ITUPublications

International Telecommunication Union
Standardization Sector

ITU-T Technical Paper

(09/2023)

YSTP.AIoT

Challenges of and guidelines to standardization on artificial intelligence of things

Technical Paper ITU-T YSTP.AIoT

Challenges of and guidelines to standardization on artificial intelligence of things

Summary

The artificial intelligence of things (AIoT) is the combination of artificial intelligence (AI) technologies with the Internet of things (IoT) infrastructure to achieve more efficient IoT operations, improve human-machine interactions and enhance data management and analytics, but is not limited. From a comprehensive review of existing standardization efforts on AI and IoT, this Technical Paper describes concepts, characteristics, technical features, and approaches of AIoT. Then, it presents challenges and guidelines for standardization on AIoT. It also aims to provide technical insight and a clear direction for AIoT standardization from an ITU-T SG20 perspective.

Keywords

Artificial intelligence (AI), artificial intelligence of things (AIoT), Internet of things (IoT).

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Table of Contents

Technical Paper ITU-T YSTP.AIoT

Challenges of and guidelines to standardization on artificial intelligence of things

1 Scope

With the advent of data and artificial intelligence (AI) technology data driven Internet of things (IoT) applications are becoming increasingly important to harness the massive amounts of data generated by devices. As a combination of AI, data and IoT, artificial intelligence of things (AIoT) focuses on intelligent things and their applications that learn from the data generated and use these insights to make autonomous decisions. This Technical Paper aims to provide guidance on AIoT standardization from an ITU-T SG20 perspective as a key deliverable of the correspondence group (CG)-AIoT activities.

This Technical Paper covers the following items:

i) concepts, characteristics, technical features and approaches of AIoT in terms of technical trends and standardization,

ii) gap analysis of related standardization efforts, and

iii) identification of challenges and guidelines for future standardization.

2 References

[ITU-T F.742.1] Recommendation ITU-T F.742.1 (2022), *Requirements for smart class systems based on artificial intelligence*.

[ITU-T F.746.11] Recommendation ITU-T F.746.11 (2020), *Interfaces for intelligent question answering system*.

[ITU-T F.746.13] Recommendation ITU-T F.746.13 (2022), *Requirements for smart speaker-based intelligent multimedia communication systems*.

[ITU-T F.747.12] Recommendation ITU-T F.747.12 (2022), *Requirements for artificial intelligence based machine vision system in smart logistics warehouse*.

[ITU-T F.748.13] Recommendation ITU-T F.748.13 (2021), *Technical framework for the shared machine learning system*.

[ITU-T F.748.17] Recommendation ITU-T F.748.17 (2022), *Technical specification for artificial intelligence cloud platform – Artificial intelligence model development*.

[ITU-T F.748.20] Recommendation ITU-T F.748.20 (2022), *Technical framework for deep neural network model partition and collaborative execution*.

[ITU-T F.748.21] Recommendation ITU-T F.748.21 (2022), *Requirements and framework for feature-based distributed intelligent systems*.

[ITU-T F.749.4] Recommendation ITU-T F.749.4 (2021), *Use cases and requirements for multimedia communication enabled vehicle systems using artificial intelligence*.

[ITU-T F.749.13] Recommendation ITU-T F.749.13 (2021), *Framework and requirements for civilian unmanned aerial vehicle flight control using artificial intelligence.*

[ITU-T Y.3531] Recommendation ITU-T Y.3531 (2020), *Cloud computing – Functional requirements for machine learning as a service*.

[ITU-T Y.4470] Recommendation ITU-T Y.4470 (2020), *Reference architecture of artificial intelligence service exposure for smart sustainable cities*.

[ITU-T Y.Suppl.58] Supplement 58 to ITU-T Y-series Recommendations (2021), *Internet of things and smart cities and communities standards roadmap*.

[ITU-T Y.Suppl.63] Recommendation ITU-T Y.Sup.63 (2020), *Unlocking Internet of things with artificial intelligence*.

[ITU-T Y.Suppl.72] Supplement 72 to ITU-T Y-series Recommendations (2022), *ITU-T Y.3000-series – Artificial intelligence standardization roadmap*.

[ISO/IEC DTR 17903] ISO/IEC DTR 17903 (n.d), *Information technology – Artificial intelligence – Overview of machine learning computing devices*.

3 Definitions

3.1 Terms defined elsewhere

This Technical Paper uses the following terms defined elsewhere:

3.1.1 Internet of things [b-ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.2 thing [b-ITU-T Y.4000]: In the Internet of things, an object of the physical world (physical things) or of the information world (virtual things), which is capable of being identified and integrated into the communication networks.

3.2 Terms defined in this Technical Paper

This Technical Paper defines the following term:

3.2.1 artificial intelligence of things (AIoT): Internet of things powered by artificial intelligence to achieve intelligent IoT applications and things.

NOTE – AI technology can be applied within the end-to-end of IoT infrastructure, and especially be implemented in the device and the edge, to enhance the intelligence of IoT applications and things.

4 Abbreviations and acronyms

This Technical Paper uses the following abbreviations and acronyms:

AIoT Artificial Intelligence of Things

CG Correspondence Group

CPU Central Processing Unit

DAIaaS Distributed Artificial Intelligence-as-a-Service

GPU Graphics Processing Unit

HITL Human-In-The-Loop

IoT Internet of Things

IP Intellectual Property

KPI Key Performance Indicator

LPWAN Low-Power Wide Area Network

ML Machine Learning

MLP Multilayer Perceptron

OAM Operations, Administration and Management

QoE Quality of Experience

QoS Quality of Service

RFID Radio Frequency Identification

SC&C Smart Cities and Communities

USN Ubiquitous Sensor Network

5 Introduction to AIoT

5.1 Background of AIoT

With the rapid growth of IoT devices, the data collected by these devices will present a challenge in how to analyse this large amount of data. Without a way to analyse and understand this data, the collection of this data will be less beneficial. With the analytic capabilities of AI, IoT data can be analysed to classify and understand patterns and make more accurate decisions.

AI is playing an increasingly important role in IoT applications and deployments. It is the driver that enables analytics and decision making from the data collected by IoT devices. AI brings the ability to identify patterns and differences in the data generated by different IoT devices.

Harnessing the power of AI with the large amount of IoT data will lead to the full benefits of IoT data. This will lead to a variety of benefits such as proactive intervention, intelligent automation, and highly personalized experiences. It can also define new ways for IoT connected devices to work better together and make these systems easier to use. In addition, AI can provide programmatic reasoning, self-correction, and ultimate learning. It can manage the large amount of data generated by IoT devices and deliver a seamless user experience.

Figure 5-1 shows data driven IoT applications that leverage massive amounts of data. The scope of IoT applications has expanded to various domains, including consumer and industrial, and large amounts of data are continuously generated. Therefore, with the emergence of data and AI technologies, data driven IoT applications are becoming increasingly important to leverage the massive amounts of data from devices. Data technology enables the collection, storage, and analysis of data based on the data collected through IoT. On top of data, AI can help support intelligent applications without human intervention through data-based learning.

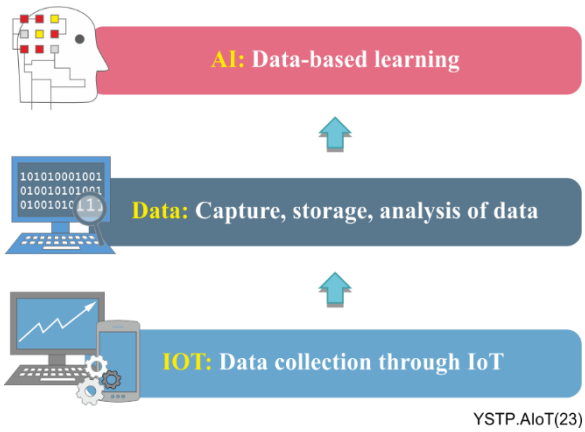

Figure 5-1 – Data-driven IoT applications to leverage the massive amounts of data

Data can be thought of as an asset that is difficult to exploit. AI can be seen as a key to unlocking the value of data; and machine learning (ML) is one of the technical mechanisms that underpins and enables AI.

Recently, IoT technology has shifted from simply connecting, sensing and communicating between devices to creating value through analytics and action. In this regard, data analytics and learning techniques are essential to support IoT applications with optimization and autonomy from relatively simple sensing and remote control. In addition, networks such as 5G networks can help support hyper-connectivity with benefits such as automated control, easy communication between devices and data sharing, high-speed, and near-zero latency for real time data processing.

As a combination of AI, data and IoT, artificial intelligence of things [b-AIoT] creates intelligent things that learn from the data they generate and use these insights to make autonomous decisions. Distributed and lightweight AI technologies enable intelligence at the edge, significantly reducing the need for and cost of cloud analytics. AI is expected to be the technology that helps IoT reach its full potential.

5.2 The concept of AIoT

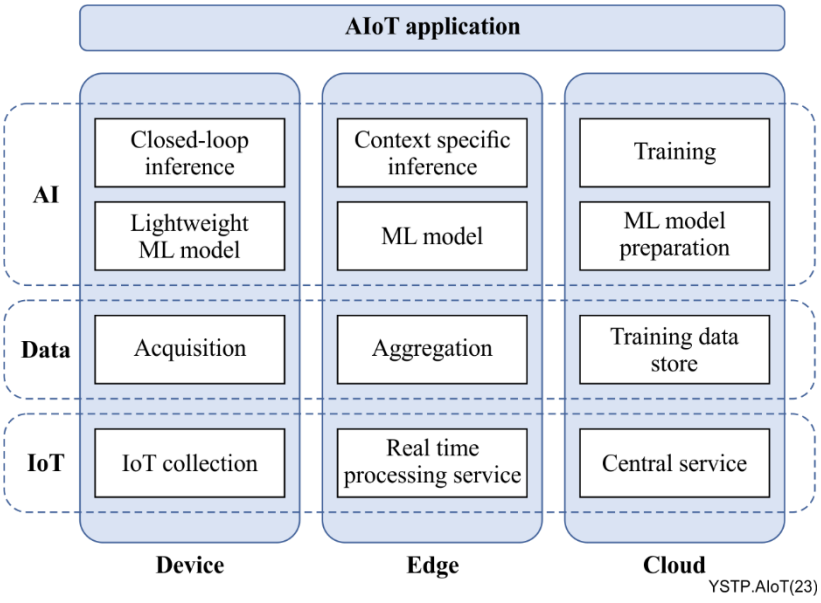

Figure 5-2 – The concept of AIoT

In AIoT, its capabilities are physically deployed not only on devices, but also in edges and clouds based on the application requirements, and these capabilities can be logically divided into AI, data, and IoT-related capabilities. Figure 5-2 shows these physical AIoT capabilities layouts and logical capabilities divisions.

A variety of user-centric AIoT applications can operate with AIoT capabilities deployed in the device, edge, and cloud.

AIoT deploys AI to the device, so that the huge amount of data is processed in real time on the device side, and only the necessary data are sent to the cloud. This approach can protect data privacy, reduce latency, and improve overall system reliability, as well as capture more valuable information from IoT devices to improve the user experience. The device should pre-process data, perform closed-loop inference, and interact with the edge or cloud to receive the embedded ML model update. AI on devices can also enable devices to make their own contextual decisions and perform autonomous control actions. AI-powered devices can also work together to accomplish a given task.

AIoT deploys AI to the edge, and the edge platform can provide a good environment for algorithm development and deployment. Deploying edge computing at the field side can efficiently support application distribution and model iteration and collaborate with the cloud where the cloud is responsible for algorithm iteration, and the edge computing is responsible for receiving new algorithms for execution at the field side. The edge should download the ML models from the cloud, perform contextual inference, and perform data analysis based on the application requirements. If the edge platform has sufficient hardware capabilities, ML models can be trained on the edge platform and deployed to devices. The edge platform can also coordinate collaboration between AI-powered devices and support local optimization of ML models deployed on devices.

AIoT deploys AI in the cloud, which is primarily responsible for data storage, data processing, data visualization, and analysis. The cloud should ingest collected data, normalize and create training data; provide storage and deployment capabilities for ML models, and interact with the edge and device to orchestrate various model deployment and training activities. Because the cloud collects and accumulates hyperparameters and processing data for all ML models on devices and at the edge, the cloud can support global optimization of these ML models.

AIoT may not work properly or may be interrupted due to AI model malfunctions, software infections due to malware, IoT breakdowns, and battery discharges. Therefore, operation management is essential to provide stable services based on AIoT, and it will be possible to provide operation management functions for AIoT devices in the edge or in the cloud.

Most importantly, depending on the application requirements and AI deployment method, the device, edge and cloud should work together to provide AIoT services to the application.

NOTE – Appendix II describes the classifications for AIoT according to several criteria.

5.3 Characteristics of AIoT

AIoT is accelerating the development of both AI and IoT technologies, which can be summarized as follows:

– AI driving IoT development

AI can learn relationships between massive amounts of complex data produced by IoT devices. In the technical field, AI algorithms perform intelligent analysis of IoT data, including positioning, prediction, classification, scheduling, etc., so that IoT devices can acquire perception, recognition, and autonomous control and collaboration capabilities. In the application area, AI helps to upgrade the IoT industry and optimize the user experience. Many smart IoT applications have been derived from AI, including smart wearable devices, smart homes, smart transportation, smart cities, smart factories, and so on.

– IoT driving AI development

AI development is inextricably linked to data. The massive amounts of data generated by the IoT can help AI optimize models and improve the accuracy, security, efficiency, and stability of AI results.

IoT systems have created a ubiquitously connected world where IoT devices collect millions of data sets and perform limited analysis. However, many practical services require analytical techniques to initiate appropriate actions. To address this issue, AI is being introduced to the IoT, ushering in the era of AIoT and achieving ubiquitous intelligent collaboration. AIoT can perform self-driven analytics, autonomous control and make smart decisions with minimal human intervention.

AIoT is the combination of AI technologies with the IoT infrastructure to support various applications. It can achieve more efficient IoT operations, improve human-machine interactions and enhance data management and analytics. The integration of IoT with AI will create a powerful technology that will be able to solve many problems related to big data integrated from different IoT devices. A huge amount of data generated by IoT devices needs to be analysed and eventually used for various applications.

Existing work on IoT-based AI implementation relies on cloud platforms; however, this approach is unacceptable for delay sensitive services. Edge computing extends cloud analytics to the edge of the network. In addition, on-site computing and analytics inside IoT devices can solve the problems of current approaches.

5.4 Advantages and considerations

There are many advantages of AIoT:

– Increased operational efficiency: AIoT can process and detect patterns in real-time operational data that are not visible to the human eye and can use this data to set real-time operating conditions that result in optimal outcomes. AI can optimize production processes and improve workflows resulting in increased efficiency and reduced operating costs.

– Enhanced risk management: AI can identify risks in a timely manner and use these insights to optimize their processes to increase safety, reduce losses, and make more informed business decisions.

– Create new applications and services: The ability to process and derive insights from large amounts of data, has opened up new technologies that did not exist before. These newly created capabilities can be used in many applications and services.

– Reduce failures: Predictive maintenance can help predict equipment failures by analysing data from machines and proactively scheduling maintenance, reducing the frequency and cost of failures (e.g., unplanned downtime).

– Enhanced customer experience: AIoT helps to tailor the user experience and provide personalized recommendations based on user intelligence, demographic information, and user behaviour.

– Reduced costs: By bringing analytics and decision making to the edge, AI helps to reduce the amount of data that needs to be transferred to the cloud, thereby reducing the costs associated with cloud connectivity and services.

– Network-agnostic services: Unlike traditional cloud-based AI services that are network-dependent, AI-enabled devices can operate autonomously and provide continuous service even when disconnected from the network.

– Autonomous control and collaboration: With minimal user intervention, AIoT devices can make their own contextual decisions and accomplish tasks through autonomous control and autonomous collaboration between AIoT devices.

However, there are some considerations for mitigating security and privacy concerns with governance and risk management as follows:

– Security, privacy and trust: The relationship between IoT devices, users, manufacturers and the network are untrusted, which can lead to security issues such as data breaches. AIoT can also be subject to malware infection and hacking.

– Policy and regulatory considerations: AIoT requires data collection and secondary data processing. At the government level, there is currently a lack of relevant policies and measures to ensure that people's privacy is not compromised. In addition, different countries have different degrees of data supervision for AIoT, which has caused difficulties in promoting AIoT.

– Risk management: AIoT involves passwords, network services, system interfaces, AI models, software components, hardware devices, device management, etc., all of which may pose risks to AIoT systems.

6 Technical features and approaches of AIoT

6.1 Technical features

6.1.1 AI/ML embedded in devices

6.1.1.1 Lightweight AI/ML (TinyML)

Considering the constraint environment of IoT, lightweight AI/ML agents for AIoT are essential. For example, tiny machine learning (tinyML) [b-tinyML] is the intersection of ML and embedded IoT devices as a fast-growing field of ML technologies and applications including hardware, algorithms, and software capable of performing on-device sensor data analytics with extremely low power consumption, thus enabling a variety of always-on use-cases and targeting battery-powered devices.

Considering ML embedded IoT devices, platforms should be provided to support prediction and inference capabilities among IoT devices.

6.1.2 AI at the edge

In the past, AI applications have mainly run in the cloud due to the complexity of ML models. However, there are some applications that cannot run in the cloud due to a lack of reliable and high-bandwidth connectivity or if the application is such that it requires the models to be run on the device itself. These could be applications that require fast, real-time operation which precludes the use of the cloud due to its latency. In addition, there may be concerns about the security and privacy of data, driving the need to store and process data on the local device.

By processing data on the device itself, a local computer or server rather than in remote data centres, AI at the edge offers the benefits of autonomy, lower latency, lower power, lower bandwidth requirements, lower costs and higher security, making it more attractive for new emerging applications and use cases.

6.1.3 AIoT during data processing

6.1.3.1 Intelligent data collection

Traditional IoT systems are unable to differentiate data as it is collected. In most cases, all the collected data is uploaded to the central system for analysis and processing. Therefore, a large amount of invalid data is collected, which wastes system resources and slows down the data processing time. Therefore, this error should be optimized to avoid negative impacts on systems such as storage and transmission.

AIoT can perform intelligent analysis during data collection and collect only valid data for specific service scenarios. This significantly reduces the amount of data collected by the system and enables the collected data to meet the requirements of specific service scenarios, thus improving the efficiency of the IoT system.

6.1.3.2 Predictive analytics and real time processing with accurate decision

The AI-enabled IoT network will generate huge datasets for businesses, which will need to perform historical analysis using pattern recognition technology to enforce predictive modelling capabilities with data analytics software. The use of algorithms will help find hidden data patterns between input and output values which is similar to human prediction and may exceed human capabilities. Predictive analytics capabilities will in turn accelerate the adoption of AIoT platforms and solutions.

At the same time, real-time data processing will contribute to the use of edge AI platforms and AIoT-driven solutions. Real time processing refers to responding quickly to a specific condition, while building knowledge to make accurate decisions about the events.

6.1.3.3 Intelligent data analytics

With the introduction of AI capabilities, AIoT systems can perform intelligent analysis of data. AI algorithms such as deep learning can be used to intelligently analyse the collected data, and data analysis can be extended to audio, image, video, and other areas that could not be processed before. This greatly expands the data processing scope of the IoT and enhances the service scenarios of the IoT.

The intelligence of data analysis is not only reflected in the fact that AI algorithms can handle more types of data, but also in the integration and analysis of data from different sources.

Intelligent data analytics can be deployed in the cloud. After various data are converged in the cloud, data from different sources are converged for analysis by AI algorithms, thus achieving effects that cannot be achieved by a single data source. Depending on the specific requirements, intelligent data analytics can also be deployed at the edge to more efficiently handle on-site data.

6.1.4 Collaboration

6.1.4.1 Algorithm management

Algorithms in AIoT systems are closely related to services and scenarios and there are a large number of algorithms running at the edge of the AIoT system. This requires a unified algorithm management to realize algorithm deployment, validation, optimization and update. Algorithm management systems are usually located in the cloud. Collaboration of algorithm deployment between the cloud and the edge must be achieved. AI services (e.g., specific algorithms for certain IoT scenarios) and orchestration of AI services should be provided to meet the requirements of the applications.

6.1.4.2 Collaboration between cloud and edge

AIoT needs to constantly support data processing, model training, learning evolution, etc. The cloud is mainly responsible for iterative model updates and data aggregation; the edge is mainly responsible for receiving data, initial processing, and then sending data back to the cloud for aggregation; and AIoT should be jointly scheduled between the cloud and the edge to meet the application requirements.

6.1.4.3 Collaboration among devices

Multiple AIoT devices can work together to accomplish a given task. Since individual AIoT devices make autonomous decisions based on information about their surroundings, global optimization can be achieved through collaboration between devices and the cloud.

6.1.4.4 Distributed artificial intelligence-as-a-service (DAIaaS)

AI is critical to embedding intelligence into smart cities and societies. Due to the exponential growth in the number of IoT devices the urgent need to reduce latency for real-time sensing and control, privacy constraints, and other challenges, the existing cloud-based AIaaS model, even with fog and edge computing support is not sustainable. Distributed artificial intelligence-as-a-service (DAIaaS) will facilitate the standardization of distributed AI deployment in smart environments, which in turn will allow developers of applications, networks, systems, etc., to focus on the domain-specific details without worrying about distributed training and inference. Ultimately, it will help systematize the mass production of technologies for smarter environments.

6.1.4.5 Decentralization with blockchain

Decentralized IoT edge computing improves speed and flexibility and is particularly suited to tasks that require short response times and the pre-processing of large amounts of data. There are several advantages to decentralization in terms of high speed, security, flexibility and robustness.

A blockchain is a distributed database of records that contains all transactions that have been executed and shared among participating parties in the network. Because the blockchain can handle the processing of billions of transactions between IoT devices, integrating IoT with blockchain and AI can significantly reduce the costs associated with deploying and maintaining large, centralized data and AI platforms and distribute computational and storage needs across the billions of devices that make up the IoT networks.

6.1.5 Trust management

Due to the potential risks of AIoT, trust management is necessary to support transparency and accountability. Accordingly, several trust features should be considered for the predictable and safe use of AIoT. In addition, appropriate indicators and weights will be selected.

NOTE – Appendix III describes the details of trust management for AIoT.

6.2 Approaches

6.2.1 User-centric AIoT

IoT systems can not only learn from users but also provide easy-to-understand explanations of decisions or predictions. In this way, users can understand the reasons behind AI decisions in order to speed up the supervision process that confirms or refutes the decision, based on whether the highlighted reasons make sense in the given context.

This Technical Paper proposes to focus on user-centric AI approaches for the automatic generation of explanations based on the analysis of discriminant inputs in the training cases and artificial neuron weights in the multilayer perceptron (MLP) trained with backpropagation. This will require extensive analysis in the following areas:

– Human-in-the-loop (HITL) ML, reasoning, and planning: Allowing humans (users) to not only understand and follow the learning, reasoning, and planning process of AI models (being explainable and accountable), but also to seamlessly interact with them to create a continuous feedback loop that allows the model to deliver better results every time with knowledge of the world, and the specific user's personal perspective.

– Multimodal perception and modelling: Enabling AI models to perceive and interpret complex real-world environments, human actions, and interactions situated in IoT environments and the associated emotions, motivations, and social structures. This requires enabling AIoT systems to build and maintain comprehensive models that should strive for a more human-like understanding of the world and incorporate common sense knowledge that captures causality and is grounded in physical reality.

– User-centred AI interaction and collaboration: Developing paradigms that enable users and AI models to interact and collaborate with wearable IoT systems and smart environments in ways that enhance human abilities and empower people.

– Societal awareness: The ability to model and understand the consequences of complex network effects in large-scale mixed communities of users, and AI models interacting over multiple temporal and spatial scales. This includes the ability to balance the needs of individual users with the public both good and its societal concerns.

– Legal and ethical foundation for responsible AI: Ensuring that the design and use of AI is consistent with ethical principles and human values, taking into account the cultural and societal context while enabling human users to act ethically and respecting their autonomy and self-determination.

7 Conceptual model of AIoT

A conceptual model of AIoT is shown in Figure 7-1. In general, it consists of five parts: the data source, the data processing and management, the application-based analytics, and the applications and sources. The data source outputs raw data which could be from IoT devices such as sensors, devices, social media, etc. The raw data is collected, ingested, and even simply analysed in the data processing and management part. Then, AI-based analytics, which includes data exploration, predictive analytics, and decision making are performed for the applications. In addition, the entire data flow from the data source to applications should be coupled with data security and governance management.

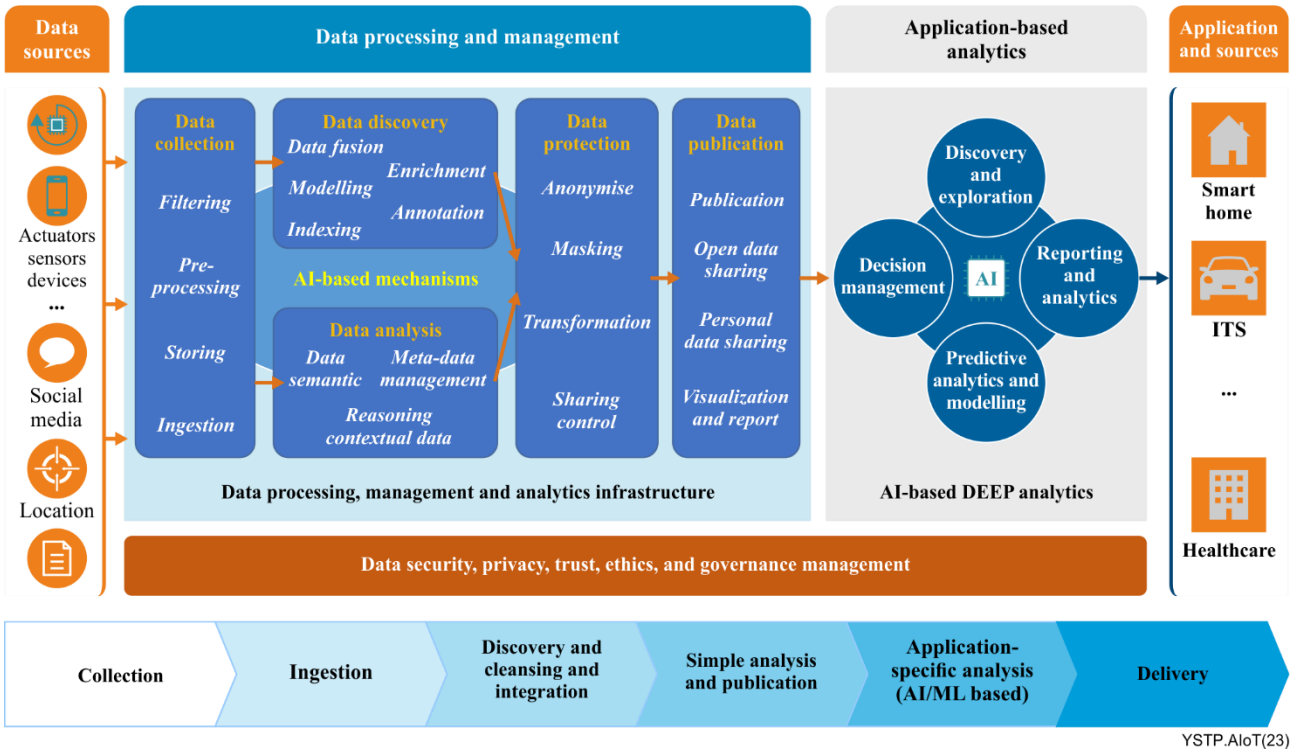

Figure 7-1 – A conceptual model of AIoT

The data processing and management part and application-based analytics are considered as the core of AIoT. In the data processing and management part, it is necessary to label data in order to transform it into training data for AI models. In addition, data from data sources are needed to cover different cases or situations to obtain generic AI models, i.e., data distribution of a data set could be a factor in the data processing and management part. In terms of application-based analytics, tiny AI is one of the most obvious features of AIoT. Due to size, power, computation, and other constraints, AI models

used in the cloud need to be tailored or cut down, but their functions and performance do not suffer much. In addition, distributed AI technology such as shared ML [ITU-T F.748.13], has emerged in recent years and has potential for AIoT.

8 Review of existing standardization efforts on AI and IoT

The AI market can be broadly categorized into AI supply and application ecosystems centred on cloud operators, network operators, and manufacturers, which are developing in vertical silos for each operator. The three categories of AI ecosystems are competing for leadership in the AI market based on their respective strengths. AI standardization such as these market trends can be classified into three types: cloud operator-centric, network operator-centric, and manufacturer-centric.

In ITU-T, AI standardization is being carried out in SG9, SG13, SG16, and SG20 and can be classified into a (draft) Recommendation with a target system to which AI is applied and a (draft) Recommendation in the form of an application service without a clear target system. The studies in ITU-T SG13 are mainly concerned with standardizing the application of AI to network nodes of AN/CN or UE of IMT-2020 and standardizing the loading of AI into cloud systems. And ITU-T SG20 mainly deals with the standardization of technologies that apply AI to IoT devices.

Companies in the ICT industry want to build an AI ecosystem in a way that maximizes their profits. Reflecting this competition in the AI ecosystem, standardization in ITU-T is also progressing with cloud operator-centric, network operator-centric, and manufacturer-centric standardization separated from each other.

Even if the same AI function is used in different application service domains, the standardization for AI is vertically separated and there may be a problem that a separate AI standard is developed despite the same AI function. In addition, the number of AI-embedded systems is increasing significantly, and despite the need to provide convergence services through collaboration among AI-embedded systems, the problem is that vertically separated AI standardization cannot support collaboration among heterogeneous AI-embedded systems.

Meanwhile, [b-ISO/IEC JTC 1/SC 42] is also in the process of standardizing various AI systems. Unlike ITU-T, the ISO/IEC SC42's AI standardization deals with general AI systems and services without clearly specifying the target system to which AI is applied such as network, cloud, or IoT.

[b-ISO/IEC JTC 1/SC 42] standards lack feasibility because they do not consider the device, platform and service environment of actual cloud operators, network operators, and device manufacturers. However, due to previous work in risk management, robustness assessment, and quality evaluation, within ISO/IEC that has been extended to AI, ISO/IEC SC42 is ahead of ITU-T standardization in terms of operations, administration and management (OAM). In particular, [b-ISO/IEC JTC 1/SC 42] is leading the standardization of issues within OAM derived from AI such as trustworthiness, explainability, and bias in AI.

ITU-T's AI standardization, which is vertically separated by network operators, cloud operators, and device manufacturers to reflect competition in the AI ecosystem needs to be conducted in cooperation with ISO/IEC SC42's standardization of OAM such as trustworthiness for general AI. It will be possible to strengthen synergies in AI standardization and reduce market confusion caused by separate AI standards.

NOTE – Appendix I provides a comprehensive overview of existing standardization efforts on AI and IoT in ITU-T and [b-ISO/IEC JTC 1/SC 42].

9 Challenges and guidelines for standardization on AIoT

9.1 Existing standard roadmap for AI and IoT

9.1.1 Standardization roadmap for AI from ITU-T SG13

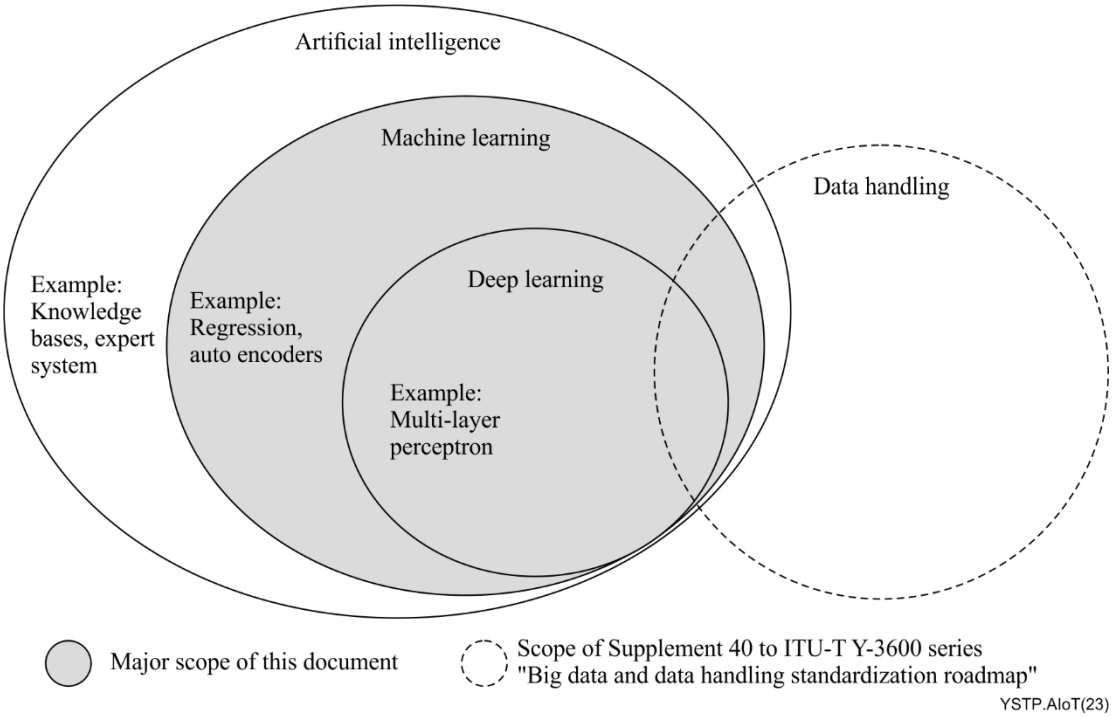

Figure 9-1 – AI technologies (from ITU-T SG13)

[ITU-T Y.Suppl.72]: "Artificial Intelligence standardization roadmap" from ITU-T SG13 provides the standardization roadmap for AI in the information technologies. This Supplement specifically covers the AI techniques developed with ML including deep learning, neural networks and so on.

9.1.2 Standardization roadmap for IoT from ITU-T SG20

[ITU-T Y.Suppl.58]: "Internet of things and smart cities and communities standards roadmap" from ITU-T SG20 presents the joint coordination activity on Internet of things and smart cities and communities (JCA-IoT and SC&C) roadmap which contains a collection of standards and ITU-T Recommendations related to Internet of things (IoT), smart cities and communities (SC&C), network aspects of identification systems, including radio frequency identification (RFID), and ubiquitous sensor networks (USN).

9.2 Challenges for standardization on AIoT

Although the integration of AI with IoT will bring many benefits that can increase the efficiency of IoT data there are many standardization challenges that stand in the way of successful convergence of IoT with AI, including:

– Complexity: Running operations with a large scale of IoT makes the coordination process very complex. Integrating AI with complex systems will not be an easy task as it requires taking into account various IoT constraints such as processing power, memory, and delay in real-time applications.

– Heterogeneity: As the IoT continues to grow, the need for services that work with multiple IoT applications will need to continue to increase in order to realize the promised efficiency gains. In addition, IoT systems use a wide variety of devices with different characteristics

which makes the connectivity and coordination process more difficult. Therefore, the deployment of AI should take these different components into account.

– Security, privacy, and trust: To build autonomous IoT systems and applications, it is essential to ensure the confidentiality, integrity and credibility of data and AI models for security and privacy while supporting the successful deployment and trustworthy operation of IoT systems.

– Accuracy and speed: The large-scale deployment of billions of IoT devices generates large amounts of data. The main goal of AIoT is expected to perform analysis and make decisions from this data in a short time especially for real-time IoT applications.

– Regulatory compliance: AIoT with many integrated services provided by multiple partners and new business models will create legal challenges and legal relationships that will need to be addressed between the parties such as intellectual property (IP) and other regulatory issues.

– Algorithm deployment: Algorithm provisioning and update interfaces need to be standardized to enable interfacing between different vendors. Cloud system vendors focus on the unified management of algorithms and data analysis. End and edge-side device vendors focus on producing devices that are suitable for field deployment. The algorithms can be provided by vendors focused on algorithms. Standardization of algorithm deployment and update interfaces is beneficial for different vendors to play their roles in AIoT development and evolution.

– Diversity: There are a wide variety of IoT scenarios and differences in the requirements for intelligent sensors, transmission, algorithms, and effects.

9.3 Landscape for AIoT standardization

Figure 9-2 depicts a layered view of AIoT, which provides an inspiration for the standardization landscape. The application layer refers to AIoT applications provided by AIoT. The supporting layer mainly includes AIoT service, algorithm management and API which provides a programming interface to AIoT applications. The network layer includes functions in communication and computation aspects. The device layer mainly includes definition and interoperation for AIoT devices that perform sensing tasks. The management and security layer mainly monitors AIoT systems and ensures its security.

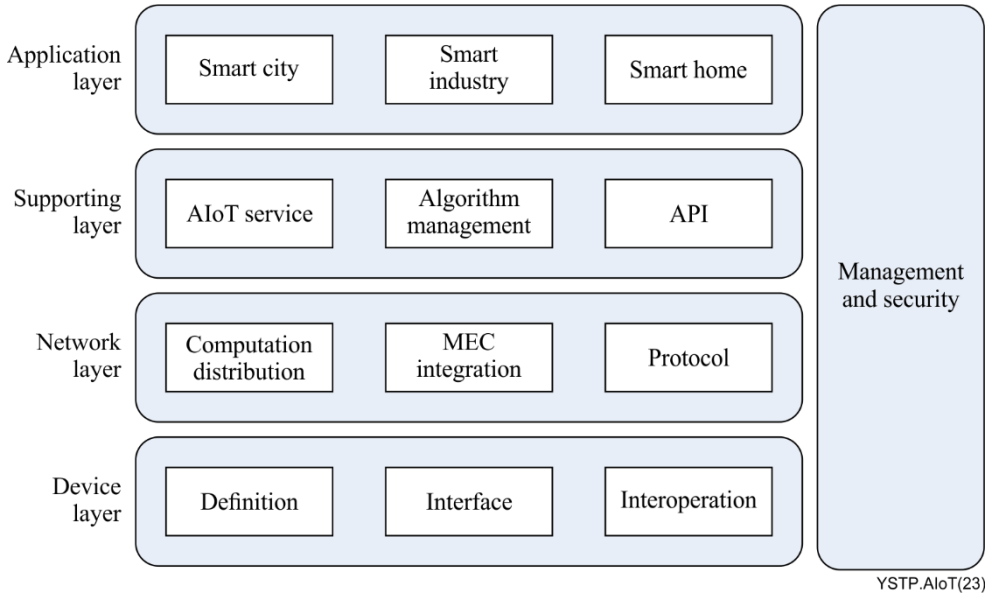

Figure 9-2 – Landscape for AIoT standardization

It is realistic to develop standards for the device layer as follows, but not limited to.

– Definition of an AIoT device. It is necessary to define the requirements, functions, and components of the AIoT device, which indicates the difference to the IoT device.

– Interface to an AIoT device. In addition to the existing interfaces of the IoT device, it is possible to extend existing interfaces and define new ones to support AIoT devices interacting with AI technologies.

– Interoperation. It is necessary to support interoperation for AIoT devices, with which AIoT devices can cooperate with each other to perform a certain task.

It is realistic to develop standards for the network layer as follows, but not limited to.

– Protocol enhancement. In addition to existing protocols for IoT such as 5G, NB-IoT, bluetooth, etc., it is possible to enhance the existing protocols for AIoT that meet its requirements and technical characteristics.

– MEC integration. It is believed that MEC plays an important role in AIoT especially due to the close position of storage and computation capability. How to integrate MEC to the AIoT system in terms of hardware and software needs to be specified.

– Computation distribution. Due to limited computation capabilities in an AIoT device, it is possible to define requirements and corresponding methods to distribute computation tasks to other entities such as data centre(s) or MEC(s).

It is realistic to develop standards for the supporting layer as follows, but not limited to.

– AIoT service. It is possible to define the AIoT service, which is integrated into AIoT applications in the application layer, in terms of requirements and functions.

– Algorithm management. It is necessary to define algorithm provisioning and update interfaces to enable collaboration among different entities.

– API. It is necessary to identify signalling and protocol to provide interfaces of AIoT service to applications.

It is realistic to develop standards in the application layer as follows, but not limited to.

– Practice. It is necessary to define requirements and practices for the application of AIoT such as smart home, smart city, smart industry, etc.

It is realistic to develop standards in the management and security layer as follows, but not limited to.

– Key performance indicator (KPI). It is necessary to define a set of KPI(s) to monitor AIoT to ensure it is operating in a normal and secure state.

– Security for AIoT. It is necessary to define requirements and security architecture for AIoT to provide standard security solutions for AIoT.

9.4 Potential work items for AIoT standardization

Table 9-1 lists some potential work items of AIoT based on the analysis above.

Table 9-1 – Potential work items of AIoT standardization

Layer	Work items	Brief description	Related Recommendations
Application layer	Applications scenarios	Vertical use cases of applying AIoT, more intelligence than existing smart services.	[b-ITU-T Y.4003], [b-ITU-T Y.4601], [b-ITU-T Y.4209], [b-ITU-T Y.4123], [b-ITU-T Y.4004]; Y.smart-education, Y.IoT-SmartBuild,

Table 9-1 – Potential work items of AIoT standardization

Layer	Work items	Brief description	Related Recommendations
			Y.smart-PBRS, Y.Smart-SBS, Y.IoT-Smartcity-Risk
	Requirements	Vertical requirements for AI effects (e.g., self-configuring, self-healing, self-optimizing, etc.).	[b-ITU-T Y.4217], [b-ITU-T Y.4482]; Y.isms, Y.AEDS-smarthome, Y.dt-ITS, Y.dt-IWCS, Y.ElecMon-Reqts, Y.EV-charging, Y.IIoT-infra-SM-fr, Y.IoT-BPM-reqts, Y.IoT-RTPS, Y.IoT-SFFS, Y.IoT-SmartBuild, Y.SRC, Y.RA-FML, Y.RA-PHE, Y.smart-education, Y.Smart-SBS
Supporting layer	AIoT service and API	AIoT services and quality of service (QoS).	
	Algorithm management	Algorithm deployment and upgrading interfaces (e.g., interface between cloud and edge / device); Algorithm package definition (e.g., deployment environment, required resource, running interface, etc.).	
Network layer	Network requirements	Requirements to network in terms of data transmission and computation transmission including requirements for protocol, MEC integration and computation distribution.	
Device layer	Definition and interface	Requirements, functions, components of the AIoT device; Interfaces to support AIoT device interacting with AI technologies; Requirements and testing specifications to AI chips.	
	Interoperation	Interoperation for corporation among AIoT devices; Lightweight AI/ML for embedded IoT devices; Cross platforms inference engine.	
Management and security	Requirements and architecture for management and security	Security requirements and architecture for AIoT to provide standard security solutions; Architecture for AIoT operation, including functionalities and components, internal and external interface;	

Table 9-1 – Potential work items of AIoT standardization

Layer	Work items	Brief description	Related Recommendations
		KPI to monitor AIoT to ensure its operating in a normal and secure state.	
Common aspects	Data processing flow	A general framework for applying AI during whole data processing procedure (e.g., data capture, data process, data analysis, etc.).	[b-ITU-T Y.4216], [b-ITU-T Y.4481], [b-ITU-T Y.4602]
	Distributed artificial intelligence	Framework of distributed artificial intelligence in IoT.	
	Semantic	Automatic data analysing, processing, and learning for IoT, to support smart services based on IoT data; Data model for IoT.	[b-ITU-T Y.4484]; YSTR.SemComm.IoT
	Architecture and framework	General AIoT architecture; Framework for machine learning in IoT-integration of ML components into IoT, preparing and deploying ML models in IoT environments; Architecture for vertical applications to apply AI.	[b-ITU-T Y.3172], [b-ITU-T Y.3179]; Y.cnce-IoT-arch, Y.RA-SDL, Y.RMDFS-arch, Y.smart-PBRS
		Platform architecture and interface.	Y.IoT-CONV-fr, Y.IoT-CRE-fr
		Requirements from different vendors (Cloud system vendor, edge system vendor, device vendor, algorithm provider); Computation distribution and collaboration between different entities (cloud, edge, device).	Y.AI-DECCS, Y.CDML-arc

10 Conclusion

AIoT refers to the combination of AI and IoT to achieve more efficient operations, improve human-machine interactions, enhance data analytics, etc. This Technical Paper provides an overall insight into AIoT, including technical features, a conceptual model and standardization and aims to promote the development and deployment of AIoT.

Appendix I

Comprehensive review of existing standardization efforts on AI and IoT

As supporting information for a brief review is given in clause 8, this Appendix provides a comprehensive review of existing standardization efforts on AI and IoT in ITU-T and [b-ISO/IEC JTC 1/SC 42] in terms of target systems (device, edge, cloud) and applications where AI technologies are deployed.

Standards for AI algorithms themselves ([b-ISO/IEC JTC 1/SC 42]), standards for data quality for AI ([b-ISO/IEC JTC 1/SC 42]), standards for generic AI systems ([b-ISO/IEC JTC 1/SC 42]), AI standards for image and speech recognition (ITU-T SG16, [b-ISO/IEC JTC 1/SC 29]), AI standards for communication networks (ITU-T SG 2, 11, 12, 13) were excluded from the gap analysis.

Table I.1 – ITU-T standardization activities related to AI and IoT

SG	Reference	Title	Status	AI applied targets and domains					Gap/ Note
				User	Appli-cation	Device	Edge	Cloud	
SG 13	[ITU-T Y.3531]	Cloud computing-Functional requirements for machine learning as a service	In force (Approved on 2020-09-29)	–	–	–	–	Functional requirements for MLaaS	–
SG 16	[ITU-T F.749.13]	Framework and requirements for civilian unmanned aerial vehicle flight control using artificial intelligence	In force (Approved on 2021-06-13)	–	Transportation	Framework for unmanned aerial vehicle	–	–	–
SG 16	[ITU-T F.749.4]	Use cases and requirements for multimedia communication enabled vehicle systems using artificial intelligence	In force (Approved on 2021-06-13)	–	Transportation and multimedia	Use cases and requirements for vehicle systems	–	–	–
SG 16	[ITU-T F.748.13]	Technical framework for shared machine learning system	In force (Approved on 2021-06-13)	–	Multimedia	–	–	Architecture and procedures for shared machine learning system	Target system is not specified
SG 16	[ITU-T F.742.1]	Requirements for smart class based on artificial intelligence	In force (Approved on 2022-12-14)	–	Multimedia and education	Requirements for class interaction	–	Requirements for AI-based smart class systems	–
SG 16	[ITU-T F.CDN-AINW]	Requirements and reference model for CDN services over AI network	Under study (Timing: 2023)	–	Multimedia and network	-	Requirements and reference model of CDN services over AI network	–	–
SG 16	[ITU-T F.748.20]	Technical framework for deep neural network model partition and collaborative execution	In force (Approved on 2022-12-14)	–	Multimedia and network	Framework of collaborative inference client	Framework of collaborative inference server	–	–

Table I.1 – ITU-T standardization activities related to AI and IoT

SG	Reference	Title	Status	AI applied targets and domains					Gap/ Note
				User	Appli-cation	Device	Edge	Cloud	
SG 16	[ITU-T F.746.13]	Requirements for smart speaker based intelligent multimedia communication system	In force (Appro-ved on 2022-03-16)	–	Multime-dia	Requirements for smart speaker	–	Intelligent multimedia platform requirement	Target platform is not specified
SG 16	[ITU-T F.746.11]	Interfaces for intelligent question answering system	In force (Appro-ved on 2020-08-13)	Func-tions and inter-faces of question answe-ring service	Multime-dia	–	–	–	Target system is not specified
SG 16	[ITU-T F.AICP-GA]	Technical specification for artificial intelligence cloud platform: General architecture	Under study (Timing: 2023)	–	None	–	–	Architecture and requirement for AI cloud platform	–
SG 16	[ITU-T F.748.17]	Technical specification for artificial intelligence cloud platform – Artificial intelligence model development	In force (Appro-ved on 2022-12-14)	–	None	–	–	Framework for the cloud-based development of AI models	–
SG 16	[ITU-T F.AI-CPP]	Technical specification for artificial intelligence cloud platform: Performance	Under study (Timing: 2024-04) [Carried to next study period]	–	None	–	–	Technique specification for AI cloud performance	–
SG 16	[ITU-T F.748.21]	Requirements and framework for feature-based distributed intelligent systems	In force (Appro-ved on 2022-12-14)	–	Multime-dia	Requirements and framework for clients	–	Requirements and framework for cloud	–
SG 16	[ITU-T F.TCEF-FML]	Trusted contribution evaluation framework on federated machine learning services	Under study (Timing: 2023)	–	None	Evaluation framework for federated ML	–	–	Target system is not specified
SG 16	[ITU-T F.747.12]	Requirements for artificial intelligence based machine vision system in smart logistics warehouse	In force (Appro-ved on 2022-12-14)	–	Logistics	Requirements for AI based machine vision	–	–	Target system is not specified
SG 16	[ITU-T F.AI-SF]	Requirements for smart factory based on artificial intelligence	Under study (Timing: 2023) [Carried to next study period]	–	Factory and multime-dia	–	Framework and requirements for edge devices	Framework and requirements for AI cloud	–
SG 20	[ITU-T Y.4470]	Reference architecture of artificial	In force (Appro-ved on	–	Smart city	–	–	Requirements and architecture	–

Table I.1 – ITU-T standardization activities related to AI and IoT

SG	Reference	Title	Status	AI applied targets and domains					Gap/ Note
				User	Appli-cation	Device	Edge	Cloud	
		intelligence service exposure for smart sustainable cities	2020-08-29)					for AI service exposure	
SG 20	[ITU-T Y.Suppl.63]	Unlocking Internet of things with artificial intelligence	In force (Agreed on 2020-07-16)	–	Smart city	IoT in smart cities	–	AI based technological implementation for smart cities	–
SG 20	[ITU-T Y.CDML-arc]	Reference architecture of collaborative decentralized machine learning for intelligent Internet of things services	In force (Approved on 2023-11-29)	–	None	Architecture of collaborative decentralized ML	Architecture of collaborative decentralized ML	Architecture of collaborative decentralized ML	–
SG 20	[ITU-T Y.RA-FML]	Requirements and reference architecture of IoT and smart city & community service based on federated machine learning	Under study (Timing: 2023-Q1)	–	Smart city	Requirements and architecture of federated ML	Requirements and architecture of federated ML	Requirements and architecture of federated ML	–
SG 20	[ITU-T Y.AI-DECCS]	Functional architecture of AI enabled device-edge-cloud collaborative services for IoT and smart city	Under study (Timing: 2023-Q3)	–	Smart city	Functional architecture of AI enabled device	Functional architecture of AI enabled edge	Functional architecture of AI enabled cloud	–

Table I.2 – [b-ISO/IEC JTC 1/SC 42] standardization activities related on AI and IoT

WG	Reference	Title	Status	AI applied targets and domains					Gap/ Note
				User	Appli-cation	Device	Edge	Cloud	
WG5	[ISO/IEC DTR 17903]	Information technology – Artificial intelligence – Overview of machine learning computing devices	WD	–	–	ML computing device	–	–	To be updated

Appendix II

AIoT classifications

The scope of AIoT is very broad, ranging from micro-sensors to autonomous vehicles, and its architecture and functions vary greatly depending on the mobility of the devices and the operation methods such as device-to-device collaboration. Therefore, after recognizing and categorizing the key characteristics of AIoT, it would be desirable to standardize AIoT limited to a clear scope. This Appendix describes the classifications for AIoT.

II.1 AIoT classifications

AIoT can be classified as follows according to the operation domain, method and size.

(1) AIoT classification based on size

– Tiny disposable AIoT: This is a device that autonomously analyses data and makes inferences and decisions with AI embedded in a sensor as small as a coin. It is typically battery powered and transmits sensed data over a low-power wide area network (LPWAN) such as LoRa when needed. Due to the low cost of the device, when the battery is depleted, the device is discarded without battery replacement.

– Small-size AIoT: This is a type of device in which AI for autonomous operation is mounted on small home appliances or unmanned aerial vehicles which have limitations in computing power and memory size for product price competitiveness and so on. Generally, it is connected to a high-speed network such as WiFi, 4G/5G mobile communication, and uses a replaceable battery or wired power supply.

– Large-scale AIoT: This is a system that operates autonomously based on high-precision inferencing and decision making with high-performance AI installed in systems with relatively sufficient power and large computing and memory capacity, such as automobiles and large home appliances.

(2) AIoT classification based on mobility

– Fixed AIoT: This is a device that does not change its installed location, has the same wired or wireless network configuration and has relatively little change in the surrounding environment.

– Mobile AIoT: This is a device that moves under its own power, such as self-driving cars and unmanned aerial vehicles, or is attached to a person or object to change location and perform autonomous operations and tasks. Mobile AIoT uses mobile communication technologies such as 4G/5G to support seamless communication, and its surrounding environment may change significantly due to movement.

(3) Classification based on cyber and physical domains

Depending on whether the scope of tasks handled by AIoT is limited to the physical domain or extends to the cyber domain, AIoT can be classified as follows:

– AIoT in the physical domain: AIoT devices are directly executed and managed in the physical domain through inference and decision-making based on input data.

– AIoT in the cyber domain: Data collection, analysis, and inference results using AIoT are used for information provision, monitoring, simulation, and prediction services in the cyber domain such as a digital twin or a metaverse.

(4) Classification based on collaboration

AIoT devices can be classified according to whether they work alone or collaborate with a server after installation as follows:

– Standalone AIoT model: The installed AIoT device operates on its own without any communication such as management and collaboration with external systems.

– Server-client AIoT model: A centralised AIoT platform or edge node is required to deploy and update AI models for AIoT devices and to manage AIoT devices.

– Peer to peer AIoT model: AIoT devices perform a given task through horizontal collaboration with other AIoT devices without the control and management of a centralised platform.

(5) Classification based on the level of autonomy

– Semi-autonomous AIoT: This is a human-in-the-loop (HITL) method that performs semi-autonomous operations with minimal administrator intervention in the case of AI malfunction for the purpose of operation management, etc.

– Fully-autonomous AIoT: This is a fully autonomous device that requires no user intervention from installation to disposal or uses AI in IoT platforms to manage and monitor individual AIoT devices without human intervention.

(6) Classification based on model training

– Self-training AIoT: In AIoT with sufficient computing and memory capabilities, a large amount of learning data can be accumulated and managed within the AIoT device, which the AIoT device uses to train the model itself and then perform inference and decision-making.

– Deploy model-equipped AIoT: Tiny disposable AIoT or small-sized AIoT cannot train its own model due to limitations in its own computing and storage capabilities, so it uses an AI model that is trained and distributed from cloud and edge systems.

(7) Classification based on the operation management

– Local operation management: The user monitors and checks the operation status of the AIoT device through the direct connection setting to the AIoT device, and changes and controls the operation options, etc.

– Remote operation management: The AIoT device supports remote operation management protocols such as TR-069, MQTT, and LwM2M to be remotely monitored and control the operation of the AIoT device.

(8) Classification based on the management entity

– Manufacturer-oriented AIoT management: A manufacturer that develops and produces AIoT devices continuously monitors and manages the normal operation of AIoT devices and firmware upgrades even after its AIoT devices are sold and installed.

– Platform-oriented AIoT management: When a user purchases an AIoT device and registers it on the service provider's platform, the service platform manages the status and normal operation of the registered AIoT device.

– User-oriented AIoT management: The owner or administrator of the AIoT device monitors and controls the operational status of AIoT devices with management rights.

II.2 Examples of AIoT classifications

The table below shows how various AIoT applications can be classified based on the AIoT classification presented in the previous section.

Table II.1 – Examples of AIoT classifications

AIoT classification	Size	Mobility	Cyber/ Physical	Collabo-ration	Autonomy	Model train	OAM	Management entity
Remote sensing	Small	Fixed	Physical	Stand-alone	Semi	Distri-buted	Local	User
Smart appliance	Medium	Fixed	Physical	Collabo-ration	Full	Distri-buted	Local	Manufacturer
Unmanned aerial vehicle	Medium	Mobile	Physical	Stand-alone	Full	Distri-buted	Remote	User
Digital twin-based facilities	Large	Fixed	Cyber	Collabo-ration	Semi	Self	Remote	Platform
Etc.	…	…	…	…	…	…	…	…

Appendix III

Trust management for AIoT

It is essential to anticipate the potential risks of AIoT, and to evaluate and manage the trustworthiness to increase transparency and accountability. For several reasons, assessing and managing the trustworthiness of AIoT are very complex. This Appendix describes trust features for the predictable and safe use of AIoT:

- Measurement and calculation: It is necessary to derive trust as a generalized formula, despite the diversity of AIoT services and differences in their intrinsic characteristics. It should be able to define measurable AIoT trust metrics and determine the level of trust in AIoT through trust calculations. The level of trust in AIoT can be measured by classifying it into an objective method that is quantitatively measured such as quality of service (QoS), or a subjective method that is qualitatively calculated such as quality of experience (QoE). Different AIoT devices and applications may require different trust attributes.
- Trust relationship: Trust relationship has been studied in the traditional social domain in addition to the human-to-human trust, as well the trust relationship between AIoT devices and humans, as well as among AIoT devices, etc., should be defined, and trust-based interactions between them should be analysed.
- Trust management: Trust management technology is required as a separate common layer covering all vertical layers. Trust management has key functions such as monitoring management, data management, algorithm management, expectation management, and decision management. In particular, trust information about reputation and recommendations can be used to support these functions.
- Dynamically changing properties: Trust indicator values for AIoT are dynamically changing and may fluctuate depending on data and the surrounding circumstances; therefore, continuous tracking and management are required.
- Constrained environment: Constraints on hardware performance such as central processing unit (CPU) / graphics processing unit (GPU), memory, and storage that make up the AIoT devices, the types of AI algorithms used, and data collection constraints must be considered.
- Lifecycle management: Lifecycle management of an AIoT from design, development, deployment, use, and disposal process is required. Risk assessment is essential as the autonomous operation and function updates of a given AIoT device during its lifecycle can have a significant impact on safety.

The indicators below are selected according to the AIoT application service area, and differential weights are applied according to their importance so that they can be used in the trust index of the AIoT devices. The main factors that can be considered as indicators to quantify the trust level of AIoT are as follows:

- Data quality: The quality of the data set used in the AIoT has a critical impact on the training of ML algorithms and the performance of classification and decision-making. Feeding malicious data into the system could alter the behaviour of the AIoT. It should be possible to remove this data before it is used for training if the collected data is biased. Validation and testing of the data set should be done carefully before it is applied to the AIoT.
- Non-discrimination: Direct or indirect discrimination based on ethnicity, gender, sexual orientation, or age can lead to the exclusion of certain groups. Discrimination in AIoT can occur unintentionally due to data issues such as bias and incompleteness or design flaws in AI algorithms. Those who control AI algorithms may seek to achieve unfair or biased results, for example by deliberately manipulating data to exclude certain groups of people.

- Privacy: Digital records of human behaviour contain highly sensitive data such as gender, age, religion, sexual orientation, and political views and preferences. Privacy and data protection must be ensured at all stages of the AIoT lifecycle, including any data provided by the user, as well as any information generated about the user in their interactions with the AIoT.
- Robustness: AIoT devices must be robust and secure enough to handle errors or inconsistencies in the design, development, execution, deployment, and use phases, and to respond appropriately to erroneous results.
- Reproducibility: AIoT training and model-building conditions should be able to produce consistent results according to the input data in a given situation. Lack of reproducibility can lead to unintended discrimination in AIoT decisions.
- Accuracy: AIoT needs to ensure accuracy such as the ability to classify data into the correct categories or the ability to make correct predictions or decisions based on data or models.
- Security: AIoT may contain vulnerabilities that attackers can exploit. An attack on AIoT, such as hacking or malware can alter data and system behaviour, causing the system to make different decisions or shut down the system completely. Security management that can quickly remove and manage vulnerabilities in the AIoT as soon as they are discovered and prevent the infection of malicious code such as viruses, worms, and ransomware must be applied.
- Explainability: Explainability should be applied so that the mechanisms by which AIoT makes decisions can be interpreted, verified and reproduced.

Bibliography

[b-ITU-T Y.3172] Recommendation ITU-T Y.3172 (2019), *Architectural framework for machine learning in future networks including IMT-2020*.

[b-ITU-T Y.3179] Recommendation ITU-T Y.3179 (2021), *Architectural framework for machine learning model serving in future networks including IMT-2020*.

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ITU-T Y.4003] Recommendation ITU-T Y.4003 (2018), *Overview of smart manufacturing in the context of the industrial Internet of things*.

[b-ITU-T Y.4004] Recommendation ITU-T Y.4004 (2021), *Overview of smart oceans and seas, and requirements for their information and communication technology implementation*.

[b-ITU-T Y.4123] Recommendation ITU-T Y.4123 (2022), *Requirements and capability framework for smart shopping mall systems*.

[b-ITU-T Y.4209] Recommendation ITU-T Y.4209 (2020), *Requirements for interoperation of the smart port with the smart city*.

[b-ITU-T Y.4216] Recommendation ITU-T Y.4216 (2022), *Requirements of sensing and data collection system for city infrastructures*.

[b-ITU-T Y.4217] Recommendation ITU-T Y.4217 (2022), *Service requirements and capability framework for Internet of things-related crowdsourced systems*.

[b-ITU-T Y.4481] Recommendation ITU-T Y.4481 (2022), *Framework for data middle platform in Internet of things and smart sustainable cities*.

[b-ITU-T Y.4482] Recommendation ITU-T Y.4482 (2022), *Requirements and framework for smart livestock farming based on the Internet of things*.

[b-ITU-T Y.4484] Recommendation ITU-T Y.4484 (2022), *Framework to support web of objects ontology based semantic data interoperability of e-health service*.

[b-ITU-T Y.4601] Recommendation ITU-T Y.4601 (2023), *Requirements and capability framework of a digital twin for smart firefighting*.

[b-ITU-T Y.4602] Recommendation ITU-T Y.4602 (2023), *Data processing and management framework for IoT and smart cities and communities*.

[b-ISO/IEC JTC 1/SC 29] ISO/IEC JTC 1/SC 29 (1991), *Coding of audio, picture, multimedia and hypermedia information*.
<https://www.iso.org/committee/45316.html>

[b-ISO/IEC JTC 1/SC 42] ISO/IEC JTC 1/SC 42 (2017), *Artificial intelligence*.
<https://www.iso.org/committee/6794475.html>

[b-AIoT] *Artificial intelligence of things*, Wikipedia.
<https://en.wikipedia.org/wiki/Artificial_intelligence_of_things>

[b-tinyML] tinyML Foundation.
<https://www.tinyml.org>