proffering computational support to energy edge servers. The authors designed two DRL approaches of energy-scheduling scheme with two phases—offline DNN and online dynamic deep Q-learning phase. The DRL scheme is deployed at the energy edge server and energy cloud server. In the first approach, the task of scheduling energy is transferred from the devices to the edge server which utilizes the DRL approach to find the best scheduling solution for devices. In the second approach, the edge server, in order to minimize computation cost, relinquishes the task of training the DNN to the cloud server and then uses the deep Q-learning operation, making use of the estimated Q-value from the server. The results of their experiments showed that the DRL scheme outperformed the traditional cloud scheduling scheme.

Miao et al.⁴⁸ proposed a blockchain and AI-based architecture for the natural gas IIoT to address the supply chain failure of existing centralized supply architectures. The authors premised that numerous supply requests from centralized energy supply sites could be overwhelming and cause the indicators such pressure, temperature, and natural gas load to exceed safety limits. They stated that problems such as obsolete infrastructure, unreliable transaction, variable prices, inaccurate gas data, and unsecured user information are associated with centralized supply architectures. To address these problems, the authors proposed an architecture with three dimensions—infrastructure, data, and value. They implemented a blockchain solution to provide trusted transaction, distributed storage, authenticity, and reliability of stored data and data generated during energy generation and transmission. They further proposed an LSTM-based model to predict natural gas load and dispatch and a transaction model that utilizes natural gas value and supply–demand interaction. Their simulation experiments validated the good effectiveness of the models.

Han et al.⁴⁵ proposed a deep learning–based framework to predict future energy consumption in smart residential homes and industries. Their aim was to

solve the problem of load forecasting in energy management. Their proposed framework is composed of edge devices connected to a cloud server in an IoT network. The IoT network is connected to smart grids to effectively maintain energy demand and supply activities. To deal with several parameters contained in energy data set, the authors applied techniques to preprocess the data before initial training. Their experimental results showed that the approach was able to predict energy consumption with high accuracy.

Industry, smart buildings, and AIoT

AIoT has been adopted in industries and manufacturing to help foresee challenges and deal with them before they cause breakdown of machinery and operations. It enables M2M sensors and other industry smart devices to receive data, analyze it, and take decision to optimize operation, avoid unplanned costly downtime, plan logistics and supply chain, respond to cyber threats, and manage staff safety. Many researches have been done to better utilize AIoT in this domain.⁸⁸

An automatic real-time online method to evaluate the reliability and trustworthiness of cyber physical systems (CPS) in an IIoT network was proposed by Lv et al.⁴⁹ The evaluation framework and online rank algorithm was designed using machine learning to achieve the online assessment and analysis in real time. The result of the assessment could be utilized in a timely manner to take preventive measures to address any system faults or malicious attacks. To obtain a broad reliability model assessment strategy, the authors analyzed quintessential CPS control model that utilizes a spatio-temporal correlation model. Based on the assessment strategy, they developed a smart control strategy and a trusted smart predictive model. The proposed model from the simulation results was very effective in guiding the CPS defenders to select applicable defense resource input depending on the type of CPS threat and defense domain.

Zhang et al.⁵⁰ presented a learning framework that recognizes the thermal model of thermal zones automatically, to control the heating, ventilation, and air-conditioning (HVAC) systems, in a smart building for the comfort of the residents, under different environmental conditions, in order to lessen energy consumption. The proposed framework learns the thermal model from the temperature reading of the smart thermostat. The authors installed an IoT platform in a real-world building and used the data collected to validate the learning framework. Their experiment results showed that the learned model can be delivered in minutes if the learning process is done both in a cloud infrastructure and on edge device for a single thermal zone. The results also showed that the learned model

produces reliable evaluation of thermal comfort in intelligent control implementation.

Jiang⁵¹ proposed an intelligent dynamic evacuation path solving model in the case of fire outbreak in public buildings using AI technology. The author discussed that in order to bring people to safety in a fire outbreak situation, there should be a means of determining the shortest effective route to evacuate people depending on the verified fire situation, internal structure of the building, and fire product influences, such as temperature, smoke, and carbon monoxide concentration. The model was built based on appropriate fire emergency evacuation practices. The model was implemented using ant colony algorithm, and an AI-based mobile terminal system was developed for large public buildings to assist in guiding people to safe exit routes.

Vehicles, smart transportation, and AIoT

AI algorithms and techniques which have been integrated into IoT (AIoT) have found important applications in vehicles and transportation. An example of such application is in self-driving or autonomous vehicles. Future self-driving cars and vehicles will be embedded with several types of sensing instruments (e.g. cameras, lidar, and radar) and will generate huge amounts of data (e.g. 100 GB per second).⁸⁹ A significant challenge to be addressed is the real-time and secure processing of these sensor data to enable fast response to complex scenarios such as obstacle avoidance and velocity adaptation. The AIoT deployed at the network edge together with federated machine learning and secure trust models offer potential solutions. Xiao et al.⁵² proposed an approach based on using blockchain for intelligent driving edge systems. The approach utilized a double auction mechanism to optimize the satisfaction of users and service providers for edge computing. Their experimental results showed that the approach could give better performance for resource utilization.

Dass et al.⁵³ proposed a trust evaluation scheme called T-Safe to evaluate the trustworthiness of data generated from sensing nodes in an IoT-based intelligent transportation system. Safety-related information are provided to end users by safety-as-a-services infrastructure based on data generated by the sensor nodes by a method termed as decision virtualization. The authors premised that the accuracy and efficiency of such information depends on the trustworthiness, security, and privacy of the sensing nodes and the communication medium through which data are transmitted. The authors designed a trust evaluation model to address this problem. They utilized direct and indirect trust mechanism on every node in order to carry out trust measures update at regular time intervals. The

trust measures are then used to evaluate trust of every data item generated from the network. An integer linear programming (ILP) model is formulated by the authors to identify optimal data with reduced effect of unauthorized nodes for decision-making. Experimental results of the proposed scheme against greedy methods show that the proposed scheme outperformed existing methods.

Biomedical, smart health, and AIoT

The AIoT has been employed to manage and process large amounts of data generated in the internet of medical things (IoMT).⁹⁰ Yang et al.⁵⁴ proposed an intelligent architecture for processing visual data from IoT-assisted health systems. Their architecture consists of three modules: (1) end processing module; (2) edge control module; and (3) cloud management module. The intelligence at the end side was generated from the analysis of human, machine, and sensor characteristics. The intelligence in the edge and cloud sides was determined by an intelligent measurement model proposed by the authors. Their experimental results showed that the proposed method could outperform existing methods.

Mustafa et al.⁵⁵ proposed an AI-based IoT system for detecting and classifying stress. In their approach, a wearable device was equipped with various sensors (skin conductance, electrocardiograph (ECG), and skin temperature sensors) to measure the physiological characteristics. The physiological data collected were transferred through the user's mobile to the cloud. An AI algorithm was used to analyze the data to ascertain the level of stress. The user is alerted of the predicted stress level through a mobile phone. In a situation of a severe stress level, the user's physician would be alerted for necessary action. Their system achieved a 97.6% performance accuracy binary classification with regards to real-time sensor data.

Environmental, smart agriculture, and AIoT

Many researches utilizing AIoT technology have been focused toward smart agriculture, food processing, and optimization of environmental conditions to increase food production. Chen et al.⁵⁶ proposed an AIoT-based scheme that detects rice blast disease called RiceTalk. The scheme is based on soil cultivation IoT platform. Agriculture IoT sensors are used to gather data, which the AI mechanism trains and analyses automatically in real time. Existing studies made use of hyperspectral image or non-image data to determine plant diseases which needs human efforts to capture the photographs and data for analysis. The novel capability of RiceTalk is that the AI model is treated and managed as an IoT device which significantly minimizes the cost of

managing the platform to deliver real-time training and prediction. Their experimental results showed that RiceTalk could give a prediction accuracy of rice blast at 89.4%.

Nurminen and Malhi⁵⁷ designed an AIoT-based system to monitor and analyze the measurement of humidity, temperature, moisture, and luminosity to support clients for optimizing the conditions of the environment for houseplants. In this work, the authors proposed a solution to provide open interfaces so as to build an Open Houseplant Database for intelligent agents. Their approach also used an open messaging interface (OMI) node for data collection from sensor and a smart device for data analysis and prediction. The users were provided with an online user interfaces with standard data virtualization using dialogues and graph. Their experimental results showed the system showed great potential to support in a smart manner, the cultivation, and management of herbs and houseplants.

Chen et al.⁵⁸ proposed an AIoT-based platform to detect and mitigate piglet crushing in pig farms termed as PigTalk. The PigTalk approach was deployed in a farrowing house made up of different farrowing cages. Smart microphones were planted on top of the cage to detect piglet screams and rotating Internet (IP) cameras to monitor the cages. Floor vibration and water drop actuators were also used to alert a sow to stand up to detect when a piglet scream. In their approach, raw audio data (the piglet scream) are preprocessed by an audio clip transform method to detect piglet screaming. When a sow lies on a piglet, the data (piglet scream) are received by PigTalk through the microphone. PigTalk processed the data in real time and automatically activated the actuators (floor vibration, water drop, etc) or the heat light to force the sow to stand up. In contrast, existing systems would require a farm worker to locate the particular cage and push up the sow to avoid crushing. The PigTalk achieved its operation using two IoT devices: (1) DataBank and (2) ML-device. The DataBank device provided the improved generation of spectrograms of vocalizations received from farrowing cages, whereas the ML_device executed the CNN machine-learning model. Their experimental results showed that crushed piglets could be saved by PigTalk within 0.05 s with a success rate of 99%.

Education, smart entertainment, and AIoT

Several authors have proposed to use AIoT in the education field to make teaching and learning more effective and rewarding. Wangoo and Reddy⁵⁹ proposed an intelligent learning environment framework for IoT wearable devices to enhance interactive learning environments. The authors made use of GUI tools such as

Node Red, NEMA GUI Builder and Embedded Wizard for developing GUI for the IoT platform. Their framework is designed to provide students the opportunity to effectively interact during teaching and learning activities. IoT wearable devices used in educational application can utilize the framework for enhanced virtualization. Their experiments showed that the framework enabled IoT wearables to provide better learning experiences to users.

Liu et al.⁶⁰ applied AI analysis and IoT to determine student's concentration levels in individualized learning environments and to enhance learning quality using an automated IoT control model. In this work, the authors employed the abilities of image recognition and brain-wave signal analysis technologies, and environmental quality detection to capture data from students learning different courses under different environmental conditions to determine their concentration levels. The data collected were passed through an ANN computation. Afterwards, the results were applied to IoT control devices to adjust the learning conditions. Their experimental results showed that learners concentration improved as learning conditions improved.

Zhao et al.⁶¹ designed an AI collection of self-built learning resources. The aim of the work was to popularize the teaching and learning of AI in China. To reduce certain learning factors that discouraged teachers and students from participating in AI teaching activities, the authors developed an open hardware resource called STEAM Suite and a graphical drag-block programming language called December. The STEAM Suite provides several types of motors, plates, tires, beams, gears, shafts, batteries, and other basic components. This enables students to try and build different shapes of mechanical structures which is expected to motivate them to develop interest in AI as they cultivate strong ability in using the components. The authors verified that due to the practical oriented nature of the learning resources, the level of interest in teaching and learning of AI increased.

The application of AIoT in the entertainment sector has offered some revolution in many ways. The enormous data generated can be analyzed and used to improve user experiences and make targeted business decisions. Researchers are utilizing AIoT to develop smart systems to empower businesses in this sector for better services delivery.⁶² De Lima et al.⁶³ proposed an adaptive method to generate personalized interactive storytelling using users' preferences. The authors investigated the application of personality modeling and generated personalized account of experience with respect to users' personality using the Big Five factors. The proposed method was evaluated in an online interactive storytelling platform. Their experimental results

showed that the proposed approach could effectively identify users' preferences for story episodes with 91.9% average accuracy and enhanced the experience and satisfaction of users.

Robotics and computer vision in AIoT

The AIoT has enjoyed tremendous application in robotics and computer vision applications. Robots are empowered with sensors and AI algorithms to capture and learn from newer data to develop intelligence. This ability of the robot has motivated its use in manufacturing, health care, and so on to perform tasks meant for human experts faster and with lower cost.⁹¹ In smart cities, AIoT-enabled drones are used for several surveillance purposes such as real-time traffic monitoring. Traffic data are transmitted and analyzed and used to make decisions on the best way to reduce congestion by automatically adjusting the speed limits and timing of the traffic lights.⁶⁴

Lee and Chien⁶⁵ designed an AIoT architecture to coordinate surface, underwater, aerial ground robots to respond to disaster situations where it is impractical to send personnel. The robots are connected to an IoT network and used to collect data from a disaster site. The data are transmitted from the field workstations through the IoT network to the cloud where it is used to train a deep learning model. After training and verification, the model is transmitted back to the robots through the field workstations in order to continue on-site object classification and would enable them make response decision as they unceasingly confirm identification with the environment. Kim et al.⁶⁶ proposed an approach termed as CONTVERB (continuous virtual emotion detection system) for an IoT environment. IoT devices are equipped with wireless signal which they transmit to a person within a signal range and also receive the reflection of the signal. The IoT devices processes the reflected signal using a set of heart beat segmentation and respiration procedure to obtain no less than four different kinds of human emotion, such as sadness, joy, pleasure, and anger. Simulations and implementations of the proposed system showed its effectiveness.

Ke et al.⁶⁷ proposed an intelligent edge computing approach for the detection of parking space occupancy in a smart city. Edge AI and IoT are employed so as to break the computation load. The volume of data to be transmitted was designed to be low to handle bandwidth problem associated with real-time processing of video data. Tensorflow Lite was used to implement an SSD-Mobilenet detector on the IoT devices and was trained with the MIO-TCD data set. A tracking algorithm was deployed on the server end to track vehicles in parking facilities. The system was tested in a real-world environment for 3 months and the system

achieved 95% accuracy. Li et al.⁹² proposed an approach for defect detection in large-scale photovoltaic plants. Their approach utilized UAVs and edge computing to perform the defect detection. In this work, the authors developed an approach that combines deep and TL with data augmentation for deployment on resource-constraint edge devices. Techniques were also used in the network to reduce the parameters and the size of the model. Some other examples of AIoT for robotics and computer vision using various techniques can be found in the literature. Velasco-Montero et al.⁹³ proposed a methodology to predict the performance of CNNs on vision-based AIoT devices. Chiu et al.⁹⁴ proposed a distributed learning approach for AIoT video-based service platforms.

Security in AIoT

The security in the AIoT is a critical factor. Research in this field shows that with AIoT, IoT devices are enabled to learn from data and make swift decisions when an abnormal behavior is detected in the network in real-time.⁹⁵ Chakrabarty and Engels⁶⁸ proposed a framework for the IoT enabled smart city using AI to mitigate a range of present and future cyber threats. The massive adoption of IoT in smart cities provides a wide surface of attack for a heterogeneous, large and complex smart city system. The authors proposed framework focused on the security of the IoT communication protocols. An AI engine was strategically positioned at different stages (devices and big data center) within the framework to learn the normal network behavior and to monitor the security and health of the network. It is also able to acquire, store, and analyze big data generated by IoT devices. Their framework showed dominance in providing better effectiveness compared to existing smart city frameworks.

A self-adaptive and parallel processing intrusion detection system for an SDN network was proposed by Suresh and Madhavi.⁶⁹ The design of the AI-based IDS was done using the self-adaptive energy BAT algorithm. In the initial stage of their design, the software layer performs analysis of arriving traffic packets and to perform feature selection. The classification of the packets is performed by the system in the second stage, and if any attack is confirmed, the system takes appropriate control measures and makes decisions regarding network restrictions, such as resource allocation, routing, traffic management, and packet management. The authors performed training using the KDD CUP 99 data set, and testing was performed using data from a real-time IoT platform. The AI-based IDS result showed a reduction in energy overhead with regards to computation time to discover important features, and a fast response time to intrusion compared to swarm intelligence-based BAT algorithm which lacks parallel

processing and self-adaptive abilities. Eskandari et al.⁷⁰ proposed an intelligent anomaly-based IDS termed as Passban. The particular quality of the system is its direct deployment on low-cost IoT devices and its platform-independent ability. The aim of the authors was to ensure the protection of data very close to the IoT data sources, so that data generated from several IoT source can be analyzed to detect anomaly. The IDS training phase was carried out on a normal network flow. After the training, the learned model is placed into the gateway's internal memory where it is used to detect attacks from arriving network traffic. The system was evaluated against common cyber threats (SYN flood attacks, port scanning and brute force attacks) and demonstrated its efficiency.

Trust recommendation is another area of importance for IoT security. Xu et al.⁷¹ proposed an approach termed as TTSVD for trust recommendation in AI-enabled IoT systems which incorporates trust and rating information. In this work, the authors used a dual truster model (TrusterSVD) and trustee model (TrusteeSVD) based on a rating-only recommendation model. The influence of the two models were combined by the weighted average to produce a hybrid model called TT-SVD. Some other examples of AIoT security using various techniques can be found in the literature. Li et al.⁷² proposed an approach for resource optimization in blockchain IoT based on dueling DQN. Wang et al.⁷³ proposed another approach using blockchains to address the issues for decentralized multiparty learning in AIoT. Hu et al.⁷⁴ and Lim et al.⁷⁵ proposed using FL toward the problems for privacy and incentive mechanism design, respectively. Jia et al.⁷⁶ proposed an approach termed as FlowGuard to defend against IoT DDoS attacks. Libri et al.⁷⁷ proposed an approach termed as pAElla for real-time malware detection in edge IoT devices.

Conclusion

This paper has reviewed and discussed the convergence of the AIoT, where the advantages of intelligent machine-learning algorithms are integrated into resource-constrained IoT sensors and devices to enable large-scale and complex sensor deployments for IoT infrastructures. The paper has discussed the AIoT from several aspects and layers (sensors and devices, communication, and networking and AIoT applications), discussed the combination of the AIoT with different emerging technologies (e.g. edge, fog, and MEC computing, SDN, 5G/6G cellular networks, etc.), and given insights into the various challenges and issues which remain to be resolved to enable practical deployments of the AIoT into increasingly varied and complex environments.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

Kah Phooi Seng  <https://orcid.org/0000-0002-8071-9044>

Li Minn Ang  <https://orcid.org/0000-0002-2402-7529>

Ericmoore Ngharamike  <https://orcid.org/0000-0002-3572-9956>

References

- Shi F, Ning H, Huangfu W, et al. Recent progress on the convergence of the Internet of Things and artificial intelligence. *IEEE Netw* 2020; 34(5): 8–15.
- Yang L, Chen X, Perlaza SM, et al. Special issue on artificial-intelligence-powered edge computing for Internet of Things. *IEEE IoT J* 2020; 7(10): 9224–9226.
- Qian S, Sengupta S and Hansen LK. Active learning solution on distributed edge computing, 2019, <https://arxiv.org/abs/1906.10718>
- Shao L, Zhu F and Li X. Transfer learning for visual categorization: a survey. *IEEE T Neu Netw Learn Syst* 2015; 26(5): 1019–1034.
- Hao M, Li H, Lao X, et al. Efficient and privacy-enhanced federated learning for industrial artificial intelligence. *IEEE T Ind Inform* 2019; 16: 6532–6542.
- Tawalbeh LA, Muheidat F, Tawalbeh M, et al. IoT Privacy and security: challenges and solutions. *Appl Sci* 2020; 10(12): 4102.
- Sodhro AH, Gurtov A, Zahid N, et al. Towards convergence of AI and IoT for energy efficient communication in smart homes. *IEEE IoT J* 2020; 8: 9664–9671.
- Chen X, Shi Q, Yang L, et al. Thrifty edge: resource-efficient edge computing for intelligent IoT applications. *IEEE Netw* 2018; 32(1): 61–65.
- Fragkos G, Tsiropoulou EE and Papavassiliou S. Artificial intelligence enabled distributed edge computing for Internet of Things applications. In: *Proceedings of the 2020 16th international conference on distributed computing in sensor systems (DCOSS)*, Marina del Rey, CA, 25–27 May 2020, pp.450–457. New York: IEEE.
- Gong C, Lin F, Gong X, et al. Intelligent cooperative edge computing in Internet of Things. *IEEE IoT J* 2020; 7(10): 9372–9382.
- Shi D, Gao H, Wang L, et al. Mean field game guided deep reinforcement learning for task placement in cooperative multiaccess edge computing. *IEEE IoT J* 2020; 7(10): 9330–9340.
- Sanchez J, Sawant A, Neff C, et al. AWARE-CNN: automated workflow for application-aware real-time edge acceleration of CNNs. *IEEE IoT J* 2020; 7(10): 9318–9329.

13. Zhou J, Wang Y, Ota K, et al. AAIoT: accelerating artificial intelligence in IoT systems. *IEEE Wirel Commun Lett* 2019; 8(3): 825–828.
14. He W, Guo S, Guo S, et al. Joint DNN partition deployment and resource allocation for delay-sensitive deep learning inference in IoT. *IEEE IoT J* 2020; 7(10): 9241–9254.
15. Yang K, Shi Y, Yu W, et al. Energy-efficient processing and robust wireless cooperative transmission for edge inference. *IEEE IoT J* 2020; 7(10): 9456–9470.
16. Liu X, Qiu T, Dai B, et al. Swarm-intelligence-based rendezvous selection via edge computing for mobile sensor networks. *IEEE IoT J* 2020; 7(10): 9471–9480.
17. Yang S, Xu K, Cui L, et al. EBI-PAI: towards an efficient edge-based IoT platform for artificial intelligence. *IEEE IoT J* 2020; 8: 9580–9593.
18. Liu D, Chen X, Zhou Z, et al. HierTrain: fast hierarchical edge AI learning with hybrid parallelism in mobile-edge-cloud computing. *IEEE Open J Commun Soc* 2020; 1: 634–645.
19. Chiang Y-H, Chiang T-W, Zhang T, et al. Deep-dual-learning-based cotask processing in multiaccess edge computing systems. *IEEE IoT J* 2020; 7(10): 9383–9398.
20. Foukalas F and Tziouvaras A. Edge AI for industrial IoT applications. *IEEE Ind Electr Mag* 2021; 15: 28–36.
21. Wang X, Wang C, Li X, et al. Federated deep reinforcement learning for Internet of Things with decentralized cooperative edge caching. *IEEE IoT J* 2020; 7(10): 9441–9455.
22. Zhou Z, Yang S, Pu L, et al. CEFL: online admission control, data scheduling, and accuracy tuning for cost-efficient federated learning across edge nodes. *IEEE IoT J* 2020; 7(10): 9341–9356.
23. Arisdakessian S, Wahab OA, Mourad A, et al. FoG-Match: an intelligent multi-criteria IoT-Fog scheduling approach using game theory. *IEEE/ACM T Netw* 2020; 28(4): 1779–1789.
24. Lu H, He X, Du M, et al. Edge QoE: Computation offloading with deep reinforcement learning for Internet of Things. *IEEE IoT J* 2020; 7(10): 9255–9265.
25. Wang A, Song C, Xu X, et al. Selective and compressive sensing for energy-efficient implantable neural decoding. In: *Proceedings of the 2015 IEEE biomedical circuits and systems conference*, Atlanta, GA, 22–24 October 2015, pp. 1–4. New York: IEEE.
26. Xu J, Wang S, Zhou A, et al. Edgence: a blockchain-enabled edge-computing platform for intelligent iot-based dapps. *China Commun* 2020; 17(4): 78–87.
27. Zhang J, Du J, Shen Y, et al. Dynamic computation offloading with energy harvesting devices: a hybrid-decision-based deep reinforcement learning approach. *IEEE IoT J* 2020; 7(10): 9303–9317.
28. Wu AKB, Li J, Yang W, et al. Blockchain-based incentive energy-knowledge trading in IoT: joint power transfer and AI design. *IEEE IoT J*. Epub ahead of print 15 September 2020. DOI: 10.1109/JIOT.2020.3024246.
29. Song H, Bai J, Yi Y, et al. Artificial intelligence enabled Internet of Things: network architecture and spectrum access. *IEEE Comput Intel Mag* 2020; 15(1): 44–51.
30. Yang K, Shi Y, Zhou Y, et al. Federated machine learning for intelligent IoT via reconfigurable intelligent surface. *IEEE Netw* 2020; 34(5): 16–22.
31. Ramírez PLG, Taha M, Lloret J, et al. An intelligent algorithm for resource sharing and self-management of wireless-IoT-gateway. *IEEE Access* 2019; 8: 3159–3170.
32. Emir A, Kara F, Kaya H, et al. DeepMuD: multi-user detection for uplink grant-free NOMA IoT networks via deep learning. *IEEE Wirel Commun Lett* 2021; 10: 1133–1137.
33. Kwon M, Lee J and Park H. Intelligent IoT connectivity: deep reinforcement learning approach. *IEEE Sens J* 2019; 20(5): 2782–2791.
34. Wang D, Chen D, Song B, et al. From IoT to 5G I-IoT: The next generation IoT-based intelligent algorithms and 5G technologies. *IEEE Commun Mag* 2018; 56(10): 114–120.
35. Zhang L, Liang Y-C and Niyato D. 6G Visions: mobile ultra-broadband, super Internet-of-Things, and artificial intelligence. *China Commun* 2019; 16(8): 1–14.
36. Tang F, Mao B, Fadlullah ZM, et al. On a novel deep-learning-based intelligent partially overlapping channel assignment in SDN-IoT. *IEEE Commun Mag* 2018; 56(9): 80–86.
37. He X, Wang K, Huang H, et al. Green resource allocation based on deep reinforcement learning in content-centric IoT. *IEEE T Emerg Top Comput* 2018; 8(3): 781–796.
38. Wu Q and Zhang R. Towards smart and reconfigurable environment: intelligent reflecting surface aided wireless network. *IEEE Commun Mag* 2020; 58(1): 106–112.
39. Li J, Zhao Z, Li R, et al. AI-based two-stage intrusion detection for software defined IoT networks. *IEEE IoT J* 2018; 6(2): 2093–2102.
40. Guo S, Qi Y, Yu P, et al. When network operation meets blockchain: an artificial-intelligence-driven customization service for trusted virtual resources of IoT. *IEEE Netw* 2020; 34(5): 46–53.
41. Jiang C, Gao L, Wang T, et al. Crowd-MECS: a novel crowdsourcing framework for mobile edge caching and sharing. *IEEE IoT J* 2020; 7(10): 9426–9440.
42. Jiang F, Wang KZ, Dong L, et al. Stacked autoencoder-based deep reinforcement learning for online resource scheduling in large-scale MEC networks. *IEEE IoT J* 2020; 7(10): 9278–9290.
43. Du J, Yu FR, Lu G, et al. MEC-assisted immersive VR video streaming over terahertz wireless networks: a deep reinforcement learning approach. *IEEE IoT J* 2020; 7(10): 9517–9529.
44. Puri V, Jha S, Kumar R, et al. A hybrid artificial intelligence and Internet of Things model for generation of renewable resource of energy. *IEEE Access* 2019; 7: 111181–111191.
45. Han T, Muhammad K, Hussain T, et al. An efficient deep learning framework for intelligent energy management in IoT networks. *IEEE IoT J* 2020; 8: 3170–3179.
46. Lei L, Tan Y, Dahlenburg G, et al. Dynamic energy dispatch based on deep reinforcement learning in IoT-driven smart isolated microgrids. *IEEE IoT J* 2020; 8: 7938–7953.
47. Liu Y, Yang C, Jiang L, et al. Intelligent edge computing for IoT-based energy management in smart cities. *IEEE Netw* 2019; 33(2): 111–117.

48. Miao Y, Zhou M and Ghoneim A. Blockchain and AI-based natural gas industrial IoT system: architecture and design issues. *IEEE Netw* 2020; 34(5): 84–90.
49. Lv Z, Han Y, Singh AK, et al. Trustworthiness in industrial IoT systems based on artificial intelligence. *IEEE Transactions on Industrial Informatics* 2020; 17(2): 1496–1504.
50. Zhang X, Pipattanasomporn M, Chen T, et al. An IoT-based thermal model learning framework for smart buildings. *IEEE IoT J* 2019; 7(1): 518–527.
51. Jiang H. Mobile fire evacuation system for large public buildings based on artificial intelligence and IoT. *IEEE Access* 2019; 7: 64101–64109.
52. Xiao K, Shi W, Gao Z, et al. DAER: a resource preallocation algorithm of edge computing server by using blockchain in intelligent driving. *IEEE IoT J* 2020; 7(10): 9291–9302.
53. Dass P, Misra S and Roy C. T-safe: trustworthy service provisioning for IoT-based intelligent transport systems. *IEEE T Veh Technol* 2020; 69(9): 9509–9517.
54. Yang Z, Liang B and Ji W. An intelligent end-edge-cloud architecture for visual IoT assisted healthcare systems. *IEEE IoT J* 2021; 8: 16779–16786.
55. Mustafa A, Alahmed M, Alhammadi A, et al. Stress detector system using IoT and artificial intelligence. In: *Proceedings of the 2020 advances in science and engineering technology international conferences (ASET)*, Dubai, United Arab Emirates, 4 February–9 April 2020, pp.1–6. New York: IEEE.
56. Chen WL, Lin YB, Ng FL, et al. RiceTalk: rice blast detection using Internet of Things and artificial intelligence technologies. *IEEE IoT J* 2019; 7(2): 1001–1010.
57. Nurminen A and Malhi A. Green thumb engineering: artificial intelligence for managing IoT enabled houseplants. In: *Proceedings of the 2020 IEEE global conference on artificial intelligence and Internet of Things (GCAIoT)*, Dubai, United Arab Emirates, 12–16 December 2020, pp.1–7. New York: IEEE.
58. Chen WE, Lin YB and Chen LX. PigTalk: an AI-based IoT platform for piglet crushing mitigation. *IEEE T Ind Inform* 2020; 17: 4345–4355.
59. Wangoo DP and Reddy SN. Smart learning environments framework for educational applications in IoT enabled educational ecosystems: a review on AI based GUI tools for IoT wearables. In: *Proceedings of the 2020 IEEE 17th India council international conference (INDICON)*, New Delhi, India, 10–13 December 2020, pp.1–8. New York: IEEE.
60. Liu CY, Yu HY and Tsai IC. Applying AI analysis-based IoT system control to the individualized learning field. In: *Proceedings of the 2019 IEEE international conference on engineering, technology and education (TALE)*, Yogyakarta, Indonesia, 10–13 December 2019, pp.1–7. New York: IEEE.
61. Zhao S, Chen S, Li W, et al. The development of artificial intelligence education resources under the background of the Internet of Things. In: *Proceedings of the 2020 Chinese control and decision conference (CCDC)*, Hefei, China, 22–24 August 2020, pp.2327–2332. New York: IEEE.
62. Hallur GG, Prabhu S and Aslekar A. Entertainment in era of AI, big data & IoT. In: Hallur GG, Prabhu S and Aslekar A (eds) *Digital entertainment*. Singapore: Palgrave Macmillan, 2021, pp.87–109.
63. De Lima ES, Feijó B and Furtado AL. Adaptive storytelling based on personality and preference modeling. *Entertain Comp* 2020; 34: 100342.
64. Dilshad N, Hwang J, Song J, et al. Applications and challenges in video surveillance via drone: a brief survey. In: *Proceedings of the 2020 international conference on information and communication technology convergence (ICTC)*, Jeju, Korea, 21–23 October 2020, pp.728–732. New York: IEEE.
65. Lee MFR and Chien TW. Artificial intelligence and Internet of Things for robotic disaster response. In: *Proceedings of the 2020 international conference on advanced robotics and intelligent systems (ARIS)*, Taipei, Taiwan, 19–21 August 2020, pp.1–6. New York: IEEE.
66. Kim H, Ben-Othman J, Mokdad L, et al. CONTVERB: continuous virtual emotion recognition using replaceable barriers for intelligent emotion-based IoT services and applications. *IEEE Netw* 2020; 34(5): 269–275.
67. Ke R, Zhuang Y, Pu Z, et al. A smart, efficient, and reliable parking surveillance system with edge artificial intelligence on IoT devices. *IEEE T Intel Transp Syst* 2020; 99: 1–13.
68. Chakrabarty S and Engels DW. Secure smart cities framework using IoT and AI. In: *Proceedings of the 2020 IEEE global conference on artificial intelligence and Internet of Things (GCAIoT)*, Dubai, United Arab Emirates, 12–16 December 2020, pp.1–6. New York: IEEE.
69. Suresh GM and Madhavu ML. AI based intrusion detection system using self-adaptive energy efficient BAT algorithm for software defined IoT networks. In: *Proceedings of the 2020 11th international conference on computing, communication and networking technologies (ICCCNT)*, Kharagpur, India, 1–3 July 2020, pp.1–6. New York: IEEE.
70. Eskandari M, Janjua ZH, Vecchio M, et al. Passban IDS: an intelligent anomaly-based intrusion detection system for IoT edge devices. *IEEE IoT J* 2020; 7: 6882–6897.
71. Xu G, Zhao Y, Jiao L, et al. TT-SVD: an efficient sparse decision making model with two-way trust recommendation in the AI enabled IoT systems. *IEEE IoT J* 2020; 8: 9559–9567.
72. Li M, Yu FR, Si P, et al. Resource optimization for delay-tolerant data in blockchain-enabled iot with edge computing: a deep reinforcement learning approach. *IEEE IoT J* 2020; 7(10): 9399–9412.
73. Wang Q, Guo Y, Wang X, et al. Ai at the edge: blockchain-empowered secure multiparty learning with heterogeneous models. *IEEE IoT J* 2020; 7(10): 9600–9610.
74. Hu R, Guo Y, Li H, et al. Personalized federated learning with differential privacy. *IEEE IoT J* 2020; 7(10): 9530–9539.
75. Lim WYB, Xiong Z, Miao C, et al. Vincent poor: “hierarchical incentive mechanism design for federated machine learning in mobile networks.” *IEEE IoT J* 2020; 7(10): 9575–9588.
76. Jia Y, Zhong F, Alrawais A, et al. Flowguard: an intelligent edge defense mechanism against IoT DDos attacks. *IEEE IoT J* 2020; 7(10): 9552–9562.

77. Libri A, Bartolini A and Benini L. pAElla: edge AI-based real-time malware detection in data centers. *IEEE IoT J* 2020; 7(10): 9589–9599.
78. Teerapittayanon S, McDanel B and Kung HT. Distributed deep neural networks over the cloud, the edge and end devices. In: *Proceedings of the 2017 IEEE 37th international conference on distributed computing systems (ICDCS)*, Atlanta, GA, 5–8 June 2017, pp.328–339. New York: IEEE.
79. Savaglio C, Gerace P, Di Fatta G, et al. Data mining at the IoT edge. In: *Proceedings of the 2019 28th international conference on computer communication and networks (ICCCN)*, Valencia, 29 July–1 August 2019, pp.1–6. New York: IEEE.
80. Guin U, Cui P and Skjellum A. Ensuring proof-of-authenticity of iot edge devices using blockchain technology. In: *Proceedings of the 2018 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)*, Halifax, NS, 30 July–3 August, pp.1042–1049. New York: IEEE.
81. Mukhopadhyay SC, Tyagi SKS, Suryadevara NK, et al. Artificial intelligence-based sensors for next generation IoT applications: a review. *IEEE Sens J* 2021; 21: 24920–24932.
82. Ang LM, Seng KP, Ijamaru GK, et al. Deployment of IoV for smart cities: applications, architecture, and challenges. *IEEE Access* 2018; 7: 6473–6492.
83. Ijamaru GK, Ang KLM and Seng JK. Mobile collectors for opportunistic Internet of Things in smart city environment with wireless power transfer. *Electronics* 2021; 10(6): 697.
84. Ijaz A, Shahabuddin S, Sauter T, et al. Challenges of AI in wireless networks for IoT. *IEEE Ind Electr Mag* 2021; 15: 16–29.
85. Danzi P, Kalor AE, Sorensen RB, et al. Communication aspects of the integration of wireless iot devices with distributed ledger technology. *IEEE Netw* 2020; 34(1): 47–53.
86. Mastorakis G, Mavromoustakis CX, Batalla JM, et al. (eds). *Convergence of artificial intelligence and the Internet of Things*. Berlin; Springer, 2020.
87. Antonopoulos I, Robu V, Couraud B, et al. Artificial intelligence and machine learning approaches to energy demand-side response: a systematic review. *Renew Sust Energ Rev* 2020; 130: 109899.
88. Trakadas P, Simoens P, Gkonis P, et al. An artificial intelligence-based collaboration approach in industrial IoT manufacturing: key concepts, architectural extensions and potential applications. *Sensors* 2020; 20(19): 5480.
89. Zhang J and Letaief KB. Mobile edge intelligence and computing for the internet of vehicles. *Proc IEEE* 2019; 108: 246–261.
90. Sun L, Jiang X, Ren H, et al. Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application. *IEEE Access* 2020; 8: 101079–101092.
91. Hu L, Miao Y, Wu G, et al. iRobot-factory: an intelligent robot factory based on cognitive manufacturing and edge computing. *Fut Gen Comp Syst* 2019; 90: 569–577.
92. Li X, Li W, Yang Q, et al. Edge-computing-enabled unmanned module defect detection and diagnosis system for large-scale photovoltaic plants. *IEEE IoT J* 2020; 7(10): 9651–9663.
93. Velasco-Montero D, Fernández-Bemi J, Carmona-Gálán R, et al. On the correlation of CNN performance and hardware metrics for visual inference on a low-cost CPU-based platform. In: *Proceedings of the 2019 international conference on systems, signals and image processing (IWSSIP)*, Osijek, 5–7 June 2019, pp.249–254. New York: IEEE.
94. Chiu T-C, Shih Y-Y, Pang A-C, et al. Semisupervised distributed learning with non-IID data for AIoT service platform. *IEEE IoT J* 2020; 7(10): 9266–9277.
95. Wu H, Han H, Wang X, et al. Research on artificial intelligence enhancing Internet of Things security: a survey. *IEEE Access* 2020; 8: 153826–153848.