TECHNICAL CODE

INTERNET OF THINGS -
HIGH LEVEL FUNCTIONAL ARCHITECTURE

Developed by

Registered by

Registered date:

6 May 2020

MCMC MTSFB TC G022:2020

Development of technical codes

The Communications and Multimedia Act 1998 ('the Act') provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
http://www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Malaysian Communications & Multimedia Commission (MCMC)
Off Persiaran Multimedia,
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
http://www.mtsfb.org.my

Contents

Page

Committee representation

This technical code was developed by the Internet of Things and Smart Sustainable Cities Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB) which consists of representatives from the following organisations:

BNetworks Sdn Bhd

Cisco Systems Malaysia

FAVORIOT Sdn Bhd

Huawei Technologies Co., Ltd.

Intel Corporation

Maxis Berhad

Telekom Malaysia Berhad

Telekom Research and Development Sdn Bhd

Universiti Putra Malaysia

webe digital sdn bhd

Foreword

This technical code for Internet of Things – High Level Functional Architecture ('this Technical Code') was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Internet of Things and Smart Sustainable Cities Working Group.

This Technical Code shall continue to be valid and effective until reviewed or cancelled.

INTERNET OF THINGS – HIGH LEVEL FUNCTIONAL ARCHITECTURE

0. Introduction

The Internet of Things (IoT) fulfil broad spectrum of unique requirements which are challenging to state using a single standard and technology hence heterogeneous standards and technologies would be required to create an end-to-end solution for different use case application domains. Developing IoT systems and solutions have several challenges as each industry vertical has different set of unique requirements which varies from functional to non-functional as well as operational perspectives. As an example, smart cities and smart factories have different complex set of deployment requirements covering computational, connectivity, security, environmental and regulatory parameters.

This Technical Code defines an open IoT functional architecture by considering the five elements of IoT namely computing, connectivity, security, manageability and analytics. All five elements are necessary to create a practical and deployment ready solution for use-cases such as smart cities. It is also recommended to adopt open standards and open source software which will grow the local eco-system without any legal implications of close and proprietary systems.

The purpose of having the five elements is to make a unification of standards by adopting and recommending an architecture which flourishes open ecosystem with innovation. The following are the goals for the high-level functional architecture:

a) to adopt available open standards for creating an inter-operable end to end systems;

b) to update the adoption of standards according to Malaysian context; and

c) to provide a baseline framework as part of IoT high level functional architecture.

1. Scope

This Technical Code specifies requirements for IoT high level functional architecture by considering Malaysian context for IoT solutions. It describes high level core systems which constructs the IoT high level functional architecture. This functional architecture can be used for vertical use cases such as smart cities and smart agriculture.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative reference (including any amendments) applies.

MCMC MTSFB TC G013, *Internet of Things (IoT) - Security Management*

3. Abbreviations

For the purpose of this Technical Code, the following abbreviations apply.

AES	Automated Enforcement Systems
AI	Artificial Intelligence
BLE	Bluetooth Low Energy

BT	Bluetooth
E2E	End-To-End
GPS	Global Positioning System
GPU	Graphics Processing Unit
GSM	Global System for Mobile Communications
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IIC	Industrial Internet Connectivity
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSO	Internet Protocol for Smart Objects
ISM	Industrial, Scientific and Medical
LoRa	Long Range
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
LWM2M	Lightweight Machine-to-Machine
MAN	Metropolitan Area Network
MCU	Microcontroller Unit
NB-IoT	Narrowband IoT
NETCONF	Network Configuration Protocol
NFC	Near Field Communication
OCF	Open Connectivity Foundation
OMA	Open Mobile Alliance
OS	Operating System
OTA	Over-The-Air
PAN	Personal Area Network
RFID	Radio Frequency Identification
RTOS	Real-Time Operating System
SHA	Secure Hash Algorithms
SNMP	Simple Network Management Protocol
SoC	System on Chip
TCP	Transmission Control Protocol
TLSv2	Transport Layer Security version 2
TPM	Trusted Platform Module
UNB	Ultra Narrow Band
WAN	Wide Area Network

WiFi	Wireless Fidelity
WISUN	Wireless Smart Utility Network

4. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.

4.1 Device

With regard to the IoT, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

4.2 Gateway

A unit in the IoT which interconnects the devices with the communication networks. It performs the necessary translation between the protocols used in the communication networks and those used by devices.

4.3 Interoperability

The ability of two or more systems or components to exchange data and use information. It can be further defined as the ability of objects or devices, whether they be sensors, computers or other everyday things, to connect with each other and communicate data in a form and format that can be understood and processed by other persons or entities and is agnostic as to the hardware or software on which the data is to be further processed and stored.

4.4 Internet of Things (IoT)

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 (ICT).

NOTES:

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.

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

3. Example such as Industrial Internet of Things (IIoT).

4.5 Internet of Things (IoT) connectivity

It is a medium for IoT devices to communicate with other components such as IoT middleware and other devices. The medium could be short range or long range, for static devices or mobile devices. Some of these mediums are Bluetooth (BT), Wireless Fidelity (WiFi), Long Range (LoRa), SigFox Ultra Narrow Band (UNB), Narrowband IoT (NB-IoT), 5G, etc.

4.6 Sensor

An electronic device that senses a physical condition or chemical compound and delivers an electronic signal proportional to the observed characteristic.

4.7 Smart home

Refers to the networking of household devices and systems through ICT. This way, processes within a household can be monitored and controlled automatically to optimise quality of life, costs, security and environmental impact.

5. High level functional architecture

A functional architecture defines a model which identifies the system functions and their interactions. There have been several IoT architectures defined by different organisations. The IoT functional architecture identifies five main elements as described in Figure 1 which shall be considered for creating IoT solutions. These five elements are also common building block for IoT architectures defined by different organisations. The adopted functional architecture is recommended to use open and interoperable subsystems that consists of vendor neutral specifications, wherever possible. This Technical Code will focus on computing, connectivity, security and manageability components.

There are various proposed conceptual architectures. It is difficult to generalise to a functional architecture which can state diversity of heterogeneous domains and solve the problems within these domains.

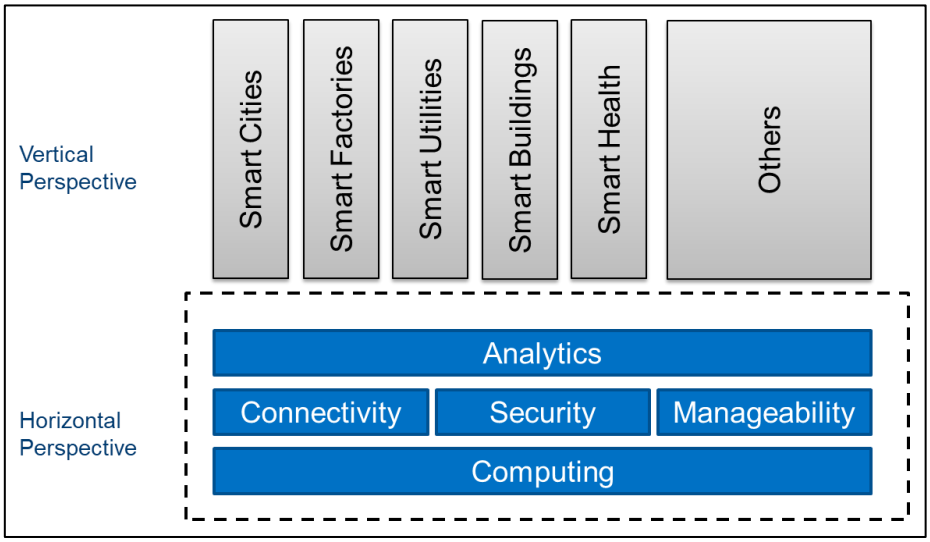

Figure 1. IoT functional architecture

5.1 Computing element

The computing element is an underlying fundamental component for a physical object to have computational capabilities. An IoT device with computational capabilities could be attached to physical object providing computing functionality.

The computational capabilities vary with the applications requirements. For example, in Agriculture, a sensing and actuating application may require as minimum as 16-bit microcontroller with the expectation of reading raw data from analogue sensors

Meanwhile computational expectations vary for high performance IoT applications such as real-time industrial robotics applications and Artificial Intelligence (AI) enabled cameras in the smart cities.

5.2 Connectivity element

An IoT connectivity is an essential element of IoT functional architecture. The heterogeneity of IoT connectivity technologies is a complex landscape which is designed to fulfil diverse set of connectivity requirements. The overall landscape for the IoT connectivity technologies is described in Figure 2.

The connectivity technologies are segmented into licensed and unlicensed technologies. These wide spectra of technologies are designed to fulfil specific purpose and building blocks for creating various types of use-cases. Primarily, the connectivity technology landscape is segmented into few categories below:

a) IoT edge nodes or devices;

b) edge gateway or edge computing system; and

c) cloud-based services.

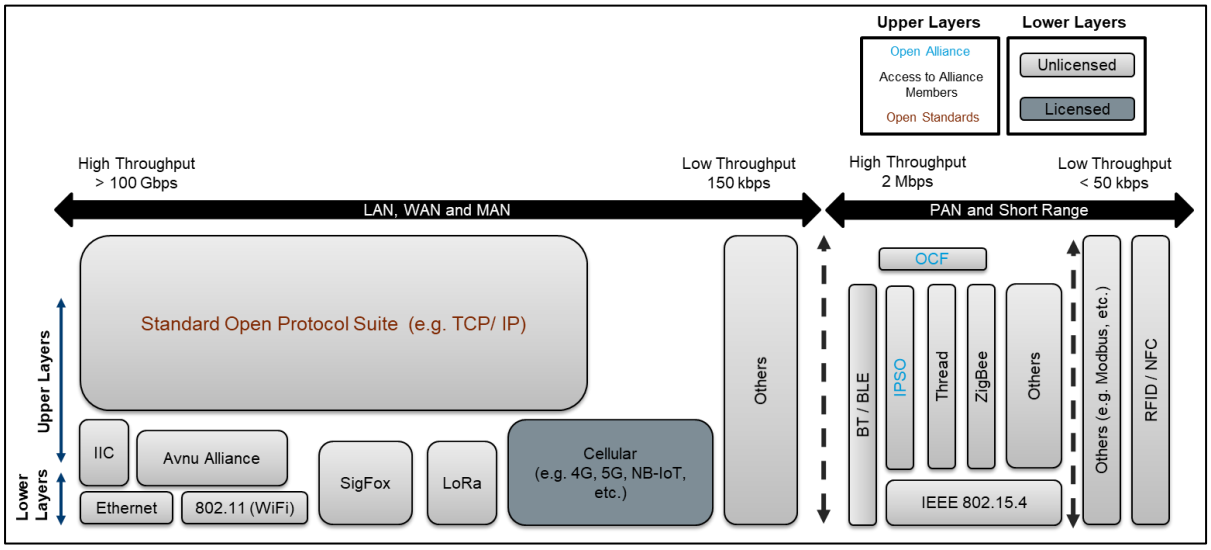

Figure 2. IoT connectivity standards and technologies

The functions for the IoT connectivity technologies are as in Table 1.

Table 1. IoT connectivity technology functions

No	Technologies	Functions
1	Radio Frequency Identification (RFID)	Designed for providing identification and tracking use cases with active and passive tagging technologies.
2	Personal Area Network (PAN)	Primarily designed with IEEE 802.15.4.
3	ZigBee and Thread	a) Focusing on smart home market with sensing and actuating applications with smart lights, thermostats and various ambient sensor devices over 2.4 GHz Industrial, Scientific and Medical (ISM) band. b) Can also be integrated with different types of devices such as smart speaker devices.
4	Wireless Smart Utility Network (WISUN)	Designed for utility network including smart energy and water meters network over sub-GHz bands such as 919 MHz.

Table 1. IoT connectivity technology functions *(continued)*

No	Technologies	Functions
5	Internet Protocol for Smart Objects (IPSO)	a) Providing a generic stack which can cater various types of applications including smart metering, smart locks and smart mining. Used in smart cities application.
6	BT	a) Based technologies for smart homes and wearable applications. Primarily used for audio streaming, file transfer and wearable technologies.
7	System on Chip (SoC)	Providing combination of integrated connectivity technology options with the core computing functionality such as Bluetooth Low Energy (BLE), WiFi and IEEE 802.15.4.
8	Wide Area Network (WAN)	Designed using diverse set of technologies to fulfil different market and technology needs
9	Local Area Network (LAN)	
10	Metropolitan Area Network (MAN)	
11	Low Power Wide Area Network (LPWAN)	a) Designed to use for various wide coverage use cases which requires low data rate with high latencies b) Key technologies in LPWAN are as follows: i) LoRa ii) SigFox UNB iii) Long Term Evolution (LTE) CAT1 iv) NB-IoT
12	LTE	Cellular based technologies for providing high throughput with long distance coverage
13	WiFi	Widely adopted for indoor and outdoor short-range coverage requirements with high throughput features

5.3 Security element

IoT security is a critical component of a functional architecture for deploying IoT technology. It has also been put in place as a mandatory national policy for various countries. The landscape consists of diverse set of requirements which needs to be stated for different application domains. The IoT security landscape for PAN, WAN and MAN is illustrated in Figure 3.

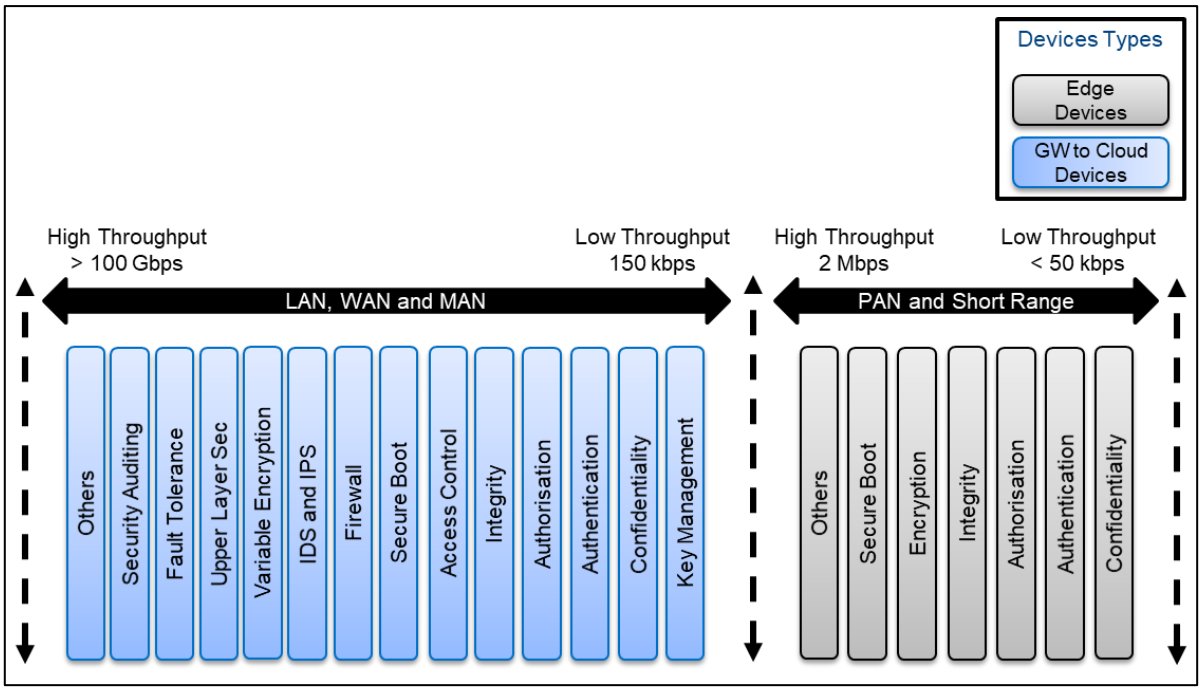

Figure 3. IoT security landscape

The IoT edge devices within the scope of is predominately low power constrained devices that are deployed in various use cases. These devices need to be deployed with set of security requirements such as authentication and confidentiality.

Constrained security sub-systems are designed for IoT edge devices with optimised hardware and software features due to the constrained nature of IoT edge devices. An IoT edge device is recommended to use the features wherever possible to avoid any malicious operations. The features are as follows:

a) confidentiality;

b) integrity; and

c) authentication.

The authorisation, secure boot and other features shall be supported based on the deployment requirements.

The IoT edge gateway and the cloud-based systems with the accessibility scope of WAN, LAN and MAN are recommended to support higher security requirements. Any compromise in the network deployment can jeopardise the IoT applications with financial loses.

There are various set of hardware and the software platforms which are currently supporting different security technologies. Below systems are recommended to support security requirement of IoT edge devices while conforming to security requirement of gateway, edge computing system and the cloud infrastructure:

a) Trusted Platform Module (TPM);

b) Automated Enforcement Systems (AES); and

c) Secure Hash Algorithms (SHA) hardware accelerators.

An overview of the IoT security management framework and the general requirements for security and privacy protection in the IoT ecosystem can be referred at MCMC MTSFB TC G013, *Internet of Things (IoT) - Security Management.*

5.4 Manageability element

The IoT manageability element is responsible for managing data, devices, network, software and other manageability aspect of IoT use case deployment. IoT technologies consist of various standards which are not interoperable. These standards also have its specification of managing the devices and features. The functional architecture recommends using open standards for manageability. Figure 4 describes the overall landscape for the IoT manageability.

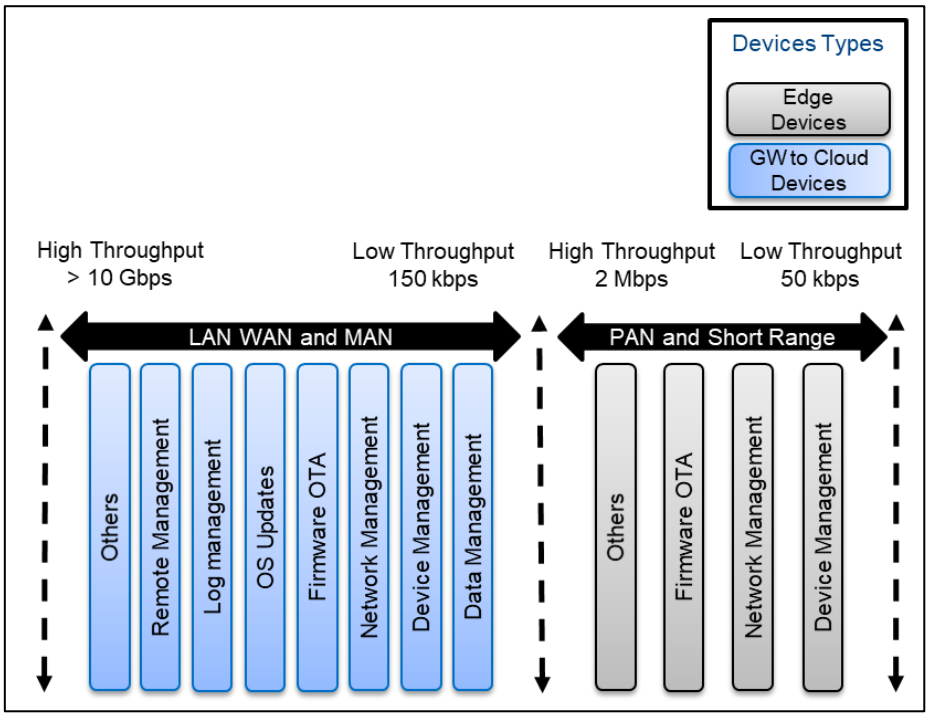

Figure 4. IoT manageability landscape

Generally, device management, networking management and firmware Over-The-Air (OTA) are recommended capabilities for short range PAN manageability. Whereas, in the LAN, WAN and MAN environment, wider capabilities need to be part of the deployment. The edge computing devices are recommended to support data, device, network and firmware OTA managements as these are crucial operations for deployments.

The IoT edge devices within the scope of PAN are constrained devices which shall support open but constrained friendly protocols. These protocols shall fulfil the device management, network management, firmware OTA update and other management related functionalities. There are open standards such as Open Mobile Alliance (OMA) Lightweight Machine-to-Machine (LWM2M) which can fulfil the requirements for IoT manageability. The IoT devices within the scope of WAN, LAN and MAN shall support open protocols such as Simple Network Management Protocol (SNMP), Network Configuration Protocol (NETCONF) etc. for fulfilling the requirements given in Figure 4.

5.5 Analytics element

An IoT analytics element is responsible for analysing the collected data over the time for making smart decisions. Data is collected using sensors from IoT edge devices or nodes and send either directly or through the IoT gateway to the cloud. Different use cases have different business problems and requirements which need to be consider while working on the analytical approaches.

It is recommended to use domain experts in understanding the collected data, as an example civil engineers for smart cities infrastructure. Usually, data preparation and modelling are performed in an engineering environment which is being trained using high computing resources such as Graphics Processing Units (GPUs). These models are validated with the testing data and evaluated in the actual deployment environment with specialise inferencing computing systems which consumes low power as compare to GPUs. A continues feedback methodology is essential for improving the analytical models. Data analytics can also be performed using various software tools that are available in the market.

6. End-To-End (E2E) IoT solution using functional architecture

The functional architecture consists of *n*-tier devices which comprises of different set of computational, communication, manageability and security technologies as illustrated in Figure 5. The source of the data comes from the IoT edge devices such as sensors and actuators. There are heterogeneous types of sensors available which can be applied for wide variety of applications such as temperature, smoke, humidity and camera sensors. There are various actuator devices which are applicable for different applications as follows but not limited to:

a) robotic arms;

b) environmental sensors;

c) motors; and

d) smart cameras.

Most of the IoT edge nodes or devices operate using specialise communication medium and protocol stack which confined these devices into their own technology centric network due to optimal deployment operational expectations. IoT devices having BT, LoRa and IEEE 802.15.4 are based on this category. Some IoT devices require IoT edge gateway device or computing system to communicate to the external networks and the Internet.

The IoT edge gateway is designed for consolidating and managing the IoT edge devices with the cloud. An IoT edge gateway can be deployed with high performance computing system for low latency use case requirements such as in industrial, automotive and smart city applications. These edge computing systems have multi-purpose functional and operational requirements such as managing multiple communication medium sessions, cryptographical and devices management operations and at the same time provide low latency analytical decisions.

An IoT edge computing system is also the extension of the cloud functional and operational features where cloud service provides offloading of some of the critical functional blocks to IoT edge computing gateway or system for low latency applications. As an example, IoT gateway can also be used for digital video recorder and consolidator which handles video streams from multiple cameras. In another scenario, the similar IoT gateway can manage hundreds of wireless sensor devices in the smart cities' scenario.

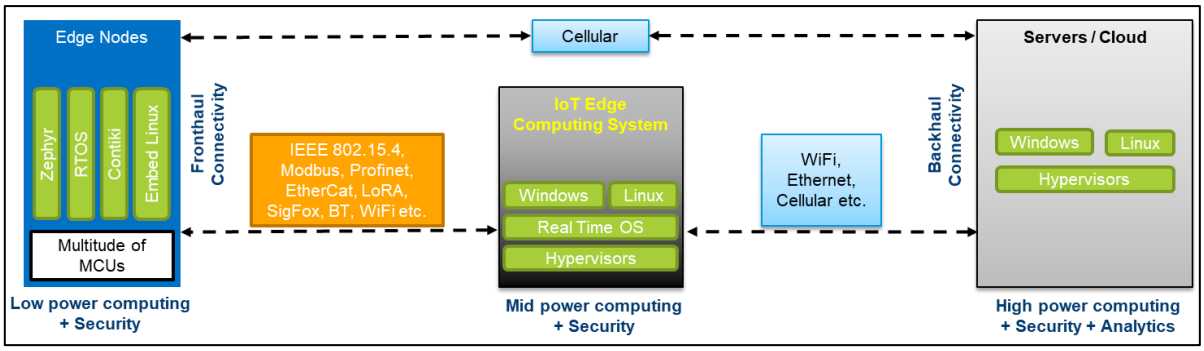

Figure 5. IoT end-to-end solutions

The cloud-based systems are the core backbone for data processing in IoT solutions which are typically used for various functional tasks including collection of data from IoT edge devices, analyse the data, and manage the devices as well as implementation of AI models on the dataset. This cloud-based system is also referred as platform or middleware systems.

The data need to be securely transferred using standardised mechanisms that are already available. These data and the heterogeneous IoT devices shall be managed efficiently. Once the data is successfully transferred to the specialised system, it will be further analysed using an analytic tool or system. These analytics systems use higher computing and memory resources for creating, training and deploying smart ambient solutions. These systems could reside on the cloud infrastructure, on the edge nodes network or a combination of both. The edge computing system shall be considered for making real-time lower latency decision-making processes in deployed IoT solutions.

7. Example of use cases using functional architecture

Use case solution provider can use this functional architecture to define the requirements for their IoT solutions. Two use case examples of using this functional architecture are given below.

7.1 IoT elderly care solution

IoT is changing the way we live, for better. It helps in improving certain aspects of work, decreases wastages and eventually provide a better environment to live. This can only be achieved if the IoT ecosystem is properly planned and deployed. Elderly care is one such vertical application. Table 2 shows an example of requirements for elderly care solution based on the functional architecture.

Table 2. Requirements for elderly care solution based on functional architecture

Requirements	Descriptions
Computing	a) Low power computing devices such as smartwatch with sensing of heart rate, pedometer, Global Positioning System (GPS) and blood pressure. b) High power computing is a server to process and analyse data transmitted by smartwatches or other sensing devices.
Connectivity	Sensors deploys within home can be connected using short range communication whereas devices like smartwatches require LoRa connectivity such as Global System for Mobile Communications (GSM), LoRA, SigFox or NB-IoT.
Security	Smartwatch to server and server to application must have secure data transmission such as using Transport Layer Security version 2 (TLSv2).

Table 2. Requirements for elderly care solution based on functional architecture *(continued)*

Requirements	Descriptions
Manageability	a) Some devices should be able to be updated regularly OTA (firmware OTA) b) Data management. System should be handling large number of distributed data streams and the data processing at the sensor should be efficient to avoid wastage of power that can extend the network lifetime.
Analytics	Data from various edge devices has to be analysed to provide current information and can be used for prediction of individuals.

7.2 Smart home

Most of the smart home products are standalone and usually only linked to user's smart phones. There will be no linkage between systems in the residential unit to their building management or security rooms. Those systems remain as conventional smart home products and a property developer will not be able to provide a more holistic connected service.

Smart home hubs/gateways shall be positioned as an enabler to link each home to the building management during an emergency for security, medical or duress. This will require a cloud based backed software integration and development of front-end application for the building management. Table 3 below shows an example of requirements for smart home based on the functional architecture.

Table 3. Requirements for smart home based on functional architecture

Requirements	Descriptions
Computing	a) Low power computing devices that can be installed are sensors to measure temperature, movement and to monitor energy usage. b) Mid power computing could be home gateway that aggregates data from various sensors and forward it to backend system for further processing. In some cases, the mid power computing device are capable to process data and provide necessary action c) High power computing devices are used to process and analyse the data stream
Connectivity	Connectivity varies depending on the devices used and most of the time the connectivity is short range. Some of the common connectivity standard used are WiFi, BLE, ZigBee, ZWave
Security	The use of strong credentials and data encryption are required. For example, door access system requires strong credentials with encrypted system.
Manageability	a) Some devices should be able to be updated regularly OTA (firmware OTA) b) Data management. System should be handling large number of distributed data streams and the data processing at the sensor should be efficient to avoid wastage of power that can extend the network lifetime. c) Some devices should be managed remotely such as surveillance system
Analytics	Analytics of data for smart home could be in many applications such as to analyse the energy usage pattern, to detect people movement or intrusion detection, to detect temperature in building and provide necessary action if required.

Bibliography

[1] ISO/IEC 20924*, Information technology - Internet of Things (IoT) - Vocabulary*

[2] ITU-T Y.4455, *Reference architecture for Internet of things networking capability exposure*

[3] IEEE, Computer Science and Information Systems (FedCSIS), *Service Modelling for the Internet of Things*

[4] IEEE, Future Internet of Things and Cloud (FiCloud), *Choosing Your IoT Programming Framework: Architectural Aspects*

[5] IEEE, P2413/D0.4.6, *IEEE Draft Standard for an Architectural Framework for the Internet of Things (IoT)*

[6] Personal Ubiquitous Computing, *Adding sense to the Internet of Things - An architecture framework for Smart Object systems*

[7] Wireless Networks, The Journal of Mobile Communication, Computation and Information, *IDRA: A flexible system architecture for next generation wireless sensor networks,* Wireless Networks

[8] 6th International Conference on Ubiquitous Information Management and Communication, Article 10, *Web-Based Wireless Sensor Networks: A Survey of Architectures and Applications*

[9] Internet-of-Things Architecture, *IoT-A Deliverable D1.5 - Final architectural reference model for the IoT* v3.0

[10] Internet-of-Things Architecture, *Introduction to the Architectural Reference Model for the Internet of Things*

[11] Internet-of-Things Architecture, *Concepts and Solutions for Privacy and Security in the Resolution Infrastructure*

[12] MCMC, *Regulatory Challenges of Internet of Things (IoT)*

Acknowledgements

Members of the Internet of Things (IoT) and Smart Sustainable Cities Working Group

Dr Gopinath Rao Sinniah (Chairman)	FAVORIOT Sdn Bhd
Mr Shariq Haseeb (Vice Chairman)	Telekom Research and Development Sdn Bhd
Mr Usman Sarwar (Draft Lead)	Intel Corporation
Mr Mohamad Norzamir Mat Taib/	Malaysian Technical Standards Forum Bhd
Ms Norkhadhra Nawawi (Secretariat)	
Mr Tharmaindran K.Gannasin	BNetworks Sdn Bhd
Mr Mukhriz Zakaria	Cisco Systems Malaysia
Ms Meloshini Rangala/	Huawei Technologies Co., Ltd.
Mr Muhamad Hazwan Halim/	
Mr Tan Kuan Thye	
Mr Arief Khalid/	Telekom Malaysia Berhad
Mr Mohd Zakir Hussin/	
Mr Thaib Mustafa	
Dr Qazi Mamoon	Telekom Research and Development Sdn Bhd
Ms Aina Awadz/	Maxis Berhad
Ms Chai Ming Ching/	
Mr Wong Chup Woh/	
Ms Yesotha Surendran	
Dr Aduwati Sali/	Universiti Putra Malaysia
Prof Borhanuddin Mohd Ali/	
Dr Mohd Fadlee A Rashid	
Mr Chan Wei Ming/	webe digital sdn bhd
Mr Rosli Abdullah/	
Mr Yeow Kok Chin	