Digital Policy Office

INFORMATION SECURITY

Practice Guide

for

Internet of Things Security

Version 1.2

July 2024

COPYRIGHT NOTICE

Amendment History				
Change Number	Revision Description	Pages Affected	Revision Number	Date
1	Updates were made on Definition of IoT Device, Asset Management, and Figures 4.1, 7.1, 7.2.	3-1, 4-2, 5-2, 7-1, 7-2	1.1	June 2021
2	Change “Office of the Government Chief Information Officer” (or “OGCIO”) to “Digital Policy Office” (or “DPO”)		1.2	July 2024

Table of Contents

1. Introduction

1.1 Purpose

This document is intended to facilitate Bureaux and Departments (B/Ds) in adoption of Internet of Things ("IoT") technology. It aims to provide guidance notes to a diverse group of audiences, such as management staff, IT administrators, system owners and information security stakeholders, who have the responsibility to assess the security impacts on the Government information system in use of IoT devices for the storage, processing, or transmission of government information.

This document highlights common security considerations and industry best practices in the adoption of IoT with the purpose to enhance the understanding of the basic of IoT security.

As each IoT deployment has its own characteristics and needs, B/Ds are advised to take a risk-based approach and implement proper security measures to protect information assets.

1.2 Normative References

The following referenced documents are indispensable for the application of this document.

- Baseline IT Security Policy [S17] , the Government of Hong Kong Special Administrative Region
- IT Security Guidelines [G3] , the Government of Hong Kong Special Administrative Region
- Information technology – Security techniques - Information security management systems - Requirements (second edition), ISO/IEC 27001:2013
- Information technology - Security techniques – Code of practice for information security controls (second edition), ISO/IEC 27002:2013

1.3 Terms and Convention

For the purposes of this document, the terms and convention given in S17, G3, and the following apply.

Abbreviation and Terms	
IoT Devices	Devices that have network connectivity and computing capabilities, which function autonomously to interact with the physical environment by ways of sensing or actuation.

1.4 Contact

This document is produced and maintained by the Digital Policy Office (DPO). For comments or suggestions, please send to:

Email: it_security@digitalpolicy.gov.hk

Lotus Notes mail: IT Security Team/DPO/HKSARG@DPO

CMMP email: IT Security Team/DPO

2. Information Security Management

Information security is about the planning, implementation and continuous enhancement of security controls and measures to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission and its associated information systems. Information security management is a set of principles relating to the functions of planning, organising, directing, controlling, and the application of these principles in harnessing physical, financial, human and informational resources efficiently and effectively to assure the safety of information assets and information systems.

Information security management involves a series of activities that require continuous monitoring and control. These activities include but not limited to the following functional areas:

- Security Management Framework and the Organisation;
- Governance, Risk Management, and Compliance;
- Security Operations;
- Security Event and Incident Management;
- Awareness Training and Capability Building; and
- Situational Awareness and Information Sharing.

Security Management Framework and Organisation

B/Ds shall establish and enforce departmental information security policies, standards, guidelines and procedures in accordance with the business needs and the government security requirements.

B/Ds shall also define the organisation structure on information security and provide clear definitions and proper assignment of security accountability and responsibility to involved parties.

Governance, Risk Management and Compliance

B/Ds shall adopt a risk-based approach to identify, prioritise and address the security risks of information systems in a consistent and effective manner.

B/Ds shall perform security risk assessments for information systems and production applications periodically and when necessary so as to identify risks and consequences associated with vulnerabilities, and to provide a basis to establish a cost-effective security program and implement appropriate security protection and safeguards.

B/Ds shall also perform security audit on information systems regularly to ensure that current security measures comply with departmental information security policies, standards, and other contractual or legal requirements.

Security Operations

To protect information assets and information systems, B/Ds should implement comprehensive security measures based on their business needs, covering different technological areas in their business, and adopt the principle of "Prevent, Detect, Respond and Recover" in their daily operations.

- Preventive measures avoid or deter the occurrence of an undesirable event;
- Detective measures identify the occurrence of an undesirable event;
- Response measures refer to coordinated actions to contain damage when an undesirable event or incident occurs; and
- Recovery measures are for restoring the confidentiality, integrity and availability of information systems to their expected state.

Security Event and Incident Management

In reality, security incidents might still occur due to unforeseeable, disruptive events. In cases where security events compromise business continuity or give rise to risk of data security, B/Ds shall activate their standing incident management plan to identifying, managing, recording, and analysing security threats, attacks, or incidents in real-time. B/Ds should also prepare to communicate appropriately with relevant parties by sharing information on response for security risks to subdue distrust or unnecessary speculation. When developing an incident management plan, B/Ds should plan and prepare the right resources as well as develop the procedures to address necessary follow-up investigations.

Awareness Training and Capability Building

As information security is everyone's business, B/Ds should continuously promote information security awareness throughout the organisations and arrange training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and conform to security best practices.

Situational Awareness and Information Sharing

As cyber threat landscape is constantly changing, B/Ds should also constantly attend to current vulnerabilities information, threat alerts, and important notices disseminated by the security industry and the GovCERT.HK. The security alerts on impending and actual threats should be disseminated to and shared with those responsible colleagues within B/Ds so that timely mitigation measures could be taken.

B/Ds could make use of threat intelligence platforms to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.

3. Overview of IoT

3.1 Definition of IoT Device

There are many different kinds of IoT devices in the market, ranging from sensors, actuators and more. As IoT technology keeps evolving, there is no unique definition commonly acceptable around the world. In the context of this document, IoT devices are referred to those have network connectivity and computing capabilities, which function autonomously to interact with the physical environment by ways of sensing or actuation. For devices that can be configured to have such network connectivity with Internet or enterprise network, regardless they are connected to such network or not, the devices are considered as IoT devices. The following is some general examples of IoT devices:

- sensors (e.g. air quality, temperature) with network connectivity;
- smart meters (e.g. electricity, water) with network connectivity; and
- smart appliances (e.g. refrigerator, TV, lighting) with network connectivity.

Today, many IT devices have built-in IoT functionalities. In this document, we would focus on those IoT devices that have general business purposes in the Government. For IoT devices applied in specialised industries, for example, actuators such as smart electric motors or smart pumps, they are generally integrated in the Operational Technology (OT) which monitors and controls industrial equipment, processes and events. OT is beyond the scope of this document. Conventional IT equipment, such as mobile devices, network appliances, workstations and servers are not the focus of this document as the general security protections have already been specified in the Baseline IT Security Policy and IT Security Guidelines as well as relevant practice guides. However, if the conventional IT equipment are deployed as IoT devices, for instance, a computer with built-in webcam is deployed as surveillance system or the GPS/Bluetooth function of a mobile phone is deployed as a location tracker, then the controls of IoT devices as a whole to such applications should also apply. Also, as many IT equipment are built on various components, due diligence is required to assess the functions of the components and decide whether the components have been disabled properly or the security controls of IoT devices have been applied properly.

As B/Ds may already have some IoT devices deployed, B/Ds can perform their security assessment of their IoT devices from the following angles:

- data processed and stored in the IoT devices;
- network and other devices being connected to the IoT devices; and
- protection of the IoT devices.

When assessing security impacts of the use of IoT devices in the office environment, the following factors should be considered whether IoT devices would:

- handle or capture sensitive information;
- connect to departmental networks or devices owned by B/Ds;
- be installed in the office environment;
- connect to the Internet or other external devices with potential of sensitive information exchange; and
- have any other security implications affecting the Government image if not properly managed.

B/Ds should assess the risks posed by the IoT devices and the impacts on the business and the Government image in case of compromise. B/Ds shall define and implement proper measures to ensure the information security of IoT devices and data commensurate with the classification of the information.

4. Introduction to IoT Security

4.1 The Challenges of IoT Security

In IoT-based systems, data protection for those smart devices poses new challenges. The attacking surfaces of IoT devices are wider and more diversified than traditional IT equipment. That said, the security threats to IoT devices can come from many sources: the device, network, storage as well as the applications/services associated with IoT deployment such as cloud, web and mobile services. All of them are susceptive to cyber threats.

In short, the major threats to IoT are described in the following areas:

Device

Devices usually are the primary targets where attacks are initiated. The vulnerabilities in the devices can come from memory, firmware, physical interface, web interface, and network services. Attackers can also exploit the vulnerabilities arose from the unsecure default settings, outdated components, and unsecure update mechanism. The lack of device management and physical hardening are also common threats to the devices. The following are some common flaws threatening the devices:

- Lack of device management

  IoT devices may lack proper management of devices, including asset management, patch management, secure decommissioning, and systems monitoring, etc. This happens usually in low-cost design sensors.

- Insecure default settings

  As some IoT devices are very small in size and are deployed in large quantity, the administrators may ease the operations by using the default setting of the devices. However, the default settings are generally vulnerable to external attacks and are easily exploited to cause unauthorised system access.

- Lack of physical hardening

  Physical hardening measures such as port restriction or physical access restriction are not available or sufficient for IoT devices, in particular those installed outside the Government premises. This allows attackers to gain control through physical break-in.

- Use of insecure or out-of-support components

  As IoT devices may be deployed in vast areas and many devices are designed under low cost constraints, the components, both hardware and software, may be out of support or insecurely customised. It would allow the devices to be easily compromised.

- Susceptive to device modification
  As the device manufacturers may not deploy security by design approach, the IoT devices may leave backdoors unintentionally.

- Susceptive to device destruction
  As IoT devices may be deployed in public areas, device theft or sabotage could damage the devices or related systems and cause system malfunction.

Data

IoT devices may need to collect data and exchange those data with peer devices. Users may underestimate the amount of data collected and capture unnecessary data. The data leakage is one of the common threats to the IoT devices with the following reasons:

- Weak or hardcoded passwords
  Some IoT devices may not support strong password settings or even do not allow change of passwords. Moreover, if the users are lack of security awareness, they may choose passwords that are easily brute forced. Attackers may then easily gain access to such systems.

- Lack of secure update mechanism
  Some manufacturers of IoT devices may lack resources to provide security update to their devices, including firmware and software modules, or may not facilitate timely security updates. Furthermore, the IoT devices may consist of third party software/code without security update available.

- Insecure data storage
  The IoT devices may consist of data storage but it may not be secured or without encryption features for storing sensitive information. Therefore, the security protection against unauthorised access may not be sufficient.

- Information leakage
  As the IoT devices may be installed in restricted areas, it may pose the risks in revealing sensitive environmental information to unauthorised parties. Moreover, if the IoT devices are interconnected to the Internet, attackers may obtain information through malware infection, unauthorised access or man-in-the-middle attack.

Network

Attackers can launch attacks to connected IoT components via communication channels. Moreover, communication protocols used in IoT systems may have security vulnerabilities that can affect the IoT systems. The following are some common threats:

- Insecure network services

  Insecure network services running on the device itself, especially those exposed to the Internet, could compromise the IoT security or allow unauthorised remote control.

- Insecure data transfer

  Some IoT devices may not provide sufficient encryption strength or access control of sensitive data due to its limited capacity.

- Malicious information gathering through network

  Although interconnectivity feature is one of the advantages of IoT devices, this also introduces attacking surfaces. The attacks such as man-in-the-middle or session hijacking may allow the attackers to gain sensitive information.

- Malicious attack

  Same as above, malicious attackers may gain access to the IoT devices through network and install malware on the devices. This would result in launching DDoS attack or even turning IoT devices to botnets.

Privacy

IoT devices may be installed in office environment or public areas. The administrators may not be aware that the IoT devices may collect excessive personal information. If not properly managed, attackers could gather these personal information and compromise privacy.

Application

Vulnerabilities in cloud services, mobile applications, web applications and related software for IoT devices can lead to compromised systems. The following are some common threats:

- Insecure application interfaces

  Insecure web, backend APIs, cloud, or mobile interfaces in the IoT ecosystem could leave the IoT devices compromised. Common issues include lack of authentication/authorisation, lack of or weak encryption, or lack of input and output verification.

- Software vulnerabilities

  Software vulnerabilities and configuration errors are common threats to IoT devices. These vulnerabilities can usually be exploited by the attackers using the exploit tools, like malware kits. For example, web applications can be exploited to steal user credentials or install malicious firmware updates.

4.2 Components in IoT Deployments

The following graph illustrates the common components in the IoT-based deployments. It consists of **IoT devices, communication, backend server and storage as well as applications**. This assists us in identifying threats and corresponding security measures. The deployment mode would be described in Section 7 - Use Cases of IoT Devices. Depending on the deployment scalability, some components are optional. For instance, not all IoT deployments need to deploy servers or databases.

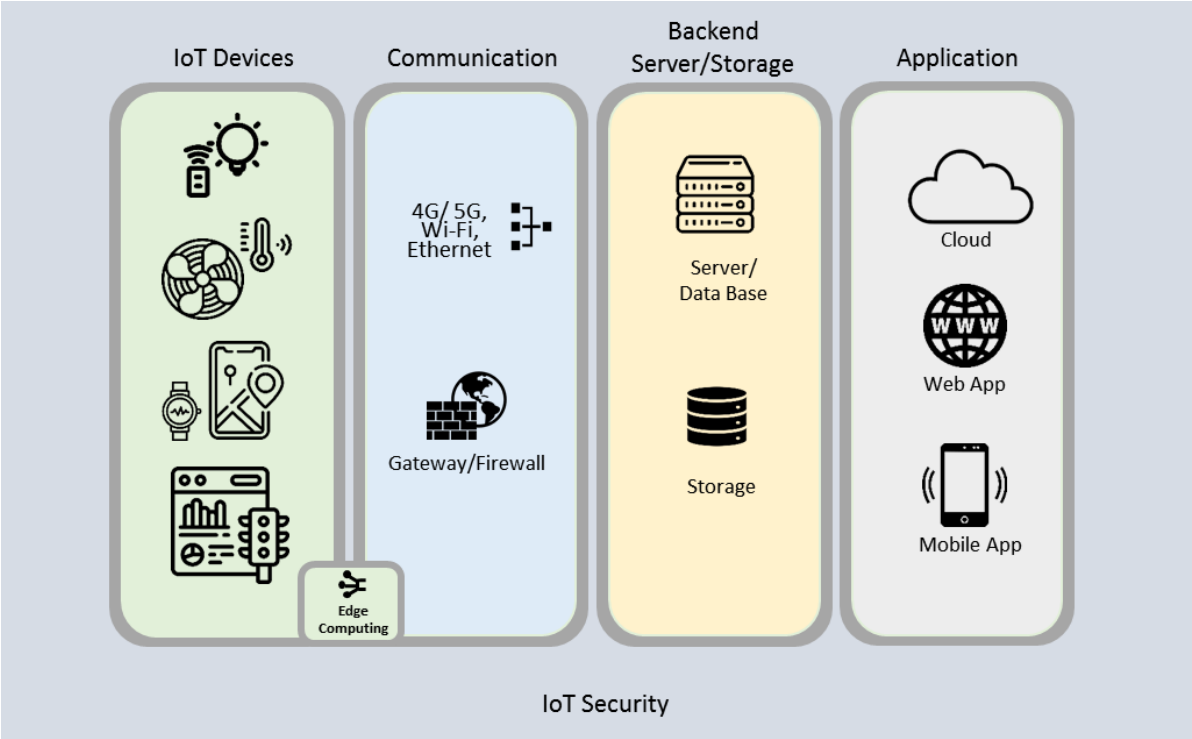

Figure 4.1 Common components in the IoT-based deployments

IoT Devices

Device layer, also known as the endpoint, is the physical interfacing layer of an IoT-based system. IoT devices come with various operating systems, CPU types, memory, etc. These devices could be located in the office environment or public areas, and some may be located in remote areas where remote controls are required in normal operations.

Edge computing is an essential component in protecting the IoT security infrastructure. As IoT devices are usually limited in capabilities on security provision, edge computing serves the role in fending off possible attacks. In such cases, edge device serves as the gatekeeper to master those IoT devices.

Communication

Connectivity is the key to the IoT devices. The IoT devices may connect to each other or connect to the Internet directly. The network infrastructure involves data, voice, image and video over LAN (Local Area Network), WAN (Wide Area Network) or mobile/wireless connections (4G/5G, Wi-Fi, etc.).

Some connectivity examples include:

- 4G/5G
- LTE
- Wi-Fi
- Ethernet
- NFC
- Bluetooth Low Energy
- RFID

Technically, there are many types of communication identifiers for IoT device, such as IP address, MAC address, phone numbers, etc, among which IP address is more commonly used. IP address works over wireless connectivity (Wi-Fi, 4G, 5G, LTE, etc.) as well as wired (Ethernet, etc.) communications.

Backend server and storage

Some IoT deployments need backend servers or databases. In some large scale IoT deployment, the backend servers or databases are required to support computing functions or data storage. The backend server or databases could be provided by data centre or through cloud platform.

Application

The IoT deployment can integrate with cloud, web or mobile applications. In some cases, cloud platform is responsible for the effective processing and management of the collected data. It also hosts applications to provide services and to manage the whole IoT architecture.

5. Security Considerations and Controls for IoT

Information security is a major concern of any Information and Communications Technology (ICT) systems. IoT system is no exception. Hence, information security management principles are applicable to IoT security. However, IoT systems present particular challenges to information security as they are highly distributed and involve a large number of diverse entities. The utilisation of IoT devices requires a holistic view of the end-to-end security and risk based approach to identify, prioritise and address the security risks of IoT devices, including but not limited to asset management, authentication and authorisation, communication network, software and application, backend infrastructure, device security, physical security, etc. Due to certain similarities in IoT devices and mobile devices such as connectivity, mobility and small in size, the security requirements and principles for mobile devices laid out in the government security documents should be similarly applied to IoT devices.

The following sections will describe the challenges and advices on IoT-specific security areas focusing on the following security domains:

- IT Security Policies
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development and Maintenance
- Compliance

5.1 IT Security Policies

B/Ds shall define and enforce their IT security policies to provide management direction and support for protecting information systems and assets in accordance with the business needs and security requirements. When a deployment of IoT devices is planned or introduced to the information systems, B/Ds are required to review their departmental security policy to cater the needs for security protection of the IoT devices. Also, a formal usage policy and procedures shall be in place, and appropriate security measures shall be adopted to protect against the risks to IoT devices. B/Ds are advised to:

- Review Departmental IT Security Policy

  Departmental IT security policy should be enforced, regularly reviewed and updated when necessary for protecting information systems and assets in accordance with the business needs and security requirements. The updates may include new or enhancement of the security requirements on various security domains such as access control, physical security, communication security, assets management, etc. especially when IoT is introduced to IT environments (e.g. IoT devices, backend servers/storage, etc.).

- Establish a formal usage policy and procedures for IoT devices.

  A formal usage policy and procedures shall be in place, and appropriate security measures shall be adopted to protect against the risks to IoT devices. The usage policy and procedures should include but not be limited to the requirements for a.) physical protection against theft or loss of IoT devices and data, b.) access control against unauthorised device manipulation and data modification, c.) communication protection against data interception or sniffing attack, d.) cryptographic requirements that provide minimum standards for basic and effective protection, e.) log management that provides tracking for abnormal activities and identify accountability, f.) vulnerability management against known security loopholes protection from malware against malicious codes and virus.

  The usage policy and procedures should also include rules and advices on securing the connection among IoT devices, and IoT devices connecting to the Government networks for protecting IoT endpoints from security threats such as becoming as a part of botnet manipulated by attackers, malware spreading, Distributed Denial of Service (DDoS) attack, etc.

5.2 Asset Management

B/Ds should ensure and maintain an appropriate level of protection of IoT devices and data. In particular, B/Ds should maintain and review an inventory of IoT devices that handle sensitive data or connect to internal/external networks, and make suitable arrangements to ensure that data is handled in accordance with the government security requirements with the goal to minimise security risks posed on IoT devices, the government data as well as the possible impact on information systems.

- Properly document and manage IoT devices.

  B/Ds should identify IoT devices from the assets, indicate in the inventory, maintain and regularly review the inventory to ensure it is update to date and accurate. An inventory of IoT devices should be drawn up to provide device asset information including models, unique identifier, firmware, serial numbers, ownership, etc. with indication on whether any sensitive data would be processed, stored or transmitted. B/Ds should consider to deploy a computer system to manage the asset records to effectively facilitate the asset management as well as IT security.

- Evaluate and classify the data handled by IoT devices.

  Data should be classified based on its level of sensitivity. Data should be protected commensurate with its classification in process, storage or transmission. Data ownership and handling procedures should be clearly defined and documented.

- Erase sensitive data stored in IoT devices when no longer required

  To prevent data leakage, loss or unauthorised access, all sensitive data shall be completely cleared or destroyed before disposal or re-use with reference to Section 10.3(b) of G3.

5.3 Access Control

B/Ds shall define and implement proper security measures to ensure that the security of IoT devices and data commensurate with the classification of the information. The measures should be effectively against compromise and manipulation of IoT devices and data through unauthorised access. The following common security measures, controls and practices for accessing and managing IoT devices should be taken into consideration but do not mean to be exhausted:

- Select IoT devices that are designed to support security features (e.g. identification, authentication and authorization).
- Restrict and control access to IoT devices and data, grant access rights based on the principle of least privilege and segregation of duties. Revoke the rights when they are no longer required.
- Ensure sufficient authentication, use of strong password and change password periodically.
- Enable two-factor authentication if available.
- Change default configurations and settings such as username and password.
- Enable account lockout mechanism against excessive invalid login attempts and brute force attack.
- Disable or remove unnecessary user accounts (e.g. guest, demo).
- Allow only trusted IP addresses or/and authorised devices to access to IoT devices or backend systems (e.g. cloud-based servers).
- Allow only authorised persons to physically access to IoT devices.
- Protect user credential (e.g. by encryption) during transmission and in storage.
- Disable unnecessary services or logical ports (e.g. telnet) and physical ports (e.g. USB) if feasible.
- Use certificates whenever possible for device authentication and confidentiality during Transport Layer Security (TLS) and other protocol negotiations, as well as to support various identity bindings when integrating with other access control mechanisms.
- Ensure that the Public Key Infrastructure (PKI) architecture supports standard services such as revocation checking, trust management, enrolment and registration procedures, and compromise recovery.

5.4 Cryptography

Cryptographic techniques are indispensable in an IoT environment, and they provide security assurance for authentication, confidentiality, integrity and non-repudiation when implemented properly. Encryption is widely used to protect the confidentiality of data, either stored or transmitted. Sensitive information must be encrypted if it needs to be stored in IoT devices. Digital signatures or message authentication codes are used to verify the authenticity or integrity of stored or transmitted sensitive or classified data. B/Ds should utilise cryptographic techniques for protecting data, systems, devices and communication among them in an IoT environment. The following common security measures, controls and practices should be taken into consideration but do not mean to be exhausted:

- Select IoT devices that are designed to support cryptographic features (e.g. encryption, PKI, etc.).
- Use cryptographic protocols to encrypt any communications among peer devices, smartphone applications, cloud services and Application Programming Interface (API) calls.
- Encrypt sensitive data in storage and transmission over un-trusted networks.
- Use standard and trusted encryption algorithm with strong key length (e.g. AES-256) for data storage encryption.
- Properly manage and use of cryptographic keys; avoid using same encryption key for multiple end points.

5.5 Physical and Environmental Security

For IoT devices, security controls shall be enforced to protect the devices against loss, theft and damage according to the classification of information being stored, processed and transmitted by the IoT devices.

IoT devices and related network equipment should be properly managed, sited and protected to reduce the risks from environmental threats and unauthorised physical access. Attackers may exploit physical vulnerabilities of IoT devices to compromise them and other endpoints that reside on the same network.

For IoT devices in use, B/Ds should avoid collecting and storing classified information in these IoT devices. If there are business needs to process classified information, the data should be encrypted and transmitted to secured backend storage where security controls conform to the relevant government security requirements. If it is unavoidable to store classified information in the IoT devices without staff attended due to business needs, B/Ds shall implement proper physical protection with compensating measures such as data wiping, network disconnection when attempt of breaking-in of physical protection is detected and confirmed.

The following common security measures, controls and practices related to physical security of IoT devices should be taken into consideration but do not mean to be exhausted:

- Provide sufficient physical protection and detection measures and controls (e.g. key locks, intrusion detection system, alarm or surveillance system, etc.) for IoT devices and related equipment to detect physical tampering when especially installed in public areas or unattended locations.
- Properly siting and installation of IoT devices with sufficient physical measures and controls can effectively protecting from loss, theft, service interruption, data interception or being physically attacked or destroyed.
- Protect power and telecommunications cabling from interception, interference or damage is also important.
- Ensure IoT devices and equipment should not be easily disassembled.
- Restrict direct access to IoT devices via physical interfaces or ports.
- Enable detailed logging of any physical access such as USB port.
- Disable all unnecessary physical interfaces and ports including those for debugging purpose.

5.6 Operation Security

B/Ds shall ensure the operations on IoT components and its environment are secure. Protection from malware, logging IT processes and events, monitoring suspicious activities, prevention of exploitation of technical vulnerabilities, etc. are considered essential and effective. The following common security measures, controls and practices related to IoT operations should take into consideration but do not mean to be exhausted:

Operational Procedures and Responsibilities

- Establish and maintain operational procedures for IoT devices, related systems and networks. The procedures are step-by-step operating instructions (e.g. the installation and configuration of IoT devices and systems, processing and handling of data, etc.),
- Apply the principle of least functionality to manage IoT devices, related systems and networks. Remove and restrict all unnecessary functions, services or components.

Protection from Malware

- Enable anti-malware protection on all IoT endpoints including IoT devices, backend systems, mobile devices, etc.
- Regularly update malware definitions as well as their detection and repair engines whenever necessary.

Vulnerability Management

- Timely install the latest security patches and update firmware on IoT endpoints as provided by product vendors or implement other compensating security measures.
- Validate the integrity and authenticity and test the security patches and firmware provided by manufacturer before deploying to IoT devices.
- Define and maintain a list of authorised software or application.

- Verify and assess the risks (e.g. program bugs, security vulnerabilities or backdoor) and impacts before using open-source software or code (e.g. libraries, databases and API, etc.).

Cloud Data and Communication Security

- Encrypt data stored in cloud and communication between the cloud and other endpoints.
- Properly manage and protect cryptographic keys for their whole life cycle. Consider using Hardware Security Module (HSM) to protect encryption key operations when data stored is considered sensitive.

Logging and Monitoring

- Define and review policies relating to the logging of activities of IoT devices and relevant information systems according to its business needs and data classification.
- Retain logs for a period commensurate with their usefulness as an audit tool.
- Protect log records against unauthorised access and tampering.
- Regular check the completeness and the integrity on log records.
- Dynamically and continuously monitor IoT endpoints and related network traffic in real-time. This could help to timely detect and response to abnormal or suspicious activities.

IoT Device Security

- Secure chips are preferred on IoT devices in which high security level is required. Enforce secure booting to prevent unauthorised firmware, bootloader or boot image update.
- Use hardware that incorporates security features to strengthen the protection and integrity of the device.

5.7 Communications Security

As IoT devices are capable to communicate with other devices and systems via wired or wireless connection, sufficient and effective security measures and controls should be in place to address the relevant security threats and attacks.

For the IoT devices connecting to the Government internal networks without proper protective measures, they can become a point to breach security such as disclosure of classified information, spreading malware into the Government internal network or being infected as attacking devices controlled by attackers to launch DDoS attack.

Users are prohibited from connecting their IoT devices to external network if these IoT devices are simultaneously connected to a Government internal network unless with appropriate approval from B/Ds.

The following common security measures, controls and practices related to communication security of IoT devices should be taken into consideration but do not mean to be exhausted:

- Keep network simple and reliable (i.e. minimise number of network interface points between "secured" network and other network).
- Maintain network information such as network diagrams, logical and physical address, and configurations of IoT devices and related network equipment to reflect the latest and comprehensive view of network environment for effective security controls and incident response.
- Divide networks into separated network domains by physical means or logical means to minimise the impact when security breach occurs.
- Ensure the communication between components/layers (i.e. IoT devices, network equipment, backend systems/storage and application) are secure.
- Restrict and control all network traffic and connections (e.g. by firewall rules, MAC address filtering, etc.) to allow only authorised inbound and outbound traffic, and legitimate devices connecting to the network.
- Disable all unnecessary and unsecure network services (e.g. telnet, FTP, etc.) and utilise secure protocols instead (e.g. SSH, SFTP, etc.).
- Enable encryption in wired and wireless communication.
- Encrypt data with standard and trusted encryption algorithm before transmitting over the network.
- Enforce strong authentication in accessing network services, and device-to-device connection.
- For device-to-device connection, user interaction is required in initial pairing process to avoid unintended pairing to unauthorised remote parties. During initial pairing process, the default wireless passphrase should be changed from the factory default or password should be reset prior to providing normal service.
- Establish frameworks of zero trust network[1] and/or secure access service edge (SASE)[2] so as to control authorised and secure access to IoT systems.

- Implement intrusion detection system (IDS) to detect abnormal activities, rogue devices, and potential information security incidents and intrusion prevention system (IPS) to prevent malicious attacks by blocking suspicious traffic. Data analytics and deep packet inspection can help identify threats and anomalies in the data generated by IoT devices.

[1] Zero trust network refers to security concept that no implicit trust granted to users, assets or services based on physical or network location (i.e. LAN or the Internet). Authorisation and authentication are strictly enforced before granting access. Least-privilege access is granted only according to user identity and role after the assessment of access request.

[2] Secure Access Service Edge (SASE) refers to network architecture that combines wide area network (WAN) capabilities and network security functions, such as secure web gateways (SWG), cloud access security broker (CASB), firewalls as a service (FWaaS) and zero trust network access (ZTNA), to deliver as a service.

5.8 System Acquisition, Development and Maintenance

Security is indispensable in information technology environment nowadays. Insufficient security awareness and measures could seriously affect IT infrastructure, business operations and reputation. For IoT related applications, systems and devices, security should be as an integral part across the whole system development life cycle (SDLC). Security should be considered at the early stage of SDLC for better management of the security risks and related issues. Security by design is an approach to achieve this security objective. Security should have its own requirements that are incorporated into the system requirements. The requirements should be properly and clearly defined based on government, legal and regulatory, and business requirements to ensure confidentiality, integrity and availability of system, device and data,

The security requirements stated in the Government IT Security Policy and Guidelines apply to IoT related applications, systems and devices. B/Ds are advised to observe Section 16 of S17 and G3 – System Acquisition, Development and Maintenance for the requirements.

In addition, security review should be conducted in the design stage. It can ensure necessary security requirements are identified and incorporated, associated security risks and impacts are assessed and addressed to effectively facilitate the subsequent stages in the SDLC.

For IoT related applications, systems and devices, security risk assessment and audit shall be conducted to verify the identified risks in security review and ensure proper and sufficient security measures are in place before production.

The following common security measures, controls and practices related to acquisition and development security of IoT applications, systems and devices should be taken into consideration but do not mean to be exhausted:

- Define and review the security requirements in accordance with the Government security policy and guidelines and departmental IT policy such as data and system access control (e.g. authentication method), cryptographic management (e.g. encryption algorithm, key protection), vulnerability management (e.g. availability of firmware, security patch provided by service provider / manufacturer), communication protocols (e.g. SSH, TLS, HTTPS), backup strategy
- Identify the stakeholders (e.g. data owner, system owner), define and document their roles and responsibilities.
- Change control should be in place. Changes on system configurations or programming code should follow the defined procedures to maintain the integrity and reliability.
- Conduct security risk assessment for systems and applications at required time period (e.g. before production, prior to major change or upgrade). Test, review and implement proper security measures and ensure the effectiveness.

IoT related systems and devices acquisition

- Research and study should be conducted to evaluate the security mechanism and features that are suitable and meet the defined security requirements.
- Choose IoT devices or systems that have design, built-in or implemented with physical and logical security features such as access controls (e.g. authentication), vulnerability management (e.g. firmware, security patch), anti-malware protection mechanism (e.g. firewall), cryptographic controls (e.g. encryption, trusted platform module) that could effectively strengthen the protection of the device, system and data.

Application design and development security

- Consider security throughout data life cycle from collection/generation to disposal.
- Ensure and maintain the integrity of an application (e.g. by version control mechanism, separation of environments for development, system testing, acceptance testing, and live operation).
- Avoid collect and store sensitive information more than required.
- Avoid collect and store classified information in IoT devices.
- Document the data item, data classification level and its protection mechanism in all design documents.
- Check web application and API service against globally recognised standards (e.g. OWASP).
- Protect web application and API service by web application firewall.
- Validate data input of web application and API service.
- Use encryption in web application and API service to protect information in transmission.
- Implement authentication in web application and enable API service with session timeout.
- Implement encryption in the communication between the mobile application and backend cloud applications or IoT devices.
- Implement data encryption and consider two-factor authentication, when stored data is considered sensitive.

5.9 Compliance

B/Ds shall avoid breaches of legal, statutory, regulatory or contractual obligations related to security requirements. B/Ds should consider not only local legislation and regulations, but also the applicability of the relevant laws or acts from other countries or regions, especially regarding personal data and privacy. B/Ds are advised to seek professional or legal advice from the corresponding parties if necessary. Security measures shall be implemented and operated in accordance with the respective security requirements.

For IoT deployment, B/Ds may subscribe off-the-shelf cloud service for IoT backend systems/storage or applications. B/Ds are advised to carefully study and understand the scope, contents, contractual terms and conditions, liability and limitation, usage policy, etc. of the cloud services before subscription. B/Ds should evaluate the sufficiency of the corresponding security measures and controls that can meet the Government security requirements especially handling classified /sensitive data in selecting the solution. Besides, B/Ds should be aware that the information systems and the stored data of the cloud services may be located outside Hong Kong which may thus be regulated by the overseas laws.

For cloud services and related security consideration, please refer to the Practice Guide for Cloud Computing Security on ITG InfoStation https://itginfo.ccgo.hksarg/content/itsecure/docs/Guidelines/DocRoadmap.shtml.

For security of outsourcing services, please refer to Section 17 of S17 and G3 – Outsourcing Security.

Documentation

B/Ds shall keep records to evidence compliance with security requirements and support audits of effective implementation of corresponding security measures. Reports or documented results of security risk assessment and security audit are considered as an appropriate and acceptable proof. As Security Risk Assessment (SRA) and Security Audit (SA) are on-going processes, the records can serve as reference to facilitate the next assessment or audit as well as further follow up actions.

Compliance with the Government security regulations and policies should be checked and clearly included in the specifications of the service contract and in Service Level Agreement (SLA). The audit report to be provided by the auditors for compliance check should assure the proper controls of IT security policies, asset management, access control, cryptography, physical security, operations security, communications security, system development and compliance are in place.

Data protection, Personal data and Privacy

B/Ds shall protect their information asset throughout its life cycle from being generated or collected, stored, processed, transmitted, to destruction.

B/Ds shall evaluate, classify and protect the data commensurate with its data classification. Data ownership, roles and responsibilities of all relevant stakeholders should be clearly defined and documented. The adoption of IoT is usually driven by business needs. Therefore, it would be the responsibility of the IT system owner involving IoT devices to manage the related security. With reference to the Organisation Chart for Departmental IT Security Management (S17 5.3.3), System Administrators of IT system can be responsible for the day-to-day administration, operation and configuration of IT systems involving IoT devices, including security monitoring against threats. Also, system owner should have sought approval from DITSO before implementing IoT in B/Ds. Moreover, if the IT system involving IoT devices would be connected to departmental network, the System Administrators may designate the task of monitoring IoT devices to network or LAN Administrator of B/D who is responsible to oversee the overall security of the departmental network.

For handling classified data, B/Ds shall observe the Government security requirements (e.g. SR, S17, G3 and departmental IT Security Policy). For handling personal data, in addition to the Government security requirements, B/Ds shall also observe the local legal requirements (e.g. Personal Data (Privacy) Ordinance), overseas data protection acts or regulations (e.g. GDPR) if applicable.

For the protection of data in IoT operations or environment, B/Ds should consider to take holistic approach to safeguard the data against unauthorised or intentional logical and physical access, loss or theft, by means of administrative (e.g. departmental IT security policy and procedures), logical (e.g. encryption, access controls) or/and physical (e.g. located in a locked room) measures or controls based on their use cases and business environment as well as comply to government security requirements.

For the legislation or issues regarding personal data and privacy, please refer to Section 6 of this document – Personal Data Protection Consideration.

Security Review

Security Risk Assessment (SRA) and Security Audit (SA) for IoT related information systems (e.g. backend server/storage) or applications (e.g. mobile apps, web application) shall be conducted at the required intervals in accordance with the Government security requirements.

- Security Risk Assessment (SRA)

  SRA is a process to identify, analyse and evaluate the security risks, and determine the mitigation measures to reduce the risks to an acceptable level.

  Similar to traditional information systems and applications, SRA for IoT related information systems and production applications shall be performed at least once every two years, and shall also be performed before production, and prior to major enhancements and changes associated with these systems or applications. B/Ds

should ensure the identified risks of IoT system and application during SRA are properly assessed and addressed.

For IoT devices handling sensitive information and installed in public area, SRA shall be conducted to assess the security risks on the information systems and data assets and sufficient security controls shall be in place to safeguard the data, in particular measures against physical security.

In addition to SRA for information systems and applications, it could be adopted on other security aspects (e.g. IoT Infrastructure, connection between IoT components/layers, etc,) to review and assess the potential security risks. Thus, B/Ds should consider to make good use of SRA to discover and address the security issues in their business environment and operations. Besides, a professional who conduct SRA for IoT components should have solid experience in IoT operations and security practices.

- Security Audit (SA)

  SA is a process or event to verify the level of compliance with the security policy or standards as a basis to determine the overall state of the existing protection and to verify whether the existing protection is being performed properly.

  SA should be performed periodically by an auditor who has relevant and sufficient knowledge, skills and experience in IoT security operations, governance and compliance. B/Ds should ensure their IoT components are well protected and comply with the Government and departmental IT security policy.

For details on SRAA, please refer to the Practice Guide for Security Risk Assessment and Audit on ITG InfoStation
https://itginfo.ccgo.hksarg/content/itsecure/docs/Guidelines/DocRoadmap.shtml.

6. Personal Data Protection Consideration

IoT devices may collect, monitor or analyse various data in related to a person. B/Ds are advised to adopt "Privacy by Design" during system design phase to avoid excessive collection of personal data. B/Ds should inform users clearly the types of personal data to be collected, the purposes of collection, the potential transferees of the personal data, and the security measures adopted to protect the personal data.

B/Ds shall ensure compliance with the Personal Data (Privacy) Ordinance, particularly the Data Protection Principle 4 (on security of personal data), when handling personal data. B/Ds should also be aware of the possible impact of the regulatory frameworks in other economies such as General Data Protection Regulation (GDPR) published by European Union. Considerations for preventing personal data leakage, abusing, include but are not limited to:

- Minimise the collection of personal data.
- Adopt "Privacy by Default" for the IoT devices.
- Implement adequate security measures such as encrypting and transmitting personal data to secured backend storage, and enforcing strong passwords to prevent account hijacking.
- Perform de-identification or anonymisation for personal data if applicable.
- Destroy personal data securely when they are no longer necessary.

7. Use Cases of IoT Devices

IoT devices can be placed in vast and diversified areas. The location of the IoT devices to collect and process data is the key to its security as security controls, in particular physical security controls, are quite different in the office environment versus public areas. Another key is the classification of data involved. Before procurement, B/Ds should study the availability of security features of IoT devices from potential suppliers so as to pursue the most secure IoT features available in the market. IoT devices should avoid storing data, in particular sensitive data in the devices themselves. Data should be collected and passed to backend storage with proper security protection. To protect the information collected/processed/stored in the IoT devices, the relevant Government security regulation, policy and guidelines that have specific requirements for the protection of classified information should be followed.

In this document, we would discuss the following two use cases for IoT device deployment so as to provide some general guidelines on IoT security for B/Ds' consideration in different deployment scenarios.

I. IoT devices installed in public areas (Case I)
II. IoT devices installed in the office environment (Case II)

7.1 High-level IoT Reference Model

A high-level IoT reference model, which encompasses the two deployment cases mentioned above, is illustrated in the following diagram. Each deployment case would be elaborated in the following sections.

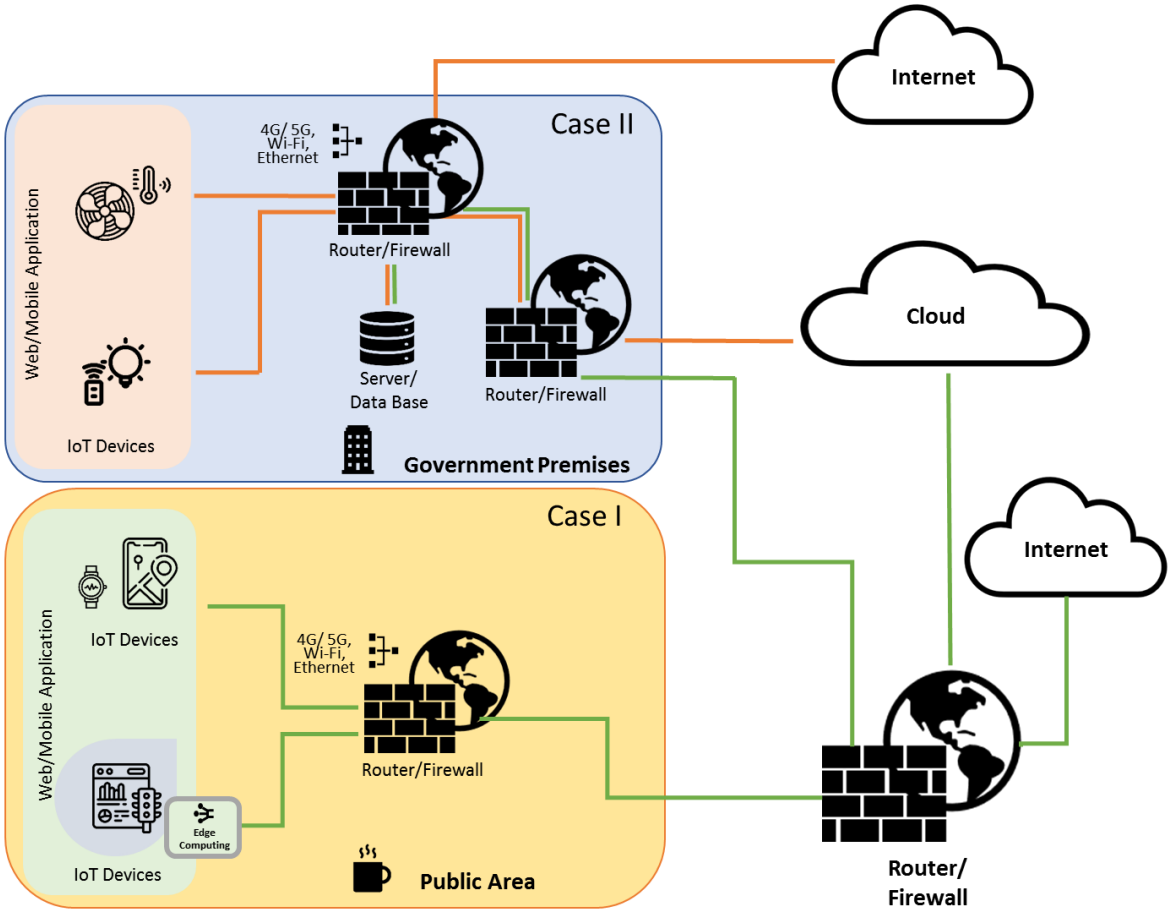

Figure 7.1 High-level IoT reference model

7.2 IoT Devices Installed in Public Areas (Case I)

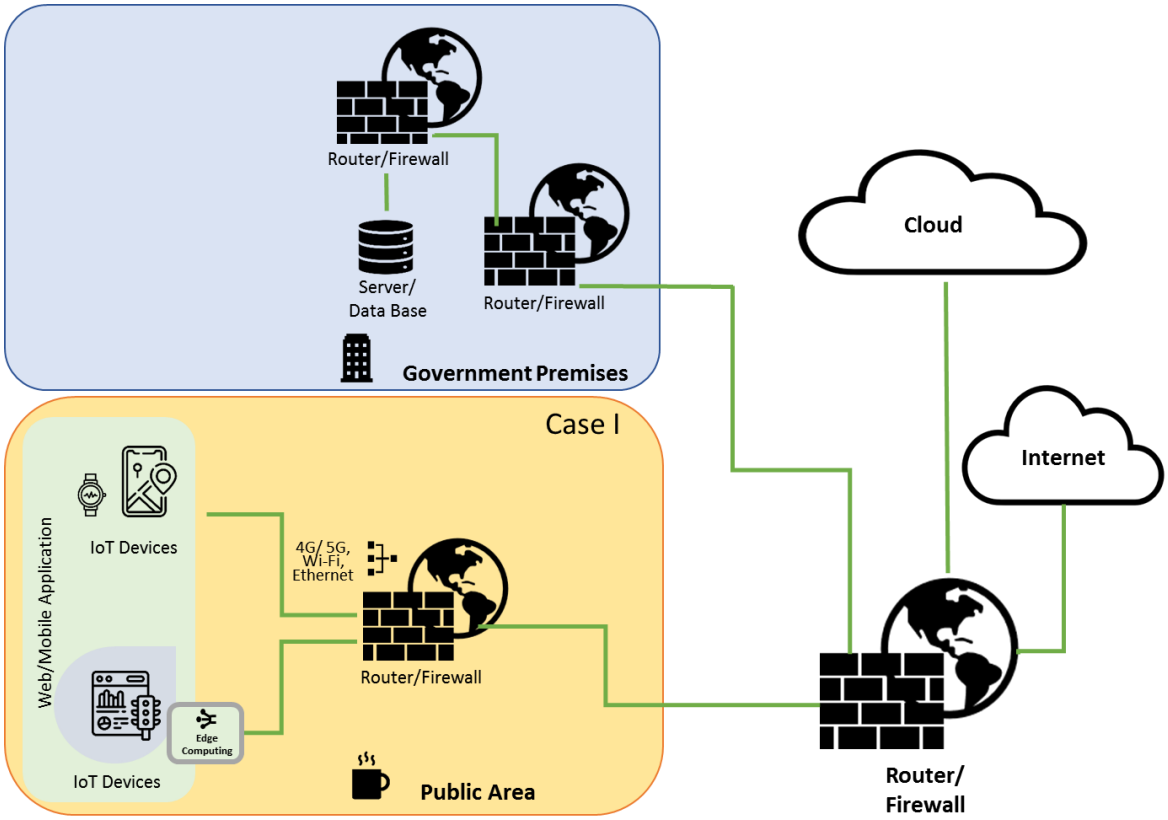

Figure 7.2 IoT deployment case I – in public areas

For Case I, the IoT devices are installed in public areas. They are interconnected or connected to a router to access the cloud or the Internet for service or data storage. The IoT devices may also indirectly connect to the government internal network via router, firewall or cloud.

As the amount of data being generated by such devices, especially IoT devices, grows very quickly, data, especially real-time data, may suffer latency issue that can affect the performance of an application. In some cases, edge computing is introduced to provide instant responses to action/data. Edge Computing is deployed to bring computation and data storage closer to the location where the edge devices, such as edge router, edge gateway or edge server, are being gathered and data is created to allow efficient data processing thus lower latency. Edge computing for IoT applications is getting more and more popular in the industry. The data processing, such as aggregation, replication and de-identification, and the general IoT functionalities, such as sensing and security management, may be able to benefit from edge computing to improve the level of service of IoT systems.

The edge computing plays an important role of security protection in IoT systems. Implementation of IDS/IPS on the edge devices can fend off possible attacks, such as DDoS, brute force attack, by further enhancing detection rate of attack and improving defence against malicious attempts to IoT infrastructure. Other security controls, such as data authentication, access control, patches update, prevention of cyber-attacks and so on, should be applied at the edge to comprehensively secure the IoT systems, as well as to ensure the data protection being maintained. The compliance of security requirements on the edge devices should be enforced.

As the IoT devices could be neither attended by staff nor installed in a physically secured area in this deployment case, the physical security protection cannot be guaranteed. In this case, B/Ds should avoid the collection of sensitive data. If it is unavoidable due to business needs, B/Ds should not store the sensitive data in IoT devices to mitigate the risks of data leakage. If storing of data is required, then the data should be encrypted and transmitted to the secured backend storage where security controls are commensurate with the relevant government security requirements. If it is unavoidable to store classified information in IoT devices without staff attended due to business needs, B/Ds shall implement proper physical protection with compensating measures such as data wiping, network disconnection when attempt of breaking-in of physical protection is detected and confirmed.

Also, a well-designed network is essential for securing the IoT-based system. The set of IoT devices should be grouped and segmented by a gateway with proper access controls. The IoT devices should never connect to internal network directly. The de-militarised zone (DMZ) should be configured to separate the internal network from the external one, and can hide the information about the internal network. Network segmentation should be enforced to mitigate the risks of security breach from IoT devices.

7.2.1 Security Recommendations for Application Interface

IoT-enabled solutions are usually built on common application interfaces, such as cloud, mobile or web platforms. These common applications form an IoT ecosystem. Any threats to the IoT ecosystem may result in compromise of the IoT devices or their related components. Common issues include lack of authentication/authorisation, lack of or weak encryption, etc. Some considerations on integrating with these application interfaces are recommended in the following sections.

Cloud interface

It is common to build IoT solution with cloud database, cloud storage platform and cloud services. In the adoption of IoT technology, security challenges are added up to what cloud already has, such as lack of visibility and controls, shared technology vulnerabilities as well as insecure interfaces. Security controls for securing IoT devices in cloud environment include but are not limited to the following:

- Ensure all cloud interfaces are reviewed for security vulnerabilities.
- Enable HTTPS whenever possible.
- Encrypt data stored in cloud and communication between cloud and other endpoints.
- Properly manage and protect cryptographic keys for their whole life cycle. Consider using Hardware Security Module (HSM) to protect encryption key operations when the stored data is considered sensitive.
- Adopt two-factor authentication option whenever possible.
- Enable web application firewall whenever possible.
- Change default password to a strong password if the system has a local or cloud-based web application; change the default username as well.
- Enable account lockout functionality.
- Enable strong passwords if provided.
- Enforce regular password change, e.g. after 90 days.

Mobile interface

IoT application is responsible for delivering application services. In most cases, users mainly interact with this application through the web application and mobile application to handle application data collection, processing, analytics, and storage. Mobile interfaces to IoT systems require targeted security, such as:

- Use a PIN or password for extra security (on client and server).
- Use two-factor authentication whenever possible.
- Enable account lockout functionality.
- Enable strong passwords if provided.
- Enforce regular password change, e.g. after 90 days.
- Encrypt communication with backend cloud applications or IoT devices.
- Do not enter sensitive information into the mobile application that is not absolutely required, e.g. address, date of birth, credit card, etc.
- Store sensitive data (e.g. personal data, user credentials, cryptographic keys, etc.) in secured storage with security controls conforming to the relevant government security requirements.

Web interface

Same as mobile application interface, the web interface is another major interface for users to interact with the IoT solutions. Web application is considered as one of the major attack surfaces that requires the implementation of effective security measures, such as:

- Enable HTTPS whenever possible.
- Use two-factor authentication whenever possible.
- Enable web application firewall if possible.
- Change default username and password.
- Enable strong passwords if provided.
- Enable account lockout functionality.
- Check against well-established web security standards to mitigate the risks.
- If the system has a local or cloud-based web application, ensure that the default password is changed to a strong one and if possible change the default username as well.
- If the system has account lockout functionality, ensure that it is enabled.
- Consider employing network segmentation technologies such as firewalls to isolate IoT systems from critical IT systems.
- Enable session timeout.

7.3 IoT Devices Installed in Office Environment (Case II)

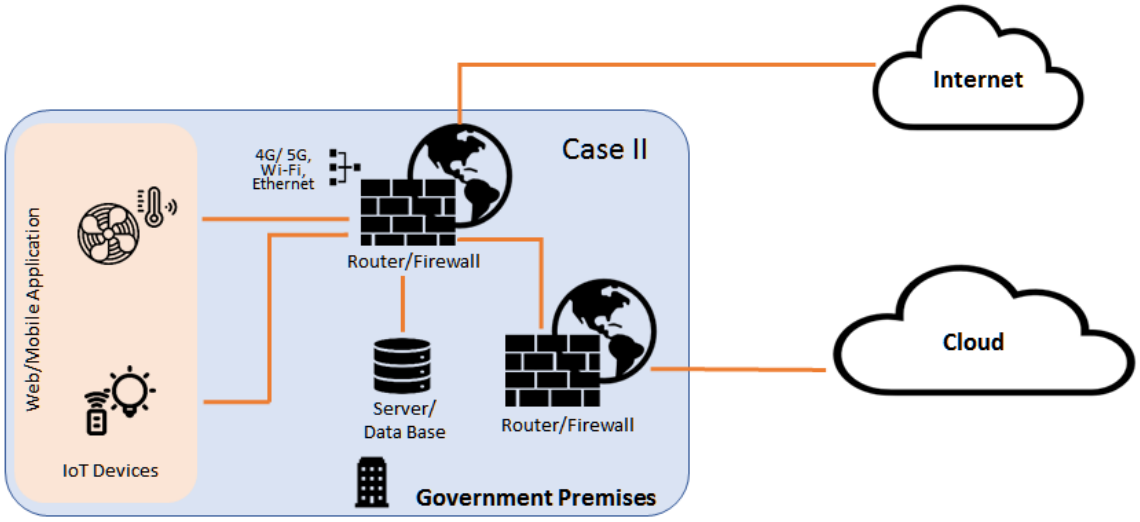

Figure 7.3 IoT deployment case II – in office environment

For case II, the IoT devices are deployed in office environment for supporting business operations. The IoT devices form an application that may or may not connect to the departmental network. The IoT devices may connect to cloud through firewall for data processing or storage. As the IoT devices are installed in office environment, they shall be protected to avoid collection of sensitive data or being compromised as a launching pad for attacking the internal network. Considerations for workstations and endpoints in the office environment should be applied, including but not limited to access controls, network segmentation, cryptographic protection, log management, device management such as applying security patch and firmware, malware detection and prevention as well as data protection in particular personal data.

From security point of view, the least functionality and privilege principles should be applied with protection mechanism against malware whenever possible. B/Ds need to assess the functionalities that are required, and disable any unnecessary functions and ports to avoid collection of sensitive information as well as connection to unauthorised devices or networks. If it is possible, white list the services/connections that are allowed. Due to certain similarity in IoT devices and mobile devices such as connectivity, mobility and small in size, the security requirements and principles for mobile devices laid out in the government security documents should be similarly applied to IoT devices in this case.

Moreover, as the IoT devices may not be attended even though in the office environment, physical security controls against loss, theft and damage should be implemented. Users should understand that their devices are only allowed to connect to approved networks and devices. Security of network connection in broadband or Wi-Fi should be ensured.

Similar to case I, B/Ds should avoid the collection of sensitive data. If it is unavoidable due to business needs, B/Ds should not store the sensitive data in IoT devices to mitigate the risks of data leakage. If storing of data is required, then the data should be encrypted and transmitted to secured backend storage where security controls are commensurate with the relevant government security requirements.

7.3.1 Sample Case for Deployment IoT Appliance

The following is an example to install an IoT appliance over Wi-Fi network connecting to the Internet without sensitive information involved. First of all, a holistic and defence-in-depth approach should be adopted. In general, the following three components should be considered:

- Broadband router
- Wi-Fi router
- Smart appliance

Broadband router

The broadband router resides between local network and the Internet, and it is the first line of defence against hackers, malware and viruses. At network level, B/Ds should ensure that the IoT appliance does not connect to office network and are advised to consider restricting all access to the local network (e.g. Wi-Fi network) at the Internet Gateway (e.g. broadband router). Apart from placing the broadband router in a secure area, it is recommended to properly configure and utilise the security features of the broadband router, including but not be limited to:

- Change factory default settings (e.g. username, password, SSID, etc.) and use strong passwords for the authentication.
- Keep firmware up-to-date and download the updated firmware from manufacturer website.
- Enable firewall functionalities.
- Enable MAC address filtering by limiting the devices that can join the network.
- Enable URL filtering to prevent users from accessing specific websites.
- Disable services/functions which introduce known security issues such as
    - WPS (Wi-Fi Protected Setup) that allows connection to the network without password.
    - Remote management.
    - Universal Plug and Play (UPnP) that allows automatic connection of unauthorised devices.
    - Unsecure protocols (Telnet, FTP, etc.).
    - Network services.
- Turn off SSID broadcast.
- Enable Denial-of-Service (DoS) protection and disable port scan service.
- Enable logging and conduct regular checking.

Wi-Fi router

B/Ds should note that the Wi-Fi network would be shared by other endpoints for broadband access. It would introduce security risks once an endpoint or smart appliance is infected. A malicious code would spread along and other endpoints would be infected within the same network. Thus, it is recommended to isolate the smart appliance from other endpoints in a network (e.g. guest Wi-Fi network) separated from departmental network which could be configured with separated SSID, authentication method, and allow only Internet access but not connection to the internal network. A separated network effectively prevents the spreading or mitigate or the impact of infection. Optionally, the separated Wi-Fi network for smart appliance, the SSID should not be broadcasted in order to reduce the attack surface to the smart appliance as well as the Wi-Fi network. Besides, it is also recommended using the latest Wi-Fi standard/protocol (e.g. Wi-Fi Protected Access 3 (WPA3)) with proper access control (e.g. authentication, strong password, etc.) for the Wi-Fi communication as WPA2 is discovered that it is vulnerable to KRACK (Key Reinstallation Attack).

Smart Appliance

For the protection of the endpoints (e.g. smart appliance), the least functionality and privilege principles could be applicable with protection mechanism against malware and physical security controls against loss, theft and damage implemented. If feasible, it is recommended to:

- Disable unused or unnecessary functionalities.
- Disable physical and logical ports or services (e.g. USB port, LAN port, Bluetooth, remote access to smart appliance from Internet, etc.).
- Keep the smart appliance up-to-date with the latest firmware and security patches for both operating system and installed Apps.
- Download and install authorised Apps from trusted the Apps Store.
- Allow only authorised devices connections to the smart appliance.
- Power off when not in use.
- Disconnect the Internet connectivity when not necessary

Finally, B/Ds are advised to perform a security risk assessment to identify, assess and evaluate the potential security risks (e.g. unauthorised accessing to the Wi-Fi network or smart appliance, malware spreading, displaying of unintended content) and impacts, then determine and implement the appropriate security measures and configurations based on the business needs so as to comply with the corresponding Government security requirements.

*** ENDS ***