Deployment Guideline
for Internet of Things in the University

VERSION 1.0

Contents

1 Document Control

1.1 Document Status

Document Name	Deployment Guidelines for Internet of Things in the University
Document Code	F-8
Author	Information Technology Services Office
Version Number	1.0
Document Status	~~Draft for Internal Review~~ / ~~Release for Consultation~~ / Approved
Date Approved	1 Nov 2019
Date of Next Review	1 Nov 2021
Superseded Version	N/A

1.2 Document Status and Review

Version Number	Published / Revision Date	Summary of Changes	Authored By	Approved By
1.0	1 Nov 2019	Published	ITS	ITS

2 Introduction

2.1 Purpose

The Internet of Things (IoT) is a rapidly evolving and expanding collection of diverse technologies that interact with the physical world. IoT technology combining the worlds of information technology (IT) and operational technology (OT). IoT devices often include sensors, microelectromechanical systems (MEMS), controllers, processors, memory and Wi-Fi/Communication along with other analogue and digital circuitry, all combined into space about a third of the size of a smartphone. IoT devices can provide edge computing functionality, data storage, and network connectivity which reduce the need for central processing load as well as contain the amount of traffic to backend, enabling new capabilities with much lower cost of ownership.

This guideline covers the various considerations for deploying IoT devices in the campus environment. Faculties / Departments should observe the suggested practice in sourcing and deploying IoT technology at campus.

- Edge IoT Devices
- Connectivity and communication
- Data Collection, Analysis and Actuation
- Cybersecurity and privacy risk consideration

3 Definitions and Conventions

3.1 Definitions

The following are the definition of the terms used in this guidelines.

Term	Definition
Advanced Encryption Standard (AES)	AES is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. It supersedes the Data Encryption Standard (DES) which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.
Advanced Message Queuing Protocol (AMQP)	AMQP is an open source published standard for asynchronous messaging by wire. It enables encrypted and interoperable messaging between organizations and applications. The protocol is used in client / server messaging and in IoT device management.
Constrained Application Protocol (CoAP)	CoAP is a protocol that specifies how low-power compute-constrained devices can operate in the Internet of Things (IoT). CoAP is designed to enable simple, constrained devices to join the IoT even through constrained networks with low bandwidth and low availability. The protocol is generally used for machine-to-machine (M2M) communication.
Data Distribution Service (DDS)	DDS is a middleware protocol and API standard for data-centric connectivity from the Object Management Group (OMG). It integrates the components of a system together, providing low-latency data connectivity, extreme reliability, and a scalable architecture that business and mission-critical Internet of Things (IoT) applications need.
Long Range Wide-Area Network (LoRaWAN)	LoRaWAN is a Low Power, Wide Area (LPWA) networking protocol developed by the LoRa Alliance, that wirelessly connects battery operated ‘things’ to the internet in regional, national or global networks, targeting key Internet of Things (IoT) requirements such as bi-directional communication, end-to-end security, mobility and localization services.
LoRa App Server	LoRa App Server is an open-source LoRaWAN application-server, part of the LoRa Server project. It is responsible for the device “inventory” part of a LoRaWAN infrastructure,

	handling of join-request and the handling and encryption of application payloads.
LoRa Gateway	LoRa Gateway is antenna that receive broadcasts from end devices and send data back to end devices.
LoRa Network Server	LoRa Network Server is a server that route messages from end devices to the right application, and back.
Low-Power Wide-Area Network (LPWAN)	LPWAN is a wireless wide area network technology that interconnects low-bandwidth, battery-powered devices with low bit rates over long ranges. It is created for machine-to-machine (M2M) and Internet of Things (IoT) networks, LPWANs operate at a lower cost with greater power efficiency than traditional mobile networks. They are also able to support a greater number of connected devices over a larger area.
Message Queuing Telemetry Transport (MQTT)	MQTT is a machine-to-machine (M2M) / Internet of Things (IoT) connectivity protocol. It was designed as an extremely lightweight publish-subscribe messaging transport. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.
MQTT Broker	An MQTT broker is a server that receives all messages from the clients and then routes the messages to the appropriate destination clients.
Narrowband Internet of Things (NB-IoT)	NB-IoT is another 3GPP proposal, but it does not operate in the LTE construct. It focuses specifically on indoor coverage, low cost, long battery life, and high connection density. It uses a subset of the LTE standard, but limits the bandwidth to a single narrow-band of 200kHz.
Open Web Application Security Project (OWASP)	OWASP is an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.
Operational Technology (OT)	OT is the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, etc.
Personal Area Network (PAN)	PAN is a computer network for interconnecting devices centered on an individual person's workspace. It provides data transmission among devices such as computers, smartphones, tablets and personal digital assistants.
Power over Ethernet (PoE)	PoE is a networking feature defined by the IEEE 802.3af and 802.3at standards. It lets Ethernet cables supply power to network devices over the existing data connection.

Security Information and Event Management (SIEM)	SIEM are software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.
Sigfox	Sigfox is a French global network operator founded in 2009 that builds wireless networks to connect low-power objects such as electricity meters and smartwatches, which need to be continuously on and emitting small amounts of data.
Tactics, Techniques, and Procedures (TTPs)	The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.
Telemetry Data	Telemetry data is the collection of measurements or other data at remote or inaccessible points and their automatic transmission to receiving equipment for monitoring.
Web Application Firewall (WAF)	WAF is an application firewall for HTTP applications. It applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection.
Wi-Fi Protected Access II (WPA2)	WPA2 is a security standard to secure computers connected to a Wi-Fi network.
ZigBee	Zigbee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection.

3.2 Conventions

The following is a list of conventions used in this document:

- **Shall** - the use of the word ‘shall’ indicates a mandatory requirement.
- **Should** - the use of the word ‘should’ indicates a requirement for good practice, which should be implemented whenever possible.
- **May** - the use of the word ‘may’ indicates a desirable requirement.

4 Internet of Things

4.1 What are Internet of Things devices?

As defined in the *A Model for the Internet of Things (IoT)* published by National Institute of Standards and Technology[i], IoT devices are devices which incorporate at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface (e.g. Ethernet, WiFi, Bluetooth, LPWAN…etc.), are not conventional IT devices for which the identification and implementation of cybersecurity features is already well understood. Many IoT devices provide computing functionality, data storage, and network connectivity for equipment that previously lacked these functions. In turn, these functions enable new efficiencies and technological capabilities for the equipment, such as remote access for monitoring, configuration, and troubleshooting. IoT devices could also enable us to analyse the data about the physical world and use the results to better inform decision making, alter the physical environment, and anticipate future events.

4.2 General IoT deployment

4.2.1 Three-Tier IoT Deployment Architecture

In general, an IoT deployment may consist of the following three tiers:

- Edge Tier

  The Edge Tier is a composite of a variety of edge devices, like sensors and actuators which produces electrical, optical, or digital data derived from a physical condition or event. Data produced from sensors is then electronically transformed, by another device, into information (output) that is useful in decision making performed by "intelligent" devices or individuals (people).

  These edge devices are connected with a variety of communication topologies such as Ethernet, Wifi, LPWAN…etc. depending on the network penetration requirements of specific IoT deployment.

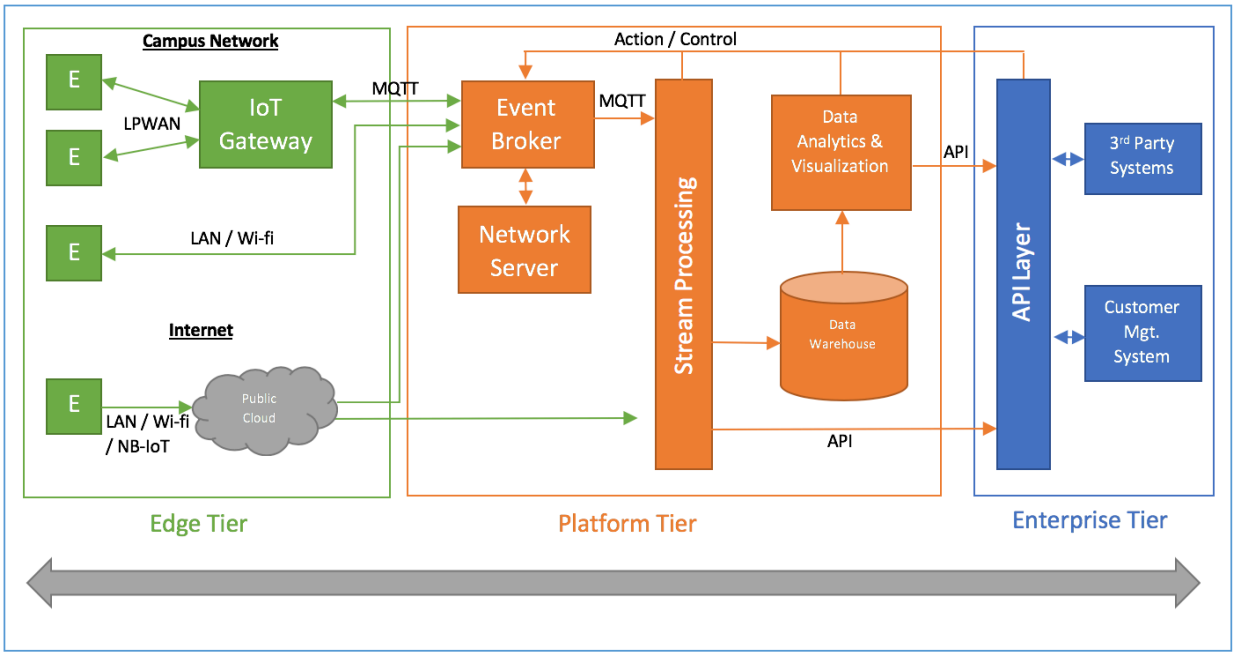
- Platform Tier

  The Platform layer presents an architecture for the centralized collection of IoT data, extracting insight from it and orchestration of the result action.

- Enterprise Tier

  To maximize the value from the insight extracted from the IoT data, organizations may integrate the IoT platform with enterprise systems so that the analysed IoT data could be used as a data feed to enrich the decision-making processes in the organization.

The following is a generic architectural diagram of the IoT deployment.



4.2.2 Type of IoT Products

In general, IoT products can be simply categorized into the following two types, consumer and enterprise grade products.

Consumer graded products

Manufacturers are creating an incredible variety and volume of Internet of Things (IoT) devices such as temperature and humidity sensors, which could be easily purchased from the Internet at a low cost. These consumer graded products could be easily deployed by simply installing the devices at the locations which you would like to collect the environmental data and providing it with a network connection such as Ethernet or WiFi. In general, the vendor may provide a cloud platform for analysing the data collected from the IoT devices.

However, the cloud platform of these consumer graded products may only provide simply data visualization function to the users to view the data collected but have no sophisticated data analysis or threshold alerting function to trigger follow up actions if anomaly condition is detected. Besides, these consumer products may not have a function for users to download the data on other IT systems for further analysis. Therefore, the value from the IoT data collected may be limited.

For users planning to deploy an IoT solution with business objectives to be achieved which requires in depth analysis with other environmental conditions collected from other IoT deployments or integration with backend IT systems, consumer graded products may not be a good choice for these cases.

Enterprise graded products

Enterprise grade IoT solution generally follow the three-tier IoT deployment architecture. The enterprise grade IoT solution could be deployed in the following models:

- **On-premise infrastructure**

All the architectural components in the three tiers (i.e. edge, platform and enterprise) are deployed on-premise and managed by the organization.

- **Hybrid cloud infrastructure**

  Under this deployment model, the platform tier components could be leveraged the infrastructure provided by various cloud service provider such as Amazon and Microsoft Azure. The beauty of this deployment model is the scalability of the data streaming infrastructure could easily be increased. However, it is important to consider the volume of the data streaming and also the privacy issues related to the data collected before adoption of this hybrid mode deployment.

5 Factors to be considered in an IoT deployment

A number of factors shall be considered in an IoT deployment in order to have business objectives to be achieved and the deployment does not pose any threats to the existing IT environment of the University.

5.1 Factors to be considered in selecting an IoT edge device

5.1.1 Selection checklist for IoT edge devices

It is not difficult to acquire an edge device at very low cost in the market. The following is a list of common sensors for different purposes[ii].

Sensor Type	Sensor Description	Examples
Position	A position sensor measures the position of an object; the position measurement can be either in absolute terms (absolute position sensor) or in relative terms (displacement sensor). Position sensors can be linear, angular, or multi-axis.	Potentiometer, inclinometer, proximity sensor
Occupancy and motion	Occupancy sensors detect the presence of people and animals in a surveillance area, while motion sensors detect movement of people and objects. The difference between the two is that occupancy sensors will generate a signal even when a person is stationary, while a motion sensor will not.	Electric eye, RADAR
Pressure	Pressure sensors are related to force sensors and measure the force applied by liquids or gases. Pressure is measured in terms of force per unit area.	Barometer, piezometer
Humidity	Humidity sensors detect humidity (amount of water vapour) in the air or a mass. Humidity levels can be measured in various ways: absolute humidity, relative humidity, mass ratio, and so on.	Hygrometer, humistor, soil moisture sensor
Light	Light sensors detect the presence of light (visible or invisible).	Infrared sensor, photodetector, flame detector
Temperature	Temperature sensors measure the amount of heat or cold that is present in a system. They can be broadly of two types: contact and non-contact. Contact temperature sensors need to be in physical contact with the object being sensed. Non-contact sensors do not need physical contact, as they measure temperature through convection and radiation.	Thermometer, calorimeter, temperature gauge
Acoustic	Acoustic sensors measure sound levels and convert that information into digital or analog data signals.	hydrophone

Source: Handbook of Modern Sensors: Physics, Designs, and Application, fourth edition

In order to determine which type of edge devices should be used for addressing the business objectives, users are recommended to review the following checklist to have a better understanding on their need:

Areas	**Checklist**	**Remark**
Data to be collected	1. What type of data will be sampled in the physical environment?	e.g. temperature, humidity
	2. What is the metadata for the sensory data?	e.g. Celsius for temperature
	3. How accurate the sampled data is required? 4. What is the noise tolerance level accepted for the application? 5. What level of resolution is required? What is the smallest incremental change in the input signal that the sensor requires to sense and report a change in the output signal?	For example, if you are going to deploy a sensor to detect the change of illuminance in a laboratory and the chemicals stored in laboratory is very sensitive to the change of the illuminance, you may need to have a highly accurate light sensor. To determine the accuracy of the sensor, users should understand the noise may be generated from the sensors or external environment and also the resolution of the data
Control actions	6. What control actions are required to be performed by the sensors?	Some sensors may allow users to define control actions but some may be predefined by vendors.
Deployment location, operating environment of the sensors and mobility	7. Where will the sensors to be deployed? How does the physical environment impact the sensors? Will the sensors be exposed to weather extremes (temperature, wind, moisture, vibration, etc.?) 8. Whether the sensors will be a fixed location or be mobile?	Location will definitely impact the selection of the sensors. For example, the sensors to be deployed outdoor, the sensors should support certain ingress protection standard. For details, please refer to the Annex A.
Projected growth rate and density of sensors	9. What is projected growth rate of the sensors to be deployed?	The growth rate of the edge devices will impact the sizing of the gateway and the need of data storage. The projected growth rate may also impact the message subscription costs, stream processing costs and cloud platform storage costs, if any. The density of sensors in a location may also impact the choice of local communication services as the

		interference may be introduced if the density of the sensors is very high.
Projected data volume	10. What is the projected volume of data generated by the edge device (e.g. bytes per second)?	This volume will directly impact endpoint storage and communication requirements. This may also affect the decision for determining whether a hybrid cloud model should be used. The projected volume of data could be estimated based on the frequency at which the data will be collected and the size of the individual data feed.
Integration with exiting operational technology and other IoT devices	11. Will the edge devices be integrated with existing operational technology? 12. Will the edge devices be connected with other IoT devices?	For example, you are going to integrate the CCTV with the building management system which only supports BACnet, you need to select the camera which support this protocol. Please refer to some examples of OT control protocols in Annex A.
Repeatability	13. Could the sensor consistently report the same response when subjected to the same input under constant environmental conditions?	Performing a proof-of-concept test and burn-in test could help users to determine whether the edge devices could consistently report the same response at same environmental condition.
Operation range	14. What is operation range of the edge device?	The band of input signals within which a sensor can perform accurately. Input signals beyond the range lead to inaccurate output signals and potential damage to sensors. The operation range may also affect the location the sensors to be installed.

By going through this checklist, users should have a better understanding on their need and hence they could select the appropriate edge devices accordingly.

5.1.2 Other factors to be considered

In addition to the factors mentioned in the checklist, users should consider the following aspects when selecting an edge device:

Power sources

When selecting an edge device, it is important to consider how the devices are powered. Edge devices are mainly powered through AC power source, power over ethernet (PoE) or batteries. These power sources may have its advantages and disadvantages:

Type of power source	**Advantages**	**Disadvantages**	**Situation of deployment**
AC power source	AC power source is relatively stable	The cost for installation power socket is high. As the device has to be attached a power socket, it limits the deployment location.	IoT devices with high demand of power such as the ones with strong computation power
Power over Ethernet	Plug-and-play technology that converges power and data in a single cable between the switch and the powered device (PD), eliminating the need for expensive electrical wiring Installation and operation safety – no high voltage work is required	The cost of PoE network switch is higher. As the devices need to gain power from a wired network connection, the mobility of the device is lower.	IoT devices could be fixed at a location
Battery	The mobility of the IoT device is increased	The capability of IoT device may be limited due to the low power availability	For location where physical access is limited

Interoperability

Most of edge devices currently in operation are proprietary and are designed for specific applications. This leads to interoperability issues in heterogeneous sensor systems related to communication, data exchange, storage, data security, and scalability.

Therefore, users should try to deploy the edge devices which support open standards to increase the interoperability of the devices.

Security vs. Usability

Due to various limitations such as lower processing power, memory capacity, and power availability at the sensor level, lightweight communications are preferable. For example, Constrained Application Protocol (CoAP) is an open-source protocol that transfers data packets in a format that is lighter than that of other protocols such as Hypertext Transfer Protocol (HTTP). However, while CoAP is well suited for energy-constrained sensor systems, it does not come with in-built security features, and additional protocols are needed to secure intercommunication between sensors and platform components.

Therefore, when users select edge devices, it is important to understand the data to be collected so that the corresponding data sensitivity could be determined in order to identify the necessary security protection is required. With this information, we could apply the appropriate security protection on the IoT deployment. Otherwise, a lot of handy and efficient edge devices would be ruled out due to the limited security features are provided on the devices.

Detailed security and privacy consideration on IoT deployment will be discussed in later section of this guide.

5.1.3 Requirements on device management capabilities on IoT edge devices

Device management is one of key aspects that users should consider when deploying IoT devices. It is because the IoT devices could be distributed across the campus and at some locations which it is hard for users to access such as elevator shaft and an effective device management could help to manage the devices in the field. When selecting an IoT device, users should ensure the devices are equipped with the following device management capabilities:

Device identification

The IoT device shall have a way to identify itself, such as a serial number and/or unique address used when connecting to network. To ease the identification, it is recommended to observe the following naming convention for the IoT devices attached to the campus network, wherever it is feasible:

[Type of device].[Dept].[Location].[Measurement]

	Description	Example
[Type of device]	This field indicates the type of the device. The device can be either a sensor or gateway.	S – Sensor G – Gateway
[Dept]	This field indicates which department captures the telemetry data	Department abbreviation e.g. ITS
[Location]	This field indicates where the device is deployed. If possible, please indicate the room number.	GH202
[Measurement]	This field indicates what kind of telemetry data is being captured	Temperature, humidity…etc.

For example, a sensor is deployed in Room ZS501e by ITS for measuring the temperature. Its name will be as follows:

S.ITS.ZS501E.TEMPERATURE

Device Configuration

To ease the management and configuration, the IoT device should provide a channel for the administrators to update the software and firmware configuration. It is preferred that IoT device should support remote configuration and software upgrade. It is reminded to change the default password of the device before deployment.

When sourcing an IoT devices to collect telemetry data in the campus, it is recommended to make sure it is feasible to configure the edge devices where to send the collected data to. Otherwise, the IoT devices could only work with proprietary platform provided by the solution providers and it will limit the usability of the collected data. Furthermore, the security of the proprietary platform for capturing the telemetry data should be well evaluated as security flaw in the platform could lead to data breach incident and cause impact to the University.

Software and Firmware Update

The software and firmware of the IoT device should be updatable using a secure and configurable mechanism. For example, some IoT devices receive automatic updates from the manufacturer, requiring little to no work from the user.

5.2 Considerations for networking design for IoT deployment

5.2.1 How does IoT edge device communicate with the other components?

In the three-tier architectural design of IoT deployment, the IoT edge devices are responsible for converting the physical conditions into data and transport it back to the other components in the platform tier for the further analysis.

The following are the common communication technologies that are frequently used for the communication between IoT edge devices and components in platform tiers or even components in the enterprise tiers:

- Personal Area Network (PAN) – e.g. Bluetooth Smart
- Local Area Network (LAN) - e.g. Ethernet or WiFi
- Low Power Wide Area Network (LPWAN) – e.g. LoRaWAN, Sigfox, NB-IoT and ZigBee

To determine which communication technologies to be used in the IoT deployment, the following aspects should be considered:

- Communication patterns of the IoT edge devices
- Throughput and range requirement
- Impact to existing IT infrastructure

Communication patterns

Users are advised to review the selection checklist for the IoT devices to understand the requirements on the IoT solution. The findings from the checklist could be served as an input to determine which

communication technology should be used for the IoT deployment. In particular, the following information is used:

- Deployment location, operating environment of the sensors and mobility
- Projected growth rate and density of sensors
- Projected data volume

Areas	**How could this information help to determine the communication technology?**	**Example**
Deployment location, operating environment of the sensors	The deployment location of the sensors could help to identify whether the coverage of communication technology is good enough to cover the planned deployment areas in the campus.	For example, users are planning to deploy air quality sensors in the toilets. In this case, WiFi is not a good communication technology to be used as there is no WiFi coverage in the toilets in the campus.
Mobility of IoT devices	This information could help to determine whether a fixed LAN connection should be used for the deployment.	For example, an IoT device is going to be installed on a drone/vehicle, it is not practical to use an Ethernet connection for the communication. As the drone / vehicle may be moving around the campus, the communication technologies to be used could either be WiFi or LPWAN.
Projected growth rate, density of sensors and data volume	The figures could help to provide a forecast of the number of data messages generated from the IoT devices. The projected figures could help to determine whether it is cost effective to adopt public communication services.	As some LPWAN communication solutions, such as public LoRAWAN service, sigfox and NB-IoT, charge users by the number of messages sent.

Throughput and range requirement

Users should understand the throughput requirement of the IoT deployment and also the areas to be covered in the deployment. It is because individual communication technology has its limitation on data throughput and range coverage.

The following table provides a summary of the data rate and range of common IoT communication technologies:

Technology	Frequency	Data Rate	Range	Power Usage	Cost
2G/3G	Cellular Bands	10 Mbps	Several Miles	High	High
Bluetooth/BLE	2.4Ghz	1, 2, 3 Mbps	~300 feet	Low	Low
802.15.4	subGhz, 2.4GHz	40, 250 kbps	> 100 square miles	Low	Low
LoRa	subGhz	< 50 kbps	1-3 miles	Low	Medium
LTE Cat 0/1	Cellular Bands	1-10 Mbps	Several Miles	Medium	High
NB-IoT	Cellular Bands	0.1-1 Mbps	Several Miles	Medium	High
SigFox	subGhz	< 1 kbps	Several Miles	Low	Medium
Weightless	subGhz	0.1-24 Mbps	Several Miles	Low	Low
Wi-Fi	subGhz, 2.4Ghz, 5Ghz	0.1-54 Mbps	< 300 feet	Medium	Low
WirelessHART	2.4Ghz	250 kbps	~300 feet	Medium	Medium
ZigBee	2.4Ghz	250 kbps	~300 feet	Low	Medium
Z-Wave	subGhz	40 kbps	~100 feet	Low	Medium

Impact to the existing IT infrastructure

Some LPWAN technologies are using same frequency band as the WiFi network deployed in the campus (e.g. PolyUWLAN and eduroam). Deploying these LPWAN technologies in the campus without due care may have interference to the WiFi services and cause interruption to the services.

A detailed comparison between the common used wireless technologies for IoT deployment is provided in Annex B.

Recommendation

In view of the potential impact to the existing IT infrastructure, users are recommended to consult Information Technology Services Office if there is a need to deploy these wireless technologies in the campus. Besides, ITS may have already built a common infrastructure for these LPWAN technologies so that the users leverage these infrastructures without additional capital investment.

5.2.2 Resilience of emerging LPWAN technologies

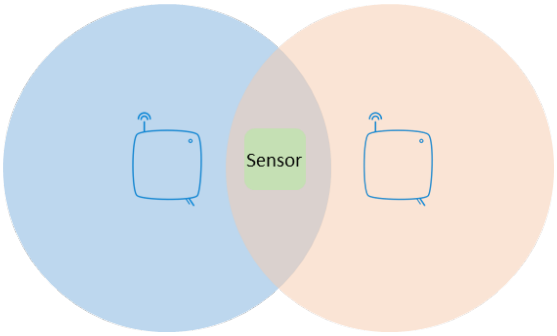
During the network topology design for the campus network infrastructure i.e. wired ethernet network and WiFi network, the resilience aspects have already been considered and implemented to ensure the availability of the network infrastructure service reaches 99.8% uptime.

Similarly, it is important to consider resilience aspects when deploying a LPWAN infrastructure. The following are some deployment design practices which could uplift the availability of the LPWAN infrastructure.

LoRaWAN infrastructure

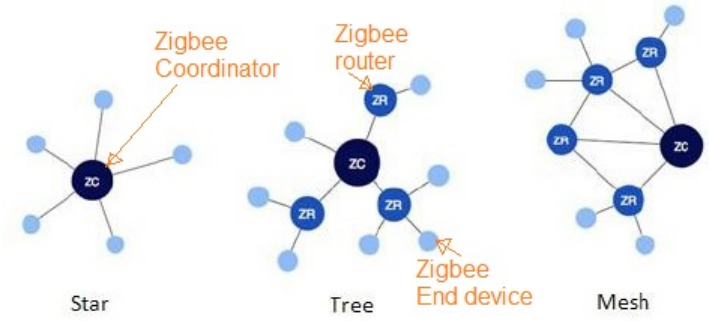
Resilience is well considered in the LoRaWAN network. When messages are transmitted over the LoRaWAN network by an end devices, it is received by all LoRa base stations that are in range. This

capability enhances the resilience of the network, improving the number of messages that are successfully received. Although having multiple LoRa base stations in an area increases the deployment capital expenditure, it does improve service resilience. Therefore, it is recommended to consider using LoRaWAN as the long-range communication protocol for IoT deployment with wide range area coverage requirements.



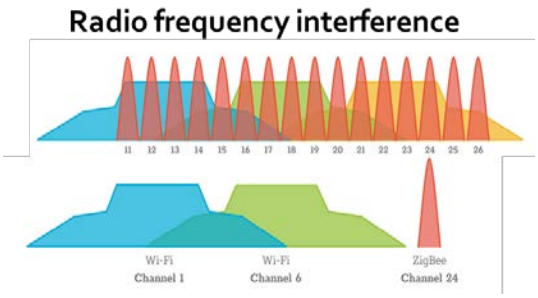
Zigbee infrastructure

Zigbee is another LPWAN technology widely used in IoT deployment. As shown in the figures below, all end nodes in a Zigbee infrastructure connect to a network connector which is either a coordinator or router. In case, the connector fails, it is required to replace the faulty connector in order to resume the data transmission in the network.



Zigbee technology supports the mesh network topology which allows sensors to connect each other to provide the network paths to the network coordinator. Therefore, it is important to ensure individual sensor connects to two or more nodes so that they have alternative network path to reach a network connector.

As Zigbee is using the same frequency band as PolyUWLAN WiFi service, it is not recommended to use Zigbee for the device connection if wi-fi service is available around the location. If it is unavoidable to use Zigbee as the communication network, ITS has to be informed to perform channel planning.



When deploying ZigBee and WiFi networks in the same environment, channel planning for peaceful coexistence is key. ZigBee channel 26 is usually relatively unaffected by WiFi, but many ZigBee devices do not support it.

A number of network design principles need to be considered in a deployment of LPWAN infrastructure. Therefore, users are highly recommended to consult ITS if they have business need to build an LPWAN infrastructure.

5.3 Consideration for data collection and analysis in IoT deployment

5.3.1 Communication protocols used in IoT deployment

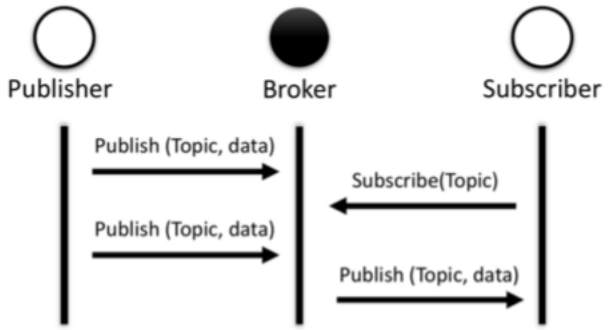
Two interaction models, i.e. request-reply and publish-subscribe, are commonly used in IoT deployment.

Request-reply communication model

Request-reply communication model is one of the most basic communication paradigms. It represents a message exchange pattern especially common in client/server architecture. It allows a client to request information form a seer that receives the request message, processes it and returns a response message. This kind of information is usually managed and exchanged centrally. The two most known communication protocols based on the request/reply model are Representational State Transfer HTTP (REST HTTP) and Constrained Application Protocol (CoAP).

Publish-subscribe communication model

Publish-subscribe communication model is an alternative to the traditional request/reply model. In this model, there are three parties i.e. publisher, subscriber and a broker as shown in figure below.



The client with a role a subscriber does not have to request information from the server. Instead of the request, the subscriber interested in receiving messages will subscribe to particular events (topics) within the system. The client subscribes to the broker, the central point in this architecture, responsible for filtering all incoming messages and routing them accordingly between publishers and subscribers. The third party is the publisher that serves as the information provider. When an event about a certain topic occurs, it publishes it to the broker who sends the data on the requested topic to the subscriber. For these reasons, publish-subscribe interaction model can be described as an event-based architecture. This model is interesting for the applications of IoT due to its ability to provide scalability and simplify interconnections between different devices, by supporting dynamic, many-to-many and asynchronous communication. The most known communication protocols based on publish/subscribe model are MQTT, AMQP and DDS.

Comparison between these two communication models

Comparing the two communication models, i.e., request/reply and publish/subscribe, it is observed that the publish/subscribe model has many benefits:

- publishers and subscribers do not need to know about the existence of each other;
- one subscriber can receive information from many different publishers and one publisher can send data to many different subscribers (many-to-many communication is supported);
- publisher and subscriber do not need to be active at the same time to exchange information, because the broker (working as a sort of queuing system) can store messages for clients that are not currently connected.
- There are many standardized messaging protocols currently implementing a publish/subscribe interaction model, most notably MQTT, AMQP and DDS.

However, request-reply model also has some advantages. In cases where the capacity of the server side for processing multiple client requests is not an issue it makes more sense to use already proven and reliable request/reply interactions. So the choice of the model depends on the application scenario for which it will be used.

Comparison between communication protocols

The following is a summary of the comparison between the protocols.

Protocol	**Model**	**Standard**	**Transport**	**QoS**	**Security**	**Developer's Choice**
REST HTTP	Request/Reply	IETF	TCP	-	TLS / SSL	✓
MQTT	Publish/Subscribe	OASIS	TCP	3 levels[1]	TLS / SSL	✓
CoAP	Request/Reply	IETF	UDP	Limited	DTLS	

[1] 3 different levels quality of service 0, 1 and 2 (QoS):

- At most once (0) - the message is sent only once and the client and broker take no additional steps to acknowledge delivery (fire and forget).
- At least once (1) - the message is re-tried by the sender multiple times until acknowledgement is received (acknowledged delivery).
- Exactly once (2) - the sender and receiver engage in a two-level handshake to ensure only one copy of the message is received (assured delivery).

AMQP	Publish/Subscribe	OASIS	TCP	3 levels	TLS / SSL	
DDS	Publish/Subscribe	OMG	TCP / UDP	Extensive	TLS / DTLS	
XMPP	Both	IETF	TCP	-	TLS / SSL	
HTTP/2.0	Both	IETF	TCP	-	TLS / SSL	

What is the preference of the IoT developers?

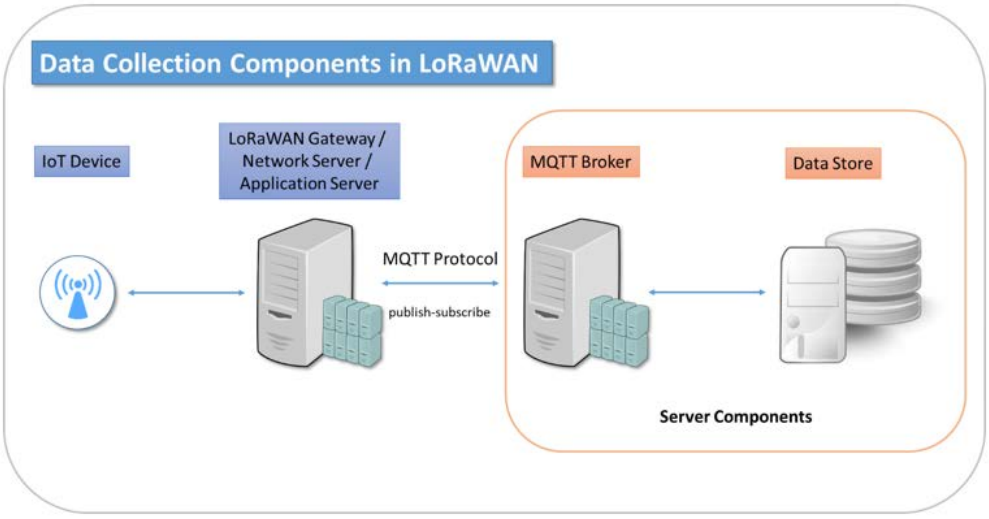
According to a collaborative survey by Eclipse IoT Working Group, IEEE, Agile-IoT EU and the IoT Council, MQTT and REST HTTP are the most used and adopted protocols by IoT developers. The reason for this is that MQTT and REST HTTP are currently comparably more mature and more stable IoT standards than other protocols. These two protocols also include many well documented and successful implementations and online resources.

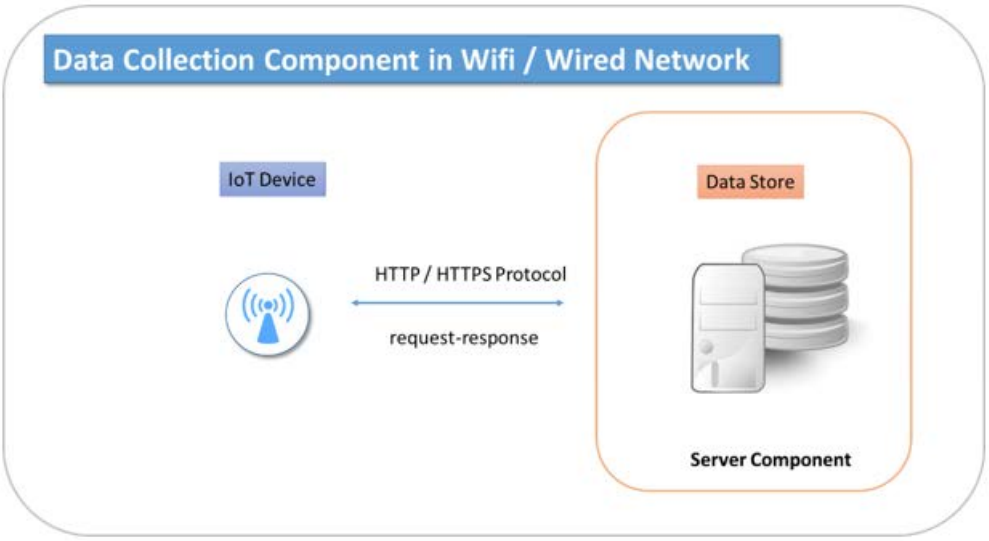
Recommendation for Communication Protocols

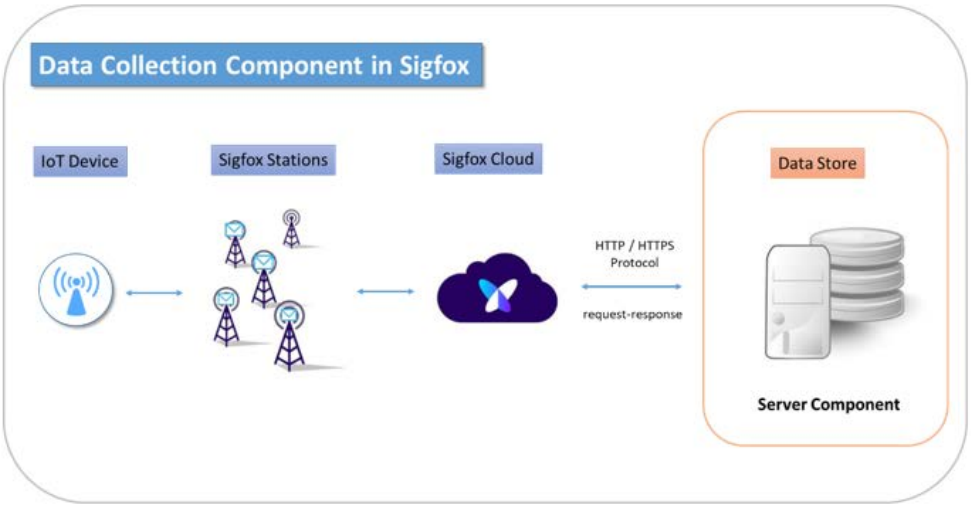
In view of its simplicity and lightweight, users should consider to use MQTT v3.1 as the communication protocol for the resource constrained devices and for non-ideal network connectivity conditions, such as with low bandwidth and high latency. However, since it was designed to be as lightweight, MQTT does not provide encryption so the data is transmitted as plain-text. Therefore, **users are recommended to use MQTT for the transfer of non-sensitive data.**

In the parts of the system where the constrained communication and battery consumption are not an issue, such in some fog and most cloud computing systems, RESTful HTTP is a straightforward choice.

The following are some sample use cases of the two communication protocols.







5.3.2 Message Broker

As mentioned previously, it is necessary to have a message broker for publish/subscribe communication model. The broker is primarily responsible for receiving all messages, filtering the messages, decide who is interested in them and then publishing the messages to all subscribed clients. The broker is the server that handles the data transmission between the clients. The broker also holds the sessions of all persisted clients, including subscriptions and missed messages. The broker is also responsible for the authentication and authorization of clients.

It is recommended that the message broker should be equipped with the following basic capabilities:

- **Messaging, event-driven and publish/subscribe communication protocols** – the broker should offer queuing, messaging, and event notification services, allowing the implementation of asynchronous and distributed architectures.
- **MQTT protocol support** – the broker shall be able to accept MQTT messages and route them to queues, insert them into the database or pass them to event handlers based on context included in the message payload itself. The broker should support the latest version of MQTT i.e. version 3.1.

It is also necessary to consider which authentication mechanism should be taken for authentication between IoT devices and MQTT Message Broker.

In order for an IoT edge device to make a connection with a MQTT Message Broker, it must initiate a request to connect. The MQTT protocol specifies that a client must report a client id when requesting a connection. **Therefore, it is recommended individual IoT edge device shall have a unique client identifier such as unique identifier (UUID) or a MAC address of the device.**

To authenticate the edge device with broker, a username and password shall be defined and set on the edge device and broker. In addition to authentication with username and password, MQTT protocol allows a device to authenticate with a X.509 certificate. Using X.509 certificate for authentication could also bring an additional benefit to the communication between the edge device and broker. In order for edge device to utilize X.509 authentication, Transport Layer Security is required to be implemented to secure the communication channel. Therefore, it could also address the issue that the telemetry data is transferred in plain-text. **Wherever possible, X.509 certificate should be considered as an option for the device authentication.**

ITS is implementing an IoT infrastructure which message brokers will be deployed to support publish/subscribe based communication model. Users who are planning to setup a message broker for their IoT deployment may consider to leverage this shared infrastructure which could help to expedite the adoption of IoT technology.

In the publish/subscribe based communication model, the data are grouped into topics which form a logical boundary for the data. The following naming convention for the topic is recommended to be adopted:

[Dept].[Purpose].[Measurement].[Access]

	Description	Example
[Dept]	This field indicates which department captures the telemetry data	Department abbreviation e.g. ITS
[Purpose]	This field indicates what the purpose the telemetry data is collected for. There are three categories: 1. Operation (OPS) – this category indicates that the data is used for administrative function of the University. For example, monitoring the temperature and humidity level in general teaching room for detecting the potential failure of the air conditioner is categorized under "Operation" 2. Research (RES) – this category indicates the telemetry data is captured for research purpose. 3. Teaching / Learning (TL) – this category indicates the data is	OPS or RES or TL

	captured for teaching and learning purpose.	
[Measurement]	This field indicates what kind of telemetry data is being captured	Temperature, humidity…etc.
Access	This field indicates the accessibility of the data. It can be open to all departments in the University or just restricted to specific department.	Public / Restricted

All topic name is case sensitive so we will use capital letters only. For example, FMO.OPS.TEMPERATURE.PUBLIC and LSGI.RES.VIBRATION.RESTRICTED. The maximum length of the topic name is 255 characters.

Therefore, users shall ensure the attributes of the payload sent from the edge devices could be modified so that the topic name standard could be observed. As some IoT devices may encode the payload with their proprietary algorithm, when selecting the edge device for their project, users shall ensure the supplier of the edge device would share the payload decoding mechanism with the University.

5.3.3 Data Management

Data fuels the entire IoT deployment value proposition. As a result, management of data itself, data quality and metadata is foundational. The data management platform should have the ability not only to ingest data, but to normalize, scrub and label data. The following are some criteria on the platform for users' considerations:

Areas	**Requirement**
Accessible data catalog	Provides a data catalog with metadata object definitions that must be accessible by the analytics and applications developed on the platform. The data catalog must be user-extensible to support IoT solution-specific metadata requirements.
Data ingest pipeline	Provides a linked set of capabilities that permit quality checks, normalization, scrubbing and tagging/labelling of the data. This task can either be performed at streaming (the time of data injection) or as a scheduled batch process.
Individual metadata object reuse	Individual metadata objects including dimensions, measures, calculations and parameters are published once and shared across applications, reports dashboards and analytics tools.
Bulk data import/export	Migrating large amounts of data between IoT applications, platform instances, enterprise data stores, third parties or cold storage is required. IoT platform must support tools for importing and exporting bulk data into and out of the environment. There are a wide range of possible data formats; as a result, this requirement will be considered fulfilled if the platform can demonstrate support

	for two formats of the platform supplier's choosing. Example formats that could be used to fulfil these requirements include (but are not limited to): • Comma-separated values (CSV) • mysqldump for MySQL • pg_dump and pg_restore for PostgreSQL • SQL Server Management Studio (SSMS) for Microsoft SQL Server

5.3.4 Data visualization & analysis

In order to turn IoT data into business value and insight, data analytics must be leveraged. How to choose a suitable analytic system for department use is another important task for building up IoT infrastructure. There are many different data analytic system on the market. No matter it is an open-source or paid application, it is ideal to support below capabilities:

- Dashboards and visualization.
- Role-based access control.
- Detection alert.
- Machine Learning algorithms
- Server cluster for high availability
- Scale up existing cluster if necessary
- Easy to learn and adopt

The shared IoT infrastructure built by ITS will be equipped with data visualization tool and also allow users to trigger alert notification if the captured data indicates an exception is detected based on a pre-defined threshold.

5.4 Security and privacy consideration in IoT deployment

5.4.1 Security risks and challenges associated with IoT deployment

By nature, an IoT deployment is often comprised of large number and variety of edge devices. In general, many IoT edge devices have only limited processing resources. Security features commonly found in conventional computers such as anti-malware software and firewall can hardly be found in an IoT edge device.

Due to all these characteristics of IoT, any IoT deployment might form a weak link in the campus network and impose significant threats to University if the devices are deployed without IT security awareness or planning specific to IoT technologies. According to OWASP Internet of Things Top 10 2018, the following is the list of common IoT risks:

	Risks	**Description**

1	Weak, guessable, or hardcoded passwords	Use of easily brute forced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed system.
2	Insecure Network Services	Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control.
3	Insecure Ecosystem Interfaces	Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.
4	Lack of Secure Update Mechanism	Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.
5	Use of insecure or outdated components	Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operation system platforms, and the use of third-party software of hardware components from a compromised supply chain.
6	Insufficient Privacy Protection	User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.
7	Insecure data transfer and storage	Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.
8	Lack of device management	Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.
9	Insecure Default Settings	Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operations from modifying configurations.
10	Lack of Physical Hardening	Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

5.4.2 Security measures for addressing the potential risks posed by IoT deployment

The following security controls should be incorporated in the planning of the IoT deployment to mitigate the potential risk associated with IoT deployment:

Area	**Security measure**	**Description**	**When to Consider (before purchase/ Self built / during deployment/ operation)**	**Applicable to Components (Edge Devices/Network Infra/Servers/User Devices)**
Application security	Deploy Web Application Firewalls	Protect web applications and API services by deploying web application firewalls (WAFs) that inspect incoming traffic for common web attacks.	during deployment	Servers
Asset management	Purge the Personal Data Before Disposal/ Resale	The edge devices may have stored personal data. Before disposing or reselling an IoT device, make sure all user account information and other personal data stored in the device are erased.	operation	Edge Devices
	Configurable firmware and security setting	The edge devices should have the capabilities as below: • To change the device's software and firmware configuration settings • To restrict configuration changes to authorized entities only • To restore the device to a secure default configuration defined by an authorized entity • To enable, disable, and adjust thresholds for any ability the device might have to lock or disable an account or to delay additional authentication attempts after too many failed authentication attempts	before purchase/self -built	Edge Devices
Asset Management	Maintain detailed IoT device inventory	Maintain a current, accurate inventory for every edge device throughout its lifecycle. The inventory shall contain information at least, hardware address, device name and asset owner.	during deployment/ operation	Edge Devices

Asset Management	Device Identification	The IoT device should have a way to identify itself, such as by serial number and/or a unique address used when connecting to networks.	before purchase/self-built	Edge Devices
Audit Trail	Monitor cybersecurity events	The edge devices should have the capabilities as below: • To log cybersecurity events across the device's software and firmware • To record sufficient details for each event to facilitate an authorized entity examining the log and determining what happened • To restrict access to the logs so only authorized entities can view them • To prevent any entities (authorized or unauthorized) from editing the logs • To make the logs available to a logging service on another device, such as a log server	before purchase/self-built	Edge Devices/Servers
Authentication	Change default passwords	Change all default passwords, especially for those accounts having administrative privilege.	during deployment	Edge Devices
Authentication	Set strong password	A complex password should be set which does not comprise the personal data (such as name, date of birth etc.)	during deployment	Edge Devices/Servers
Authentication	Prohibit hard-coded passwords	Verify the product does not contain an authentication mechanism that checks for a hard-coded password. A hard-coded password is the same for each installation of the product, and it usually cannot be changed or disabled even by the system administrator without modifying the program. Anybody with knowledge of this password can access not only a device, but also all installations in the environment.	before purchase/self-built	Edge Devices
Data Privacy	Collect only necessary personal identifiable information	Verify that the IoT device collect only necessary but not excessive personal data. Personal data should be collected just for a purpose directly related to a function/activity of the data user.	during deployment	Servers

Data Protection	Maintain an Inventory of Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.	before purchase/self-built	Edge Devices
Data protection	Restrict sensitive data access according to business need	Restrict sensitive data access from Internet if there is no business need. This applies to the IoT devices or backend systems that may store/process/transmit sensitive data.	operation	Edge Devices/Servers
Data protection	Ensure support of data encryption in transit for sensitive information	If sensitive data will be collected by the edge devices, they should have the data encryption capability.	during deployment	Edge Devices/Servers
Data protection	Encrypt sensitive information in transit	If sensitive data will be handled, enable encryption to protect wireless data transmission against eavesdropping or tampering.	before purchase/self-built	Edge Devices
Data protection	Restrict open access to messaging broker	Unless you are setting up an open broker to which allow anyone to connect, the broker should be configured to require client authentication such that no anonymous user can establish connection to the messaging broker.	during deployment	Edge Devices/Servers/User Devices
Data Protection	Enable user authorization in messaging broker	Access control list (ACL) or equivalent control should be defined to restrict which action (e.g. publish, subscribe) an authenticated user can take based on the principle of least privilege.	during deployment	Servers
Minimal Attack Surface	Restrict sensitive data access according to business need	Restrict sensitive data access from Internet if there is no business need. This applies to the IoT devices or backend systems that may store/process/transmit sensitive data.	during deployment	Servers
Minimal Attack Surface	Turn off unnecessary communication ports and services	Ensure that only network ports, services and communication protocols with validated business needs are running on the edge device.	during deployment	Edge Devices

zigbeeNetworking	Expose only approved network services to the Internet	Unless passed the vulnerability assessment and approved by departmental CLO, no service port shall be directly exposed to the Internet.	during deployment/ operation	Network Infra
Networking	Monitor the network of IoT devices	The network which IoT devices connecting to shall be monitored for any abnormality. The cybersecurity events should be fed to the University security information and event management (SIEM) system to correlate event logs from IoT devices, backend servers, network appliances, or other events within the University network.	operation	Network Infra
Networking	Place IoT devices on a separate network	Place IoT devices on a separate network to prevent intrusion or malware from spreading to the core network in case any of the IoT devices is compromised.	during deployment	Network Infra
Physical Security	Verify that physical access does not allow intrusion	Physical security controls such as positioning the edge devices in locked cases or high ground that is difficult to reach should be considered to avoid easy physical intrusion by forced factory reset or unauthorized access to hardware ports.	during deployment	Edge Devices
Software Update	Do not use products that cannot be updated	No matter sourced from third party or developed internally, verify the IoT device is capable of installing further firmware update to fix security issues.	before purchase/self-built	Edge Devices
Software Update	Keep firmware and software up-to-date	Regularly check for system updates and install updates via automatic update mechanism or monthly check	during deployment/ operation	Edge Devices
Software Update	Validate firmware update	A secure firmware validation mechanism shall be implemented to prevent loading of a tampered/malicious software that compromise the IoT device	before purchase/self-built	Edge Devices
Vulnerability Management	Conduct full vulnerability assessment	Before the production launch of an IoT solution, vulnerability assessment exercises should be performed to identify what technologies/services are running on each component of the whole IoT solution, and to find	during deployment	All

		vulnerable, deprecated or exploitable components if any.		
Vulnerability Management	Threat intelligence focused on IoT solutions and technologies	Monitor and regularly review the current Tactics, Techniques, and Procedures (TTPs), and assess the risk based on impact and probability analysis. Taking the newly identified risks into consideration, set appropriate risk mitigation plan and take actions accordingly.	operation	All

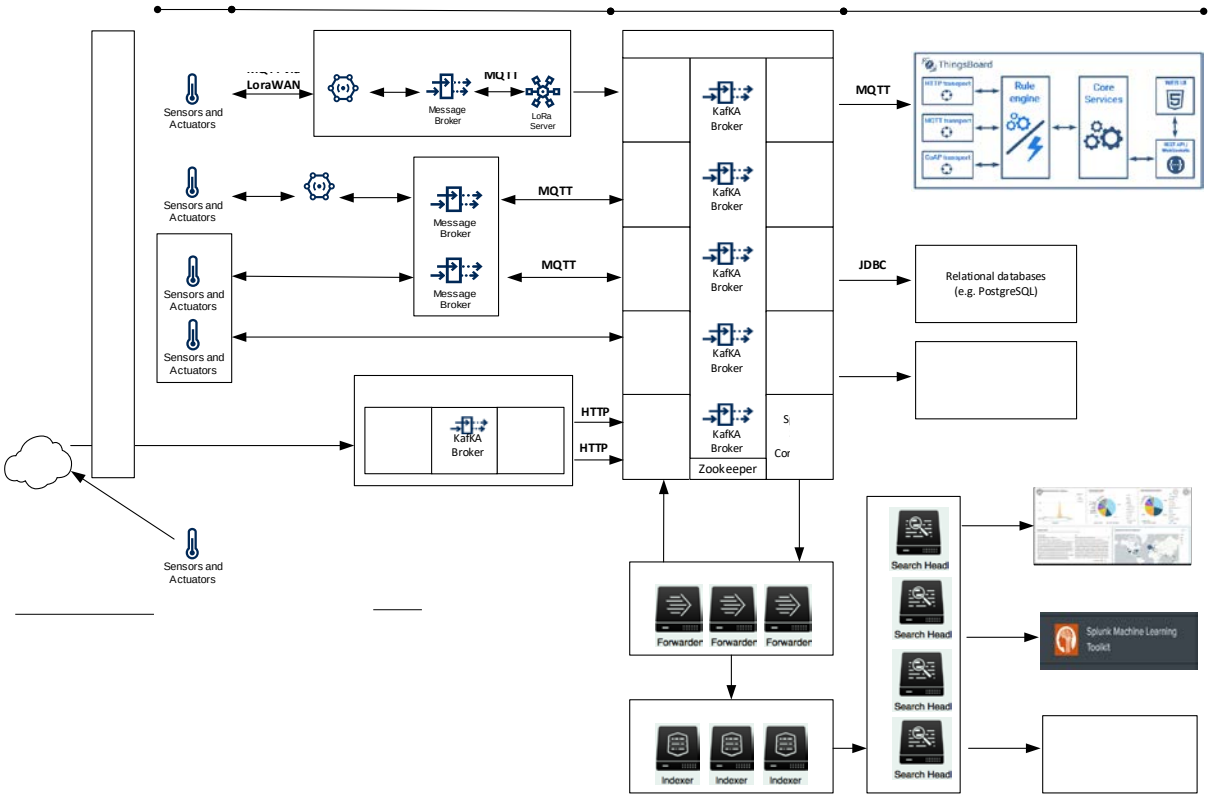
6 What could ITS help in IoT deployment project?

6.1 A shared IoT infrastructure

The main objective of deploying IoT edge devices in the campus is either to collect and analyse the environmental condition from the physical world to improve our business decision making processes or collect the environmental data for research purpose. However, as mentioned in previous sections, in order to achieve these goals, a number of factors need to be well considered and incorporate in the IoT infrastructure setup.

To allow our users to put more focus on business operation or academic researches, ITS is building a shared IoT infrastructure which have incorporated the necessary components. So that users may only acquire the necessary IoT edge devices and register the devices to this shared IoT infrastructure then they could collect the necessary data from through this infrastructure.

The shared IoT infrastructure is composite of the following components.



The shared IoT infrastructure is built with open source components which provide more flexibility to the University to adopt various type of IoT technologies and products. The infrastructure will consist of the following layers:

- Network & Communication Layer
- Data Streaming & Collection Layer
- Data Visualization & Analytics Layer

As the deployment of IoT edge devices is driven by business need, the selection and deployment of the sensory devices will be open to departments. However, in order to leverage this infrastructure to analyse and visualize the data collected, the IoT edge devices shall be able to send the data back the infrastructure and the solution providers shall share the decoding algorithm with the University.

6.2 IoT Services provided by ITS

The following IoT services will be provided by ITS:

- Data capturing and provisioning service

  Departments could connect their IoT edge devices to the shared IoT infrastructure and leverage the network communication components and data streaming components to capture the telemetry data they need. ITS could assist departments to provision edge devices for data capture and communicate with gateway. ITS could provision the collected data to their data stores.

- Data visualization and alerting service

  ITS could help departments to develop simple dashboards to visualize the telemetry data collected through their edge devices and setup alert for detecting the anomalies based on the user pre-defined threshold. Besides, ITS could also train up users to build their own dashboards using the shared infrastructure.

- Data analytics platform as a service

  ITS could provide the splunk platform for department users to perform predicative analysis on the telemetry data captured.

- One-stop shop IoT solution deployment service

  ITS could also provide a project management support service to user departments to study a specific business problem which may possibly be resolved with IoT technologies. After business analysis process, if it is confirmed that IoT deployment could be a possible solution for the business problem, ITS could help the department to implement the solution riding on the shared IoT infrastructure.

6.3 Contact

Should users have any queries about this document or are interested in the IoT related services that ITS could provide, please send an email to its_iot_core@polyu.edu.hk.

~~~~End of Document~~~~
~~~~

Annex A: Supplementary information to be considered while selecting an edge device

Example of Operational Technology Control Protocols

The following is a list of control protocols used in operational technologies

Type	Example
Industrial Control	Open Platform Communication (OPC) Distributed control system (DCS) OPC Unified Architecture (UA)
Automotive	CAN Specification Version 2.0
Building Automation and Control	BACnet
Energy Metering	International Electrotechnical commission (IEC) 620544

Ingress Protection Rating

The IP rating code is a two-digit (or optionally three-digit) designator to standardize the rating of protection level against intrusion of solids and liquids into mechanical and electrical enclosures. An enclosure can be a piece of equipment, an assembly unit, a cable or simply a connector.

The number designator was originally established by the International Electro-Technical Commission (IEC) and the "IP" letters stand for "International Protection" rating or "Ingress Protection" rating. The third digit in the designator is not part of the official IEC standard and is sometimes included (but more often omitted) to reference additional protections.

The IP designator references as follows:

- First Digit – Protection from solid objects or materials
- Second Digit – Protection from liquids and fluids (water)
- Third Digit – Protection against mechanical impacts

It's allowable to use a "X" in place of one of the digits if there is only a single class of protection.

Solid objects and materials can be anything from large – body parts (e.g., limbs, hands, feet, fingers), to medium – tools, wires, plants, to small – dust. This doesn't include a rating for microbe or biological. Those are covered under HEPA standards created by the Department of Energy (DOE).

The two numbers in the IP67 rating code rating refer to:

- 6 – " Dust Protected "; Totally protected against dust ingress.; complete protection against contact
- 7- " Immersion Protected "; Protected against short periods of immersion in water.Ingress of water in harmful quantity shall not be possible when the enclosure is immersed in water under defined conditions of pressure and time (up to 1 m of submersion). Test duration: 30 minutes; Immersion at depth of at least 1 m measured at bottom of device, and at least 15 cm measured at top of device

The complete listing for each of the three numbers in the IP designator are provided below.

In addition to the IEC standard, the United States National Electrical Manufacturers Association (NEMA) also publishes protection ratings for enclosures. The NEMA standard goes beyond the IP ratings by addressing additional product features such as construction practices, gasket and sealant aging and resistance to corrosion. In general, an IP rating can be considered as a sub-set to the NEMA rating.

In this case, the IP67 rating meets a minimum NEMA Enclosure rating of 6.

IP #	First digit:	Second digit:
	Ingress of solid objects	Ingress of liquids
0	No protection	No protection

1	Protected against solid objects over 50mm e.g. hands, large tools.	Protected against vertically falling drops of water or condensation.
2	Protected against solid objects over 12.5mm e.g. hands, large tools.	Protected against falling drops of water, if the case is disposed up to 15 from vertical.
3	Protected against solid objects over 2.5mm e.g. wire, small tools.	Protected against sprays of water from any direction, even if the case is disposed up to 60 from vertical.
4	Protected against solid objects over 1.0mm e.g. wires.	Protected against splash water from any direction.
5	Limited protection against dust ingress.(no harmful deposit)	Protected against low pressure water jets from any direction. Limited ingress permitted.
6	Totally protected against dust ingress.	Protected against high pressure water jets from any direction. Limited ingress permitted.
7	N/A	Protected against short periods of immersion in water.
8	N/A	Protected against long, durable periods of immersion in water

Annex B: Comparison between commonly used wireless communication technologies in IoT deployment

	Sigfox	NB-IoT	LoRaWAN	ZigBee	WIFI 802.11
Descriptions	A proprietary network and protocol. It means for remote meter reading, but can be used for any remote data uplink. It is low speed and low power but also long range.	Runs in the mobile telephone radio spectrum, and piggybacks on old, unused GSM channels, or free space between LTE channels. Target stationary sensor with few uplink per day. Carry higher data rate than other LPWAN technologies.	A low speed, but long range and low power communication protocol. It is an open specification so anyone is free to implement the protocol themselves on their own equipment.	A low-power, low data rate, and close proximity (i.e., personal area) wireless ad hoc network.	WIFI is meanly meant for broadband network connections in a confined space. Normally less than 100 square meter per access point.
Distance	24km	10-15km	5-10km typical (heavily dependent on line of sight)	10-100m	50m (indoors)
Frequency	920-925MHz	Private bands	920 - 925MHz	2.4 Ghz(worldwide) 868 Mhz(Europe) 900-928 Mhz(NA)	2.4 and 5 Ghz
Standards	Proprietary	3GPP	LoRa-Alliance LoRa/LoRaWAN	Zigbee-Alliance	802.11 a/b/g/n/ac
Date Rate	100bps	50-100kbps	50 kbps (intermittent transmission)	20, 40 and 250 Kbits	11 & 54 Mbits/sec

Bidirectional	Limited/Half-duplex	Yes/Half-duplex	Yes/Half-duplex	Unlimited	Yes/Half-duplex
Maximum Messages/Day	140 (Uplink), 4 (Downlink)	Unlimited	Unlimited	Unlimited	Unlimited
Network Topology	Star	Star	Star	Peer to peer, star or mesh	Point to hub
Power Consumption (Battery option and life)	Very low	High	Very low	Very low (low power is a design goal)	High
Complexity (Device and application impact)	Low	Low	Medium	Low	High
Able to build own network infrastructure?	Impossible	Impossible	Possible	Possible	Possible
Security	By default, data is conveyed over the air interface without any encryption. Every device has a unique static ID. It has the ability to do end-to-end encryption in the application layer.	Inherits 4G-LTE's authentication and encryption e.g. device/network mutual authentication, securing of communication channels, secure provisioning and storage of device identity and credentials, and "End-to-End" security for traffic to and from telco's IoT data platform (e.g. HKT)	Based on sessions, where every session is started with static keys, but after a key exchange a unique set of AES keys are used.	Data encryption between sensors and LAN gateway is available.	Data encryption between sensors and LAN gateway is available. Users are requested to use sensors with WPA2 or above. MAC address registration in WIFI controllers for connections can be implemented.

Authentication & Encryption	Not supported	Yes (LTE encryption)	Double 128AES	128 AES plus application layer security	Yes (Requested to be WPA2 at least. Preferably WPA2 Enterprise or above)
What does the setup require to make it work?	Sigfox coverage where you need it, as well as subscription to use the sigfox network Public Network 1. Sensors 2. Providers' cloud platform 3. Subscription on messages delivery 4. Subscriber self-owned data analytic platform (optional)	A subscription with a mobile telephone provider Public Network 1. Sensors 2. If NB-IoT signal from telcos cannot cover a corner, users can deploy a gateway nearby to collect the data from sensors and send it to the telcos. 3. Subscription on messages delivery 4. Subscriber self-owned data analytic platform (optional)	Invest in one's own network with base stations, or get a contract with a service provider that has coverage where you need it. A base station will however need an internet connection and power. Public Network 1. Sensors 2. Providers' cloud platform 3. Subscription on messages delivery 4. Subscriber self-owned data analytic platform (optional) Private Network 1. Sesnors 2. Network Gateway 3. Application Server 4. Data Analytic platform (optional)	Invest in one's own network with LAN gateways. Private Network 1. Sensors 2. LAN Gateway 3. Application server (one's own server or cloud platform provided by vendors) 4. Data Analytic platform (optional)	A WiFi access point, which can be connected to the internet or a local area network Private Network 1. Sensors 2. APs (probably available in the environment already) 3. Application server (one's own server or cloud platform provided by vendors) 4. Data Analytic platform (optional)

Management of network	Management of network has to go through Sigfox	Management of network has to go through telco, except when gateways are used (and hence the sections between the sensors, gateways and internet egress from the organizations can be managed by users)	For private network, users can manage the network.	Users can manage the network.	Users can manage the network unless the management of APs is performed by other parties (e.g. other departments)
Good for…	Remote electricity or water meter reading. Mostly uses where you do not need to have downlink messages to the devices.	Mostly for sensor readings, tracking and fleet management	Running an isolated or private network on a farm or in a city. Ideal for sensors that only seldomly send a value, like a soil moisture sensor sending its measurements every 10 minutes, or a water trough alarming that it is empty. It is also a good system for the tracking and monitoring of wildlife in a predefined area.	Works well within the area it is setup in. Ideals for home automation, smart grid, remote monitoring and control etc.	Works well within the area it is setup in. Great for security cameras, power meters or anything that is installed in a fixed location, has power, and needs the bandwidth.

Doesn't Work well for…	Message heavy applications as Sigfox limits the amount of messages one can send to a message every 10 minutes in a 24 hour period. Slow speed as a sms can take a minute to send thus not an option for IoT products that require an immediate feedback loop such as health monitoring. Not ideal for live tracking a vehicle.	A high speed internet connection	Limitations on the used frequency band can cause high latency delivered messages. It is therefore not an option for IoT prodcuts that require an immediate feedback loop such as health monitoring. Due to the limited coverage of a private network, it is not ideal for tracking of vehicles that travel long distances.	Not as secure as WIFI based secured system. Since the coverage is limited and hence cannot be used as outdoor wireless communication system.	Only works in space where it is setup and has limited range. Also uses a substantial amount of power, so it is not ideal for battery operated devices.
Costing	One cannot install one's own base station and are limited to where the stations are setup. This limit the coverage range. However, the costs of setting up one's own network may be prohibitive.	Subscription, sim card, data costs and hardware.	The costs of investing in creating one's own network will be offset by having one's own network which means you can create coverage where it is needed and nothing else exists.	Sensors, LAN gateway, application server	Although we cannot assume that everyone has home WIFI, this is a great option for industry.

[i] Simmon E (forthcoming) A Model for the Internet of Things (IoT). (National Institute of Standards and Technology, Gaithersburg, MD).
[ii] Jacob Fraden, Handbook of Modern Sensors: Physics, Designs, and Applications, fourth edition (Springer: April 2010)