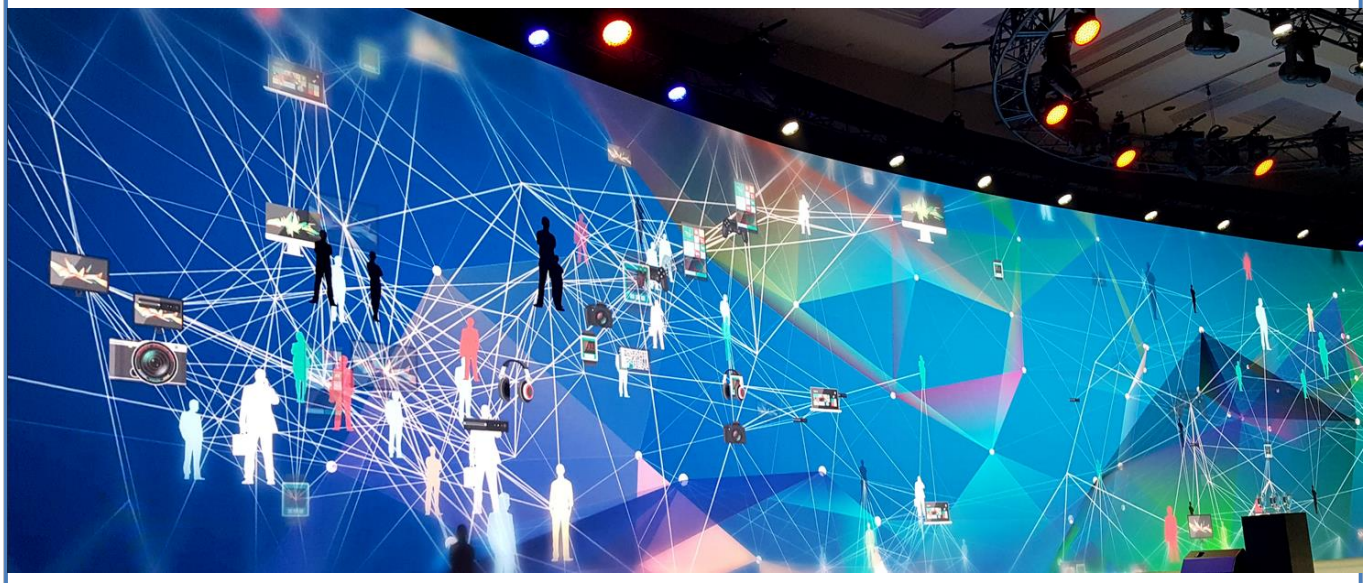
CSCSS CENTRE FOR STRATEGIC CYBERSPACE + SECURITY SCIENCE

INTERNET OF THINGS (IoT) SECURITY WHITEPAPER



Contents

Acknowledgements

This report was prepared by Christopher Lek, Ethan Chen, Henry Hu, Mickey Law and Wyatt Lee and members of the Centre for Strategic Cyberspace + Security Science (CSCSS) IoT Security Standard Development Technical Committee. Contributors were David Nordell and Richard Zaluski. Overall guidance was provided by Aloysius Cheang.

This work is a product of the staff and volunteers of CSCSS. The findings, interpretations, and conclusion expressed in this work do not necessarily reflect the views of the donors of the CSCSS or its Board of Directors.

The whitepaper benefitted from close partnership and extensive discussion with staff of the iSyncGroup Inc. that had provided the initial draft of this whitepaper.

In addition, we would like to thank The Association of Information Security Professionals (AISP) in Singapore for the strong support and extensive discussion that made this whitepaper possible.

Executive Summary

Smart cities, connected worlds and a sea of data. The Internet of Things (IoT) is a game changer, with the interconnection of computing devices enabling new possibilities in automation and the management of resources. From cities where electronic devices are used to monitor consumption, reduce costs and interface between citizens and government, to stores that send notifications to restock when low on a product, the applications of IoT are immense. However, the IoT also poses new risks in privacy, data governance and cybersecurity. It may even change the current trust model that we are so familiar with!

There are three key reasons why IoT has the potential to become the largest security threat that we are seeing in the past two decades. Firstly, when smart cities/nation projects were first conceptualized, IoT was never a major part of the design. It was not even considered as a basic building block for designing smart cities/nation. Must smart cities/nations are designed with the aim to convert all services into electronic format, to build a fully e-government, with the aim to digitise as many services as possible, including contracts and payment. In the event that sensors are used, these sensors are not treated as full computing devices that can not only collect data, but also input and process requests to manipulate data collected in these sensors or the entire systems of sensors as well!

Secondly, the proliferation of consumer IoT devices is happening at an alarming speed. In the Internet era, Moore's Law is obviously inadequate to address security issues brought about by emerging technology trends. In the effort to automate most processes and to alleviate the human effort, people embrace technology and all the "smart" devices, especially home automation. These "smart" IoT devices are often designed without security in mind. It is not uncommon to find IoT devices without even basic access control management features such as having a log in name and password. This was the primary reason behind the Mirai botnet attack in 2016 that brought down the global Internet with less than 500,000 IoT devices (mainly IP cameras), either with no access control or protected by simple default passwords.

Thirdly, even when security is included in the design of the IoT devices, the design of the security controls is not consistent and does not adhere to any widely recognized and adopted security best practices. The security process are not sustainable and repeatable to the extent that basic assurance that the security can be managed and measurable. This will prove to be challenging within an environment with many disparate IoT devices, each with a different security design This also makes building a dashboard view managing all the IoT devices extremely difficult, and as a result the managers and users of IoT-enabled systems cannot establish a common baseline of security cannot be established, and it will be extremely difficult to monitor, share and react to IoT specific security threats and incidents in the most effective and efficient manner. Take for example, in a larger scheme of things, a smart city. In a smart city, the entire city is wired together, bringing systems of different complexity and severity of damage when the system is compromised, for instance industry control systems that run the power stations to that smart street lights with surveillance cameras to smart interconnect cars. If one is running a smart city, one would prefer to have a dashboard view of all these "assets", their "health status" and how to manage any security risk down to a baseline of security and operations, for example, whether different part of the systems can be cut off or to the extent, a complete shutdown as a last resort is possible and the problem containable. As such it helps to have a basic security control set baked into any IoT devices that can be tested and certifiable against a commonly accepted IoT security standard, especially if these are secured by design by the designers and manufacturers of IoT devices and solutions.

Thus, this is the focus for Centre for Strategic Cyber Space and Security Science (CSCSS) Internet of Things Security Framework, which aims to address trusted IoT ecosystem all the privacy, governance, risk and compliance as well as security issues brought about by any IoT devices, through a well-defined IoT security framework. In this paper, we have focused on key IoT components identified - the edge clients, the gateways and the cloud. Through this whitepaper, our intention is to bring all the IoT device design manufacturers and IoT fabrication facilities to a set of common technical and policy standards, providing clear and precise guidelines. In addition, with this whitepaper, users and solution providers can build from this framework, a managed and measurable process to test and certify IoT devices and solutions that gain trust of the general public.

1. Introduction

Internet of Things (IoT) technology has grown rapidly around the world in the past years. The growth will continue, and it is expected to have billions of IoT devices installed and operate by 2025.

IoT enables anything that is embedded with electronics, software, sensors, actuators, and connectivity to interact with each other. Devices within the IoT network are able to communicate and interact over the internet, and can be remotely monitored and controlled. For example, we can monitor our pets at home from office via an IoT enabled webcam. Although IoT devices make life easier and simpler, the convenience also has brought along new security challenges. The lack of trust on the IoT security becomes a huge barrier for IoT adoption.

IoT vulnerabilities were introduced by uncertainty and negligence on IoT devices during the design, deployment, maintenance and usage of the devices. A well-defined IoT security framework is required to educate both the IoT device developers and users, as well as providing necessary recommendations and best practices for the development and application of IoT.

1.1. Purpose and Scope

The Centre for Strategic Cyber Space and Security Science (CSCSS) Internet of Things (IoT) Security Framework described in this whitepaper aims to define processes and standards for secure IoT infrastructure usage and development. This whitepaper will help to strengthen the security of IoT by making technical and policy recommendations and developing best practices for the design, deployment, maintenance and usage of IoT devices.

Due to the complexity of the IoT architecture, it is not ideal to include all security issues related to each architecture in the world in the framework. Instead, this framework focus on the most common core components of the IoT architecture, which are: Edge Clients, Gateway and Cloud.

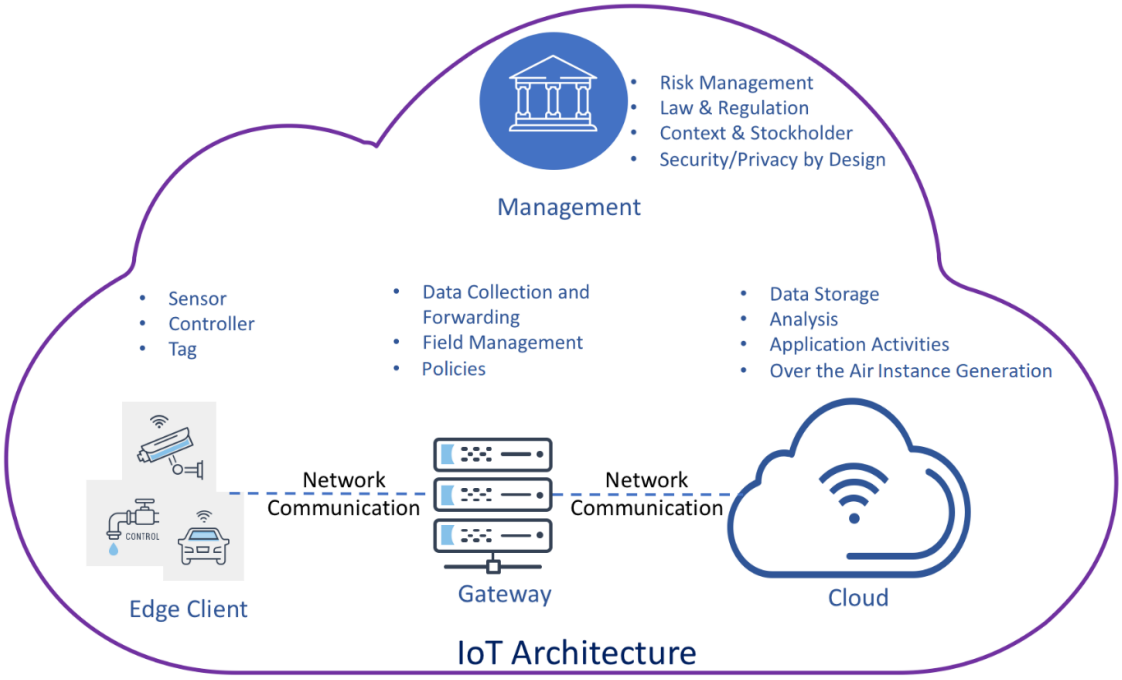


Figure 1 IoT Architecture

Common use cases of the core IoT components:

- **Edge Clients**[1] senses and collects data, then send the collected data to the **Gateway**.
- **Gateway** acknowledges and confirms the reception of the data with **Edge Client**, then perform identification on the data before sending it to the **Cloud**.
- **Cloud** receives the data from **Gateway**, then saves the data into its storage. After analyzing the data, output will be broadcasted to the **Edge Clients** through **Gateway**.

As IoT ecosystem consists of various IoT devices and cloud services from different vendors to collect data, preprocess data or filter data. Security issues might not be produced by only one type of IoT component but in fact, might cause by the poor design of the an entire IoT or through the technical incompatibility of two or more IoT components. As such, the design of IoT architecture should also be taken into account while evaluating the security of an IoT ecosystem. On the other hand, IoT ecosystem management issues such as risk management, law & regulation and security/privacy by design should also be considered throughout the whole IoT development lifecycle as well as during the adoption of IoT.

[1] Edge clients are IoT devices that are commonly installed or used in the client environment. For example, sensor or IP camera.

1.2. Market Need

The overarching purpose of this whitepaper is to make it possible for new IoT-enabled products and services to enter the market and meet the needs of both industrial and consumer users with the minimum possible risk. This obviously requires high levels of security at every level in order to create trust and reduce possible harm; but these high levels of security must be anchored in security standards that are definable, practicable and compatible with each other across entire supply and value chains, and where it is possible to measure and enforce compliance. Specifically, these security standards must answer the following market needs:

1. Governments and other large users and providers of IoT systems need to be able to rely on clear minimal standards of IoT security when sourcing and purchasing technology. There is currently a proposed law in the US Congress, the 'Internet of Things Cybersecurity Improvement Act,' that requires all IoT devices to be free of known security vulnerabilities and to be patchable in order to protect them from future attacks.
2. Clear standards will make it easier for both providers and users to deal with product liability issues that will inevitably arise as IoT become increasingly ubiquitous.
3. Clear standards will also make it easier for the insurance industry to provide suitable and unambiguous cover against both malicious attack on IoT-based systems and failures caused by negligence.

1.3. Normative References

ENISA Baseline Security Recommendations for IoT [1]

NIST Federal Information Processing Standards Publication 140-2: Security Requirements for Cryptographic Modules [2]

OWASP Internet of Things Top Ten [3]

1.4. Structure of this Paper

This whitepaper covers four major chapters.

Chapter 1 introduces purpose and scope; normative references; and outlines the structure of this whitepaper.

Chapter 2 examines the key security challenges that are associated with IoT technology.

Chapter 3 discusses the CSCSS IoT security requirements and provides recommendations to the development and adoption of IoT.

Chapter 4 provides mapping for the use of CSCSS IoT security requirements on edge clients, gateway and cloud. It also lists out the IoT security controls related to each of the IoT security requirements.

2. Internet of Things Security Challenges

With the rapid growth of IoT, new IoT vertical domains such as Industrial Internet of Things (IIoT), Internet of Medical (IoM) and Internet of Agriculture (IoA) emerge as a part of integration of IoT ecosystem. As the subcategories of IoT, each of these verticals utilize similar Edge clients – Gateway – Cloud architecture. Although IoT brings opportunities to innovation such as connectivity and data collection for big data analytics to the industries, but at the same time, introduces new security threats to the environment as well. Such integrations might not be able to fulfil the regulations or standards of the security compliance, and thus slow down the adoption of IoT throughout the industries.

CSCSS has identified 8 common IoT security challenges that has emerged during the adoption and integration of IoT, which includes the following:

1. Privacy: IoT devices are instrumental in collection and analysis of sensitive data. These devices might not be secured enough to protect the users against security incidents such as data leakage.
2. Vulnerability: Due to the massive network connectivity generated by IoT devices, if one of the nodes is vulnerable to malicious attack, attackers might take advantage over the weakest link and attack the IoT network through the vulnerable node.
3. Mobile Devices: Mobile devices are becoming an indivisible part of our life and is often connected to the IoT network. These mobile devices are often used in checking or verifying the operation of the IoT network through it's own application and connectivity to the cloud infrastructure. Others could participate as part of the sensor network in the data collection process. These mobile devices, if not properly secured, could become a new attack vectors to the IoT network.
4. IoT Architecture: An IoT network consists of numerous IoT nodes which can be sensors, gateways or mobile devices. With the increasing number of nodes being connected to the IoT network, the chance of having a vulnerable node or malicious node within the network also increases.
5. Hardware Security: Hardware security is often neglected during the development of IoT devices. The IoT devices becomes vulnerable if security mechanisms against hardware attacks such as physical intrusion or physical tapping of these devices are not in place.
6. IoT Networking: Being remote controllable is often a key feature of IoT products. If network security mechanisms such as authentication is absent on the IoT device, malicious attacks can simply perform a remote attack toward the IoT network and gain access to multiple IoT devices or eventually other segments of the network.
7. System Upgrade/Update: System upgrade or update are common features for IoT devices. Without a strong authentication and verification mechanism, malicious users can leverage the system update/upgrade interface to control the software, hardware or firmware of the IoT devices.
8. Data Transmission: Distances between the IoT nodes varies. They can be next to each other, or they can be installed in different continents. As data transmissions between IoT nodes usually rely on wireless connections, without sound authentication and identification mechanism, or even a secured network infrastructure for the data transmission, security incidents such as data leakage may occur.

The above eight IoT security challenges are the most common and critical security challenges associated with IoT. If they have not been considered during the development IoT, the IoT

ecosystem will become vulnerable if more and more vulnerable IoT devices start to kick in. As such, CSCSS develops this whitepaper to provide recommendations and best practices for IoT developers.

The next section talks about the security requirements that are necessary to create a more secure IoT ecosystem.

3. CSCSS Internet of Things Security Requirements

Considering the security challenges associated with the IoT devices, such as unauthorized access and signal jamming, security recommendations and best practices on IoT are necessary to help secure the IoT ecosystem, as well as building trust on IoT utilization. As mentioned in the previous section, this whitepaper not only focuses security issues related to the development of IoT devices but also the application of IoT devices. IoT security incidents are not only caused by poorly designed IoT devices, but often, by the negligence on overall IoT infrastructure security from the IoT users.

Through outlining security requirements associated with IoT, CSCSS aims to provide recommendations and best practices for IoT development. It is also important to educate the IoT users on the security requirements of their IoT devices and how they can utilize the security mechanisms to have a more secured IoT experience.

CSCSS has identified 21 IoT security requirements and they can be categorized into 6 different categories, which are: general security, physical security, system security, communication security, authentication and authorization security, and privacy protection. Below is a list of the requirements:

3.1. General Security Requirements

3.1.1. Security by design

Consider the security of the whole IoT system from a consistent and holistic approach during its whole lifecycle across all levels of device/application design and development, integrating different security policies and techniques and design architecture by compartments to encapsulate elements in case of attacks throughout the development, manufacture, and deployment.

For IoT hardware manufacturers and IoT software developers it is necessary to implement test plans to verify whether the product performs as it is expected. Penetration tests help to identify malformed input handling, authentication bypass attempts and overall security posture.

Furthermore, human safety should be considered together with cyber security in mentioned lifecycle and designing for power conservation so as to ensure security will not be compromised.

3.1.2. Risk and Threat Identification and Assessment

A defense in depth approach to identify significant risk among the IoT ecosystem needs to be adopted. This include identifying the key network/information systems and the intended use/environment of a given IoT device within the IoT ecosystem.

3.1.3. Management of Security Vulnerabilities and Incidents

Establish procedures for analyzing and handling security incidents and participate in information-sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.

Based on the mentioned information-sharing platforms, create and coordinate and a publicly disclosed mechanism for vulnerability reports.

3.1.4 Third-Party relationships

It is necessary for IoT hardware manufacturers and IoT software developers to adopt cybersecurity supply chain risk management policies and communicate the cyber security requirements to their suppliers and partners.

All data processed by a third-party must be protected by a data processing agreement, especially when personal data of consumer sharing is involved. Developer should only share personal data of consumer with third parties with express consent of the consumers, unless otherwise required and limited for the use of product features or service operations.

3.1.5. Cryptographic Management

Proper and scalable management mechanism and requirements should be implemented and enforced for cryptographic key generation, exchange, storage, usage, replace and discard.

Adopt well known cryptographic algorithms that are well recognized by the scientific community instead of proprietary or custom cryptographic algorithms for data process and communication.

3.1.6. Assessment of Impacts on Sensitive Information

Privacy impact assessments should be conducted before launching of any new developments and sensitive information should be identified and classified according to local laws during the development of IoT.

3.2. Physical Security Requirements

3.2.1. Physical Interface

IoT devices are not usually equipped with physical user interface as the requirement of user interaction is very limited. The physical ports on the devices are generally designed for debugging, providing connection to power source and network, entering engineering mode. Protection mechanism should be implemented against unauthorized access to firmware and operating system. If protection mechanism implementation is not possible, intrusion detection mechanism should be implemented.

A physical ‘reset’ button on the device or another physical buttons on the device should be implemented to trigger to ‘reset’ function which will be discussed in 3.1.2.. Security mechanisms should be in place to prevent users from accidently pressing or unauthorized personnel on pressing the reset button. Such mechanisms can be having the ‘reset’ button ‘inside’ the device where it can only be reached after the device is dissembled or its cover is taken off. More secure mechanisms such as triggering the function only after the button is pressed for a period of time, or when a combination of different physical buttons is pressed at the same time should also be considered for restoring the devices to factory default settings.

3.2.2. Physical Layer

In most cases, IoT devices are installed in an unattended environment to function as sensors, monitors or data collectors. IoT devices should be protected against attacks such as physical damaging, signal jamming and signal interferences.

An IoT device should be setup by authorized personnel. The authorized personnel should input the basic parameters to the device and store them in the device’s built-in memory.

A ‘reset’ function should also be implemented for debugging, recycling and redeployment purposes. The function can either be triggered with a physical ‘reset’ button on the device or with another physical buttons on the device.

3.3. System Security Requirements

3.3.1. Operating System

Operating System is the core of IoT devices. Basic tasks such as memory management and configuration, system resource supply and demand prioritization, input and output control, network operation and file system management are all handled by the operating system. A user interface for the users to interact with the IoT devices can also be found in the operating system. Operating system is mostly embedded in the firmware stored in the flash memory, EEPROM, or PROM, within the application integrated circuit or programmable logic device. Functional or security updates can be performed through either internet or physical connection port.

Similar to operating systems on the other platforms (i.e. personal computers or networking devices), IoT operating systems may have flaws in design and are vulnerable to attacks such as privilege escalation attack and injection attack.

To manually update IoT device firmware, users are required to obtain the firmware themselves. Usually this can be done by downloading the firmware from the manufacturer official website. However malicious parties might modify the firmware to include malicious backdoor. They could advertise the firmware as a better version of the original firmware and lure the IoT users to download it.

Malicious application is also a security threat to IoT operation systems. Since most IoT devices run with single-chip computing architecture, anti-virus software that is designed for various platforms such as personal computer cannot be installed onto the devices. As such, malicious applications can easily be installed onto the devices and disrupt the operation of IoT services. Security mechanism against malicious code execution should be in place to protect IoT devices from malicious application. Such mechanisms can be whitelisting and verification using encrypted chips.

3.3.2. Sensitive Data Storage

IoT edge clients such as sensors are often being used to collect information such as images, sounds, motions and geographical information. More sensitive information such as heart rate, blood pressure, and blood glucose measures are often being collected via edge clients for medical purposes. These data are temporary stored in a specific data storage within the edge client for pre-processing purposes or act as a backup to prevent data loss if transmission of such data is being interrupted. Due to the sensitive nature of the data, security mechanisms such as encryption or privilege control should be implemented.

3.3.3. Web-Based Management Interface

IoT devices are often appear as a micro device or installed at a location that is not easy to be reached. Device management can be done through a web-based management interface provided by the devices. It is known that web has the most security issues since the invention of internet, including injection, cross-site scripting (XSS) and man-in-the-middle attack. Malicious users can utilize these attacks to obtain the highest level of authorization through the web-based management interface. Thus, gain control over the IoT device or leak the information collected by the IoT device.

Security of web-based management interface should be considered during the IoT development life cycle. It is important to make sure security mechanism is in place during the design of the IoT and penetration testing against the interface is performed.

3.3.4. Application Programming Interface

An Application Programming Interface (API) is the convention for connecting different components of a software system. Using the API to quickly integrate without system applications can simplify and accelerate the formation of IoT ecosystem.

Third-party API or library (LIB) are often used in IoT development. These API and LIB are “black boxes” to the developers as they cannot verify the security of the API and LIB through their source code. Developers should use API or LIB that are verified and code signed by the IoT manufacturers.

3.3.5. System Logging

The system log is used to record device system changes, such as settings changes, system errors, data file changes, and security incident auditing. It can also be used for system debugging, data recovery, or security incident investigation.

As security incident investigators use system log to understand the nature of security incidents, the completeness and accuracy must not be tampered. This can be achieved by enforcing security mechanism such as cryptography and privilege control on the system log.

Another consideration is that the built-in storage of IoT devices is very limited. Developers can consider using compression, backup and uploading the log to another location, depending of the regulation, security risk, storage life span and cost.

3.4. Communication Security Requirements

3.4.1. Network Port

A network port is a logical construct that identifies a type of network service. Edge clients can establish connection with the server (i.e. IoT gateway) for specific services with corresponding IP address and port number. Typically, there are two types of communications in IoT: communication between edge clients and gateway, and communication between gateway and cloud. IoT developers should choose a suitable network port for the IoT connections, such as ports that are not commonly used by network services (i.e. TCP 80/443). On the other hand, only enable ports that are required for the functionalities of IoT to prevent malicious attacks such as guessing, eavesdropping and service interruption.

3.4.2. Sensitive Data Transmission

Sensitive data might be collected or transmitted in the IoT ecosystem. To protect the security and privacy of the data owner, security mechanism should be implemented with reference to applicable regulations and guidelines. Also, transmission channel that is not known by unauthorized parties should be used for transmission of personally identifiable information (PII) or confidential information. Encryption should also be used to further protect the security of such information.

3.4.3. Communication Interface

IoT user should have the ability to enable/disable the connectivity of their devices. For example, if the user only uses Wi-Fi for IoT connection, he/she should be able to disable other functions such as Bluetooth and near-field communication. By disabling unused connection channel, it reduces the attack vectors for the malicious users to take advantage on. Encrypted communication and user authentication should also be considered to further protect the security of user-edge clients communication.

3.4.4. Communication Protocol

Various communication protocols are used between the IoT devices, services and users for different purposes. IoT developers should consider the maintainability and security of the protocols before adopting them into the design. For example, the developers can check rather the protocols have known vulnerabilities and their capabilities on mitigating attacks.

3.5. Authentication and Authorization Requirements

3.5.1. Authentication

Authentication is the function of verifying the identity of a user. To prevent unauthorized access, authentication should be used during the communication between IoT edge clients, gateway and cloud. Multifactor authentication should also be considered to further improve the strength of the authentication mechanism.

3.5.2. Password

The use of password is the most common method for user authentication to prove identity. Mechanism such as complex composition rules, forcing password changes after certain period of time and limiting number of password guesses should be implemented to increase the security of the passcode.

Mirai malware was one noticeable attack that utilized IoT devices with default username and password pairs to create a botnet for distributed denial of service (DDoS) attacks. During the incident, Dyn, a DNS service provider was the target of the botnet created by IoT devices with Mirai malware installed. As the result, several high-profile websites from various fortune 500 companies were inaccessible for more than 6 hours in the 3-waves DDoS attack.

3.5.3. Authorization

Authorization is the function of specifying access right/privileges to resources. IoT users and devices should be given access to resources or IoT devices following the principle of least privilege. When designing the IoT, developers should consider the interaction between devices and devices, and users and devices to assign proper authorization to the user or devices.

3.6. Privacy Protection Requirements

3.6.1. Assessment of Sensitive Information

Privacy should be taken into account throughout the entire development process. The following are design strategies that are related to sensitive data access and protection from “Privacy and Data Protection by Design – from policy to engineering” by European Union Agency for Network and Information Security (ENISA) [1]:

Minimize: The amount of personal data that is processed should be restricted to the minimal amount possible.

Hide: Personal data, and their interrelationships, should be hidden from plain view.

Separate: Personal data should be processed in a distributed fashion, in separate compartments whenever possible.

Authentication and authorization recommendation mentioned in the previous subsections should also be used to protect the privacy of IoT users.

The above 21 security requirements are commonly found in the IoT ecosystem. General security, physical security, system security, communication security, authentication and authorization, and privacy protection should be considered in the development and usage of IoT. Any negligence on such requirements may result in security incidents such as data leakage, or even causing a systemwide crash. In the next chapter, it includes the CSCSS IoT security requirements mapping on the 3 core IoT components: edge client, gateway and cloud.

4. CSCSS Internet of Things Security Requirements Mapping

Due to the nature of each core IoT components, security requirements that are mentioned in chapter 4 might not be applicable for each of them. In this chapter, it includes the mapping of each security requirements against the core IoT components which are edge client, gateway and cloud. Below is a table (Table 1) of applicability for the security requirements with the core IoT components.

Table 1 Applicability of security requirements

Component Category	Security Requirement	Manage-ment	Archi-tecture	IoT Components		
				Edge Client	Gateway	Cloud
General Security	Security by Design	O	O	O	O	O
	Risk and Threat Identification and Assessment	O	O	O	O	O
	Management of Security Vulnerabilities and Incidents	O	O	N/A	N/A	N/A
	Third-Party Relationships	O	N/A	N/A	N/A	N/A
	Assessment of Impacts on Sensitive Information	O	N/A	N/A	N/A	N/A
	Cryptographic Management	N/A	O	O	O	O
Physical Security	Physical Interface	N/A	N/A	O	O	N/A
	Physical Layer	N/A	N/A	O	O	N/A
System Security	Operating System	N/A	N/A	O	O	N/A
	Sensitive Data Storage	N/A	N/A	O	O	O
	Web-Based Management Interface	N/A	N/A	O	O	O
	Application Programming Interface	N/A	N/A	O	O	O
	System Logging	N/A	N/A	O	O	N/A
Communicatio-n Security	Network Port	N/A	N/A	O	O	N/A
	Sensitive Data Transmission	N/A	N/A	O	O	O
	Communication Interface	N/A	N/A	O	O	N/A

	Communication Protocol	N/A	N/A	○	○	○
Authentication and Authorization	Authentication	N/A	N/A	○	○	○
	Password	N/A	N/A	○	○	○
	Authorization	N/A	N/A	○	○	○
Privacy Protection	Assessment of Sensitive Information	○	○	○	○	○

Applicable：○ Non-applicable：N/A

The next six sections list out the CSCSS IoT security controls which are categorized under the 6 requirements.

4.1. General Security

4.1.1. Security by Design

MP-A01 Security by design

Manufacturer should have a stringent security by design procedure for firmware, driver and operating system components development. Security tests should be performed before the release of each update patches. Manufacturer should also have proper notification procedure to notify the users on updating their IoT devices.

4.1.2. Risk and Threat Identification and Assessment

MP-A02 Conducting risk and threat assessments

Risk assessments which include the following specific tasks should be conducted:

I. Identify threat sources that are relevant to IoT ecosystem/environment or components within;
II. Identify threat events that could be produced by those sources;
III. Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation;
IV. Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful;
V. Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events); and
VI. Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.

MP-A03 Development of action plan

Based on the risk and threat assessed/identified, organization should develop a risk treatment strategy and action plan including: (i) proposed actions, priorities or time plans (ii) resource requirements (iii) roles and responsibilities of all parties involved in the proposed actions (iv) performance measures (v) reporting and monitoring requirements

4.1.3. Management of Security Vulnerabilities and Incidents

MP-A04 Establish procedures for responding security incidents

Procedures should be established for (i) Detection and analysis incident (ii) Containment, eradication, and recovery from an incident (iii) Post-Incident Activity of an incident.

MP-A05 Vulnerability Report and Disclosure via information-sharing platforms

Developers should participate in information-sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.

MP-A06 Create and maintain public vulnerability report channels

Create a publicly disclosed mechanism for vulnerability reports, such as Security escalation channels or Bug Bounty programs.

4.1.4. Third-Party relationships

MP-A07 Data process outsourcing

Data processed by a third-party must be protected by a data processing agreement.

MP-A08 Supply chain cybersecurity management strategy.

Security requirements and supply chain security management strategy should be implemented and communicated to suppliers and partners. The strategy should include (i) Security governance (ii) Security in manufacturing and operations (iii) Asset management (iv) Security incident management.

MP-A09 Share personal data of consumers with third parties

Only share personal data of consumers with third parties with express consent of the consumers, unless otherwise required and limited for the use of product features or service operations.

4.1.5. Assessment of Impacts on Sensitive Information

MP-A10 Identify sensitive data

Identify sensitive data according to the operating environment.

MP-A11 Identify local regulations

Identify regulations of countries that are involved in the sensitive data transmission.

MP-A12 Privacy by design

Privacy by design should be implemented. Privacy should be taken into account throughout the entire development process.

4.1.6. Cryptographic Management

AP-B01 Key management

Proper management mechanism and requirements should be implemented for cryptographic key generation, exchange, storage, usage, replace and discard.

4.2. Physical Security

4.2.1. Physical Interface

TC-C01 Physical port safety control

To prevent unauthorized access via physical port to operating system.

TC-C02 Plug and unplug alert

To help detecting and alerting unauthorized access, during the event of plugging or unplugging physical port, alert should be issued or the event should be logged for audit purpose.

TC-C03 Reset Button Protection

There should be physical protection mechanism to prevent reset button from unauthorized access.

4.2.2. Physical Layer

TC-C04 Anomaly detection

Device should have the capability to create event log or alert when anomaly events such as sensing components, accessory component, ethernet port, wireless network antennas and power cable disconnection, or bad signaling occur.

TC-C05 Device destruction and disassembly

Physical security mechanism should be implemented to protect the device from easily destroyed or disassembled. The mechanism should also protect the data storage medium from easily removed.

TC-C06 Environmental factors

Natural disasters or accidental factors in the installation location, such as earthquakes, fires, floods, winds, abnormal temperature and humidity should be considered. Appropriate material and design should be used to protect device from failure or reduced performance caused by environmental factors.

4.3. System Security

4.3.1. Operating System

TC-D01 Firmware version

The firmware, driver and operating system components version should be verified during system boot.

TC-D02 Secure boot

Completeness of firmware, driver and operating system components version should be checked during system boot. Secure boot can be implemented with encryption module to ensure that the system is not tampered.

TC-D03 Trustable runtime environment

Secure boot on firmware, drivers and components should be confirmed before any trust is claimed in any other software or executable program.

TC-D04 Tamper protection and detection

Security mechanism should be implemented to detect and react to firmware tampering. Notification should be sent to the operator and the mechanism should interrupt system operation or restore the firmware to a secure version.

TC-D05 Security and patch support

A product lifecycle should be defined and disclosed. The lifecycle should include the duration and end-of-life security and patch support. During the period of a product lifecycle, the device should be monitored and patched against known vulnerabilities until the “end-of-support’ period.

TC-D06 Secure offline update

Authorization certificate or encrypted channel should be used if IoT operating system utilize intranet or offline for updates. Security mechanism should be designed and implemented to ensure the completeness and correctness of the firmware, drivers and operating system components.

TC-D07 Secure online update

Authorization certificate or encrypted channel should be used if IoT operating system utilize internet (remote) for updates. Security mechanism should be designed and implemented to ensure the completeness and correctness of the firmware, drivers and operating system components.

TC-D08 Updates backward compatibility

Firmware updates should not modify user-configured preferences, security, and/or privacy settings without user notification.

TC-D09 Change Log

Firmware, driver and operating system components update should be logged in the change log. The device should have the capability to record at least 10 records.

TC-D10 Secure system restoration

The operating system should have mechanism to restore the firmware, drivers, operating system to a stable version during system update.

TC-D11 Prevent access to debug mode

The operating system should have mechanism to prevent user from entering operating system debug mode via direct connection ports or internet.

TC-D12 Secure whitelisting

The operating system should use whitelisting mechanism on applications and core components to prevent unauthorized application operating in the system.

TC-D13 Code signed system components

Code signing and whitelisting mechanism should be implemented to ensure system components and code execution will not be tampered or overwritten after they are loaded.

TC-D14 Secure configuration

Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default.

TC-D15 System resilience

Physical impact of the system, such as external force, power surge or low voltage, instantaneous power failure and other abnormal conditions should be considered during the design. Mechanism should be implemented to maintain the system integrity and functionality after recovering to normal operating environment.

TC-D16 Auto recovery

Self-diagnosis and self-repair/healing mechanism should be implemented to recover the system from failure, malfunction or a compromised state.

TC-D17 Standalone operation

The device should maintain operational and temporary store of undelivered data even with connection lost or chronicle negative impacts from compromised devices.

4.3.2. Sensitive Data Storage

TC-D18 Secure storage

A secure storage that complies with The Federal Information Processing Standard (FIPS) Publication 140-2 cryptographic modules should be designed and implemented for the storage of sensitive data.

TC-D19 Privilege control

Privilege control mechanism should be implemented for the secure storage.

TC-D20 Data encryption

Advanced Encryption Standard (AES) 256 bits or other cryptographic algorithms that have same level of encryption strength should be used to protect the sensitive before it is stored in the secure storage. Lightweight encryption and security techniques can be used to lower the power consumption or if the device has limited computational resources.

TC-D21 Data segmentation

Different storage segmentations should be implemented for the storage of common data and sensitive data.

4.3.3. Web-Based Management Interface

TC-D22 Web vulnerability mitigation

Web-based management interface should not be vulnerable to injection and cross site scripting attacks.

TC-D23 Transmission encryption

Security mechanism should be implemented for remote web-based management interface setting with reference to requirements in TC-E03 – TC-E12.

TC-D24 Identity authentication

Identity authentication mechanism should be implemented for access to web-based management interface with reference to TC-F01 – TC-F12. Multifactor authentication should be implemented for critical infrastructure.

4.3.4. Application Programming Interface

TC-D25 Secure source

Code signature should be used to verify the reliability and security of application interface and third-party API.

TC-D26 Application Security

Security should be considered during the entire development cycle of API and any third-party API should be subjected to security accreditation.

TC-D27 Connection authorization

Authorization management mechanism should be implemented on the integrated application interface and third-party API.

TC-D28 Error message

Integrated application interface and third-party API should not reveal or leak any sensitive information through error message issued by authentication or authorization management mechanisms.

4.3.5. System Logging

TC-D29 Basic log information

System log should have the capability to log and display all access from users logging in via console or remote access. The system log should at least include full timestamp, user identity and action.

TC-D30 Secure log access

Access control should be implemented for the system log.

TC-D31 System log storage

There should be sufficient storage reserved for system log.

TC-D32 System log exportation

Device should have the capability to export system log to external system log server.

4.4. Communication Security

4.4.1. Network Port

TC-E01 Use appropriate network ports

For the communication between edge clients and gateway, and communication between gateway and cloud, IoT developers should choose suitable network ports for the IoT connections. These ports can be ports that are not commonly used by network services (i.e. TCP 80/443).

TC-E02 Identify service port requirement

Only enable ports that are required for the functionalities of IoT to prevent malicious attacks such as password guessing, eavesdropping and service interruption.

4.4.2. Sensitive Data Transmission

TC-E03 Identify sensitive data

Carry out data classification within operating environment.

TC-E04 Identify local regulations

Identify regulations of countries that are involved in the sensitive data transmission.

TC-E05 Secure sensitive data transmission

Personally identifiable information (PII) or confidential information should not be transmitted over channel that could be accessed by unauthorized parties. Encryption should also be used to further protect the security of such information. Ensure that communication security is provided using state-of-the-art, standardized security protocols, such as TLS for encryption.

TC-E06 Secure credential transmission

Both internal and external credential transmission should be encrypted.

4.4.3. Communication Interface

TC-E07 Communication interface management

Manufacturer should consider enabling IoT user the ability to manage the connectivity of their devices, such as enabling and disabling wireless communication.

TC-E08 Necessity of communication interface

Manufacturer should implement communication interface according to the operating environment of the IoT device. Keeping only communication interfaces that are necessary for delivering the device functions can reduce the attack vectors.

TC-E09 Security mechanism integration

Manufacturer should consider the integrability of the communication interface with its security mechanisms such as encryption channel and device identity identification.

TC-E10 Blocking internet debug mode

Access to operating system debug mode via internet should be prevented.

4.4.4. Communication Protocol

TC-E11 Communication protocol security

Evaluate security of communication protocol ensuring that it conform to standard specification and not impacted by known vulnerabilities.

TC-E12 Communication protocol maintenance

Evaluate the maintainability of the communication through factors such as capability to respond to attacks and capability to fix vulnerability after product release.

TC-E13 Security mechanism integration

Developer should consider the integrability of the communication protocol with its security mechanisms such as encryption channel and device identity identification.

TC-E14 Unauthorized connection

Security mechanism should be in place to prevent unauthorized connection at all Open System Interconnection (OSI) level.

TC-E15 Connection speed limitation

Limit speed of network traffic to reduce the risk of denial of service.

TC-E16 Use proven solutions

Only proven communication protocols and cryptographic algorithms should be used. Such proven solutions could be solutions that are recognized and adopted by the scientific community. Unproven solutions such as customized cryptographic algorithm should be avoided.

4.5. Identification, Authentication and Authorization

4.5.1. Authentication

TC-F01 Identity authentication

Identity authentication mechanism should be designed, and the system should only provide services to users or other devices after they are authenticated. Example authentication mechanism can be device certificate, user certificate, or user account and password matching.

TC-F02 Re-authentication

According to the operating environment of the IoT device, authentication system designs should automatically provide a mechanism requiring re-authentication after a period of inactivity or prior to providing services to users or other devices.

TC-F03 Replay attack protection mechanism

Identify authentication mechanism should have the capability to protect the system against replay attack.

TC-F04 Limited disclosure of personal identifiable information

The device should not disclose personal identifiable information or related messages due to incorrect/improper access.

TC-F05 Multifactor authentication

Multifactor authentication should be implemented to ensure credibility if resource is available and without affecting user experience.

TC-F06 Two-way authentication

Two-way authentication should be implemented to ensure credibility if resource is available and without affecting user experience.

4.5.2. Password

TC-F07 Password strength requirement

Proper password length and complex composition rules should be used to increase the strength of password.

TC-F08 Incorrect password protection

Proper password protection mechanism such as limiting number of password guesses should be implemented.

TC-F09 Default password differentiation

Each of the developed IoT should have different default password.

TC-F10 Default password management

Default password management mechanisms should be implemented. Enforce mechanism which require users to change password after initial login and limit user access using default password.

TC-F11 Secure authentication credentials

Authentication credentials should be salted, hashed and/or encrypted.

TC-F12 Secure password recovery

Ensure password recovery or reset mechanism is robust and does not leak information indicating a valid account to an attacker. The same applies to key update and recovery mechanisms.

4.5.3. Authorization

TC-F13 Access control policy

In order to maintain data confidentiality and integrity, device access control should be based on the necessity, importance and privacy requirements of the subject to access the object. Authorization schemes based on system-level threat models should also be implemented.

TC-F14 Least privilege

IoT users and devices should be given access to resources or IoT devices following the principle of least privilege according to the operating environment of the IoT.

TC-F15 Blocking privileged mode

Special operation privilege should not be given to users and other device if resource is available and without affecting user experience.

TC-F16 Privileged code isolation

Device firmware should be designed as privileged code and can only be accessed with the presence of privilege authorization. It should also be isolated from application and data.

4.6. Privacy Protection

4.6.1 Assessment of Sensitive Information

TC-G01 Minimize personal data collection

The amount of personal data that is processed should be restricted to the minimal amount possible according to the operating environment of the IoT.

TC-G02 Hide personal data

Secure personal data storage structure should be implemented to make sure personal data, and their interrelationships, be hidden from plain view during storage and access.

TC-G03 Separate personal data

Secure personal data storage structure should be implemented to make sure personal data is processed in a distributed fashion, in separate compartments whenever possible.

TC-G04 Data deletion right protection

Data deletion right protection should be implemented to allow users to delete their stored personal data.

Annex

List of CSCSS IoT Security Requirements and Controls

A. Management Principles

A1

Control Number	MP-A01	Control Name	Security by design
Applicable Components	☑Management ☑Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Security by design
Description	Manufacturer should have a stringent security by design procedure for firmware, driver and operating system components development. Security tests should be performed before the release of each update patches. Manufacturer should also have proper notification procedure to notify the users on updating their IoT devices.		

A2

Control Number	MP-A02	Control Name	Conducting risk and threat assessments
Applicable Components	☑Management ☑Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Risk and Threat Identification and Assessment
Description	Risk assessments should be conducted with the following tasks: (i) Identify threat sources that are relevant to IoT ecosystem/environment or components within (ii) Identify threat events that could be produced by those sources (iii) Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation (iv) Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful (v) Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events) (vi) Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.		

A3

Control Number	MP-A03	Control Name	Development of Action Plan
Applicable Components	☑Management ☑Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Risk and Threat Identification and Assessment
Description	Based on the risk and threat assessed/identified, organization should develop a risk treatment strategy and action plan including: (i) proposed actions, priorities or time plans (ii) resource requirements (iii) roles and responsibilities of all parties involved in the proposed actions (iv) performance measures (v) reporting and monitoring requirements		

A4

Control Number	MP-A04	Control Name	Establish procedures for responding security incidents
Applicable Components	☑Management ☑Architecture ☐Edge Client ☐Gateway ☐Cloud	Security Requirement	Management of Security Vulnerabilities and Incidents
Description	Procedures should be established for (i) Detection and analysis incident (ii) Containment, eradication, and recovery from an incident (iii) Post-Incident Activity of a incident.		

A5

Control Number	MP-A05	Control Name	Vulnerability Report and Disclosure via information-sharing platforms
Applicable Components	☑Management ☑Architecture ☐Edge Client ☐Gateway ☐Cloud	Security Requirement	Management of Security Vulnerabilities and Incidents
Description	Developers should participate in information-sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.		

A6

Control Number	MP-A06	Control Name	Create and Maintain Public Vulnerability Report Channels

Applicable Components	☑Management ☑Architecture ☐Edge Client ☐Gateway ☐Cloud	Security Requirement	Management of Security Vulnerabilities and Incidents
Description	Create a publicly disclosed mechanism for vulnerability reports, such as Security escalation channels or Bug Bounty programs.		

A7

Control Number	MP-A07	Control Name	Data process outsourcing
Applicable Components	☑Management ☐Architecture ☐Edge Client ☐Gateway ☐Cloud	Security Requirement	Third-Party relationships
Description	Data processed by a third-party must be protected by a data processing agreement.		

A8

Control Number	MP-A08	Control Name	Supply chain cybersecurity management strategy
Applicable Components	☑Management ☐Architecture ☐Edge Client ☐Gateway ☐Cloud	Security Requirement	Third-Party relationships
Description	Security requirements and supply chain security management strategy should be implemented and communicated to suppliers and partners. The strategy should include (i) Security governance (ii) Security in manufacturing and operations (iii) Asset management (iv) Security incident management.		

A9

Control Number	MP-A09	Control Name	Share personal data of consumers with third parties
Applicable Components	☑Management ☐Architecture ☐Edge Client ☐Gateway ☐Cloud	Security Requirement	Third-Party relationships
Description	Only share personal data of consumers with third parties with express consent of the consumers, unless otherwise required and limited for the use of product features or service operations.		

A10

Control Number	MP-A10	Control Name	Identify sensitive data
Applicable Components	☑Management ☐Architecture ☐Edge Client ☐Gateway ☐Cloud	Security Requirement	Assessment of Impacts on Sensitive Information
Description	Identify sensitive data according to the operating environment.		

A11

Control Number	MP-A11	Control Name	Identify local regulations
Applicable Components	☑Management ☐Architecture ☐Edge Client ☐Gateway ☐Cloud	Security Requirement	Assessment of Impacts on Sensitive Information
Description	Identify regulations of countries that are involved in the sensitive data transmission.		

A12

Control Number	MP-A12	Control Name	Privacy by design
Applicable Components	☑Management ☐Architecture ☐Edge Client ☐Gateway ☐Cloud	Security Requirement	Assessment of Impacts on Sensitive Information
Description	Privacy by design should be implemented. Privacy should be taken into account throughout the entire development process.		

B. Architecture Principles

B01

Control Number	AP-B01	Control Name	Key management
Applicable Components	☐Management ☑Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Cryptographic Management
Description	Proper management mechanism and requirements should be implemented for cryptographic key generation, exchange, storage, usage, replace and discard.		

C. Physical Security

C01

Control Number	TC-C01	Control Name	Physical port safety control
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Physical Interface
Description	To prevent unauthorized access, restriction on accessing operating system via physical port should be implemented.		

C02

Control Number	TC-C02	Control Name	Plug and unplug alert
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Physical Interface
Description	To help detecting and alerting unauthorized access, during the event of plugging or unplugging physical port, alert should be issued or the event should be logged for audit purpose.		

C03

Control Number	TC-C03	Control Name	Reset Button Protection
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Physical Interface
Description	There should be physical protection mechanism to prevent reset button from unauthorized access.		

C04

Control Number	TC-C04	Control Name	Anomaly detection
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Physical Layer
Description	Device should have the capability to create event log or alert when anomaly events such as sensing components, accessory component, ethernet port, wireless network antennas and power cable disconnection, or bad signaling occur.		

C05

Control Number	TC-C05	Control Name	Device destruction and disassembly
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Physical Layer
Description	Physical security mechanism should be implemented to protect the device from easily destroyed or disassembled. The mechanism should also protect the data storage medium from easily removed.		

C06

Control Number	TC-C06	Control Name	Environmental factors
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Physical Layer
Description	Natural disasters or accidental factors in the installation location, such as earthquakes, fires, floods, winds, abnormal temperature and humidity should be considered. Appropriate material and design should be used to protect device from failure or reduced performance caused by environmental factors.		

D. System Security

D1

Control Number	TC-D01	Control Name	Firmware version
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	The firmware, driver and operating system components version should verified during system boot.		

D2

Control Number	TC-D02	Control Name	Secure boot
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	Completeness of firmware, driver and operating system components version should be checked during system boot. Secure boot can be implemented with encryption module to ensure that the system is not tampered.		

D3

Control Number	TC-D03	Control Name	Trustable boot environment
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	Secure boot on firmware, drivers and components should be confirmed before any trust is claimed in any other software or executable program.		

D4

Control Number	TC-D04	Control Name	Tamper protection and detection
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	Security mechanism should be implemented to detect and react to firmware tampering. Notification should be sent to the operator and the mechanism should interrupt system operation or restore the firmware to a secure version.		

D5

Control Number	TC-D05	Control Name	Security and patch support
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	A product lifecycle should be defined and disclosed. The lifecycle should include the duration and end-of-life security and patch support. During the period of a product lifecycle, the device should be monitored and patched against known vulnerabilities until the “end-of-support’ period.		

D6

Control Number	TC-D06	Control Name	Secure offline update
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	Authorization certificate or encrypted channel should be used if IoT operating system utilize intranet or offline for updates. Security mechanism should be designed and implemented to ensure the completeness and correctness of the firmware, drivers and operating system components.		

D7

Control Number	TC-D07	Control Name	Secure online update
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	Authorization certificate or encrypted channel should be used if IoT operating system utilize internet (remote) for updates. Security mechanism should be designed and implemented to ensure the completeness and correctness of the firmware, drivers and operating system components.		

D8

Control Number	TC-D08	Control Name	Updates backward compatibility
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	Firmware updates should not modify user-configured preferences, security, and/or privacy settings without user notification.		

D9

Control Number	TC-D09	Control Name	Change Log
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	Firmware, driver and operating system components update should be logged in the change log. The device should have the capability to record at least 10 records.		

D10

Control Number	TC-D10	Control Name	Secure system restoration
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	The operating system should have mechanism to restore the firmware, drivers, operating system to a stable version during system update.		

D11

Control Number	TC-D11	Control Name	Prevent access to debug mode
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	The operating system should have mechanism to prevent user from entering operating system debug mode via direct connection ports or internet.		

D12

Control Number	TC-D12	Control Name	Secure whitelisting
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	The operating system should use whitelisting mechanism on applications and core components to prevent unauthorized application operating in the system.		

D13

Control Number	TC-D13	Control Name	Code signed system components
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Operating System
Description	Code signing and whitelisting mechanism should be implemented to ensure system components and code execution will not be tampered or overwritten after they are loaded.		

D14

Control Number	TC-D14	Control Name	Secure Configuration
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default.		

D15

Control Number	TC-D15	Control Name	System resilience
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	Physical impact of the system, such as external force, power surge or low voltage, instantaneous power failure and other abnormal conditions should be considered during the design. Mechanism should be implemented to maintain the system integrity and functionality after recovering to normal operating environment.		

D16

Control Number	TC-D16	Control Name	Auto recovery
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	Self-diagnosis and self-repair/healing mechanism should be implemented to recover the system from failure, malfunction or a compromised state.		

D17

Control Number	TC-D17	Control Name	Standalone operation
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Operating System
Description	The device should maintain operational and temporary store of undelivered data even with connection lost or chronicle negative impacts from compromised devices.		

D18

Control Number	TC-D18	Control Name	Secure storage
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Sensitive Data Storage
Description	A secure storage that complies with The Federal Information Processing Standard (FIPS) Publication 140-2 cryptographic modules should be designed and implemented for the storage of sensitive data.		

D19

Control Number	TC-D19	Control Name	Privilege control
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Sensitive Data Storage
Description	Privilege control mechanism should be implemented for the secure storage.		

D20

Control Number	TC-D20	Control Name	Data encryption
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Sensitive Data Storage
Description	Advanced Encryption Standard (AES) 256 bits or other cryptographic algorithms that have same level of encryption strength should be used to protect the sensitive before it is stored in the secure storage.		

D21

Control Number	TC-D21	Control Name	Data segmentation
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Sensitive Data Storage
Description	Different storage segmentations should be implemented for the storage of common data and sensitive data.		

D22

Control Number	TC-D22	Control Name	Web vulnerability mitigation
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Web-Based Management Interface
Description	Web-based management interface should not be vulnerable to injection and cross site scripting attacks.		

D23

Control Number	TC-D23	Control Name	Transmission encryption
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Web-Based Management Interface
Description	Security mechanism should be implemented for remote web-based management interface setting with reference to requirements in TC-E03 – TC-E12.		

D24

Control Number	TC-D24	Control Name	Identity authentication
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Web-Based Management Interface
Description	Identity authentication mechanism should be implemented for access to web-based management interface with reference to TC-F01 – TC-F12. Multifactor authentication should be implemented for critical infrastructure.		

D25

Control Number	TC-D25	Control Name	Secure source
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Application Programming Interface
Description	Code signature should be used to verify the reliability and security of application interface and third-party API.		

D26

Control Number	TC-D26	Control Name	Application Security
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Application Programming Interface
Description	Security should be considered during the entire development cycle of API and any third-party API should be subjected to security accreditation.		

D27

Control Number	TC-D27	Control Name	Connection authorization
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Application Programming Interface
Description	Authorization management mechanism should be implemented on the integrated application interface and third-party API.		

D28

Control Number	TC-D28	Control Name	Error message
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Application Programming Interface
Description	Integrated application interface and third-party API should not reveal or leak any sensitive information through error message issued by authentication or authorization management mechanisms.		

D29

Control Number	TC-D29	Control Name	Basic log information
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	System Logging
Description	System log should have the capability to log and display all access from users logging in via console or remote access. The system log should at least include full timestamp, user identity and action.		

D30

Control Number	TC-D30	Control Name	Secure log access
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	System Logging
Description	Access control should be implemented for the system log.		

D31

Control Number	TC-D31	Control Name	System log storage
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	System Logging
Description	There should be sufficient storage reserved for system log.		

D32

Control Number	TC-D32	Control Name	System log exportation
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	System Logging
Description	Device should have the capability to export system log to external system log server.		

E. Communication Security

E1

Control Number	TC-E01	Control Name	Use appropriate network ports
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Network Port
Description	For the communication between edge clients and gateway, and communication between gateway and cloud, IoT developers should choose suitable network ports for the IoT connections. These ports can be ports that are not commonly used by network services (i.e. TCP 80/443).		

E2

Control Number	TC-E02	Control Name	Identify service port requirement
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Network Port
Description	Only enable ports that are required for the functionalities of IoT to prevent malicious attacks such as password guessing, eavesdropping and service interruption.		

E3

Control Number	TC-E03	Control Name	Identify sensitive data
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Sensitive Data Transmission
Description	Carry out data classification within operating environment.		

E4

Control Number	TC-E04	Control Name	Identify local regulations
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Sensitive Data Transmission
Description	Identify regulations of countries that are involved in the sensitive data transmission.		

E5

Control Number	TC-E05	Control Name	Secure sensitive data transmission
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Sensitive Data Transmission
Description	Personally identifiable information (PII) or confidential information should not be transmitted over channel that could be accessed by unauthorized parties. Encryption should also be used to further protect the security of such information. Ensure that communication security is provided using state-of-the-art, standardized security protocols, such as TLS for encryption.		

E6

Control Number	TC-E06	Control Name	Secure credential transmission
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Sensitive Data Transmission
Description	Both internal and external credential transmission should be encrypted.		

E7

Control Number	TC-E07	Control Name	Communication interface management
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Communication Interface
Description	Manufacturer should consider enabling IoT user the ability to manage the connectivity of their devices, such as enabling and disabling wireless communication.		

E8

Control Number	TC-E08	Control Name	Necessity of communication interface
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Communication Interface
Description	Manufacturer should implement communication interface according to the operating environment of the IoT device. 以限制為原則，Keeping only communication interfaces that are necessary for delivering the device functions can reduce the attack vectors for malicious users to take advantage on.		

E9

Control Number	TC-E09	Control Name	Security mechanism integration
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Communication Interface
Description	Manufacturer should consider the integrability of the communication interface with its security mechanisms such as encryption channel and device identity identification.		

E10

Control Number	TC-E10	Control Name	Blocking internet debug mode
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☐Cloud	Security Requirement	Communication Interface
Description	Access to operating system debug mode via internet should be prevented.		

E11

Control Number	TC-E11	Control Name	Communication protocol security
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Communication Protocol
Description	Evaluate security of communication protocol ensuring that it conform to standard specification and not impacted by known vulnerabilities.		

E12

Control Number	TC-E12	Control Name	Communication protocol maintenance
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Communication Protocol
Description	Evaluate the maintainability of the communication through factors such as capability to respond to attacks and capability to fix vulnerability after product release.		

E13

Control Number	TC-E13	Control Name	Security mechanism integration
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Communication Protocol
Description	Developer should consider the integrability of the communication protocol with its security mechanisms such as encryption channel and device identity identification.		

E14

Control Number	TC-E14	Control Name	Unauthorized connection
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Communication Protocol
Description	Security mechanism should be in place to prevent unauthorized connection at all Open System Interconnection (OSI) level.		

E15

Control Number	TC-E15	Control Name	Connection speed limitation
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Communication Protocol
Description	Limit speed of network traffic to reduce the risk of denial of service.		

E16

Control Number	TC-E16	Control Name	Use proven solutions
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Communication Protocol
Description	Only proven communication protocols and cryptographic algorithms should be used. Such proven solutions could be solutions that are recognized and adopted by the scientific community. Unproven solutions such as customized cryptographic algorithm should be avoided.		

F. Authentication and Authorization

F1

Control Number	TC-F01	Control Name	Identity authentication
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Authentication
Description	Identity authentication mechanism should be designed, and the system should only provide services to users or other devices after they are authenticated. Example authentication mechanism can be device certificate, user certificate, or user account and password matching.		

F2

Control Number	TC-F02	Control Name	Re-authentication
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Authentication
Description	According to the operating environment of the IoT device, authentication system designs should automatically provide a mechanism requiring re-authentication after a period of inactivity or prior to providing services to users or other devices.		

F3

Control Number	TC-F03	Control Name	Replay attack protection mechanism
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Authentication
Description	Identify authentication mechanism should have the capability to protect the system against replay attack.		

F4

Control Number	TC-F04	Control Name	Limited disclosure of personal identifiable information
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Authentication
Description	The device should not disclose personal identifiable information or related messages due to incorrect/improper access.		

F5

Control Number	TC-F05	Control Name	Multifactor authentication
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Authentication
Description	Multifactor authentication should be implemented to ensure credibility if resource is available and without affecting user experience.		

F6

Control Number	TC-F07	Control Name	Two-way authentication
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Authentication
Description	Two-way authentication should be implemented to ensure credibility if resource is available and without affecting user experience.		

F7

Control Number	TC-F07	Control Name	Password strength requirement
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Password
Description	Proper password length and complex composition rules should be used to increase the strength of password.		

F8

Control Number	TC-F08	Control Name	Incorrect password protection
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Password
Description	Proper password protection mechanism such as limiting number of password guesses should be implemented.		

F9

Control Number	TC-F09	Control Name	Default password differentiation
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Password
Description	Each of the developed IoT should have different default password.		

F10

Control Number	TC-F10	Control Name	Default password management
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Password
Description	Default password management mechanisms should be implemented. Enforce mechanism which require users to change password after initial login and limit user access using default password		

F11

Control Number	TC-F11	Control Name	Secure authentication credentials
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Password
Description	Authentication credentials should be salted, hashed and/or encrypted.		

F12

Control Number	TC-F12	Control Name	Secure password recovery
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Password
Description	Ensure password recovery or reset mechanism is robust and does not leak information indicating a valid account to an attacker. The same applies to key update and recovery mechanisms.		

F13

Control Number	TC-F13	Control Name	Access control policy
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Authorization
Description	In order to maintain data confidentiality and integrity, devices/ cloud services access control should be based on the necessity, importance and privacy requirements of the subject to access the object. Authorization schemes based on system-level threat models should also be implemented.		

F14

Control Number	TC-F14	Control Name	Least privilege
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Authorization
Description	IoT users and devices should be given access to resources or IoT devices /cloud services following the principle of least privilege according to the operating environment of the IoT.		

F15

Control Number	TC-F15	Control Name	Blocking privileged mode
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Authorization
Description	Special operation privilege should not be given to users and other device if resource is available and without affecting user experience.		

F16

Control Number	TC-F16	Control Name	Privileged code isolation
Applicable Components	☐Management ☐Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Authorization
Description	Device firmware should be designed as privileged code and can only be accessed with the presence of privilege authorization. It should also be isolated from application and data.		

G. Privacy Protection

G1

Control Number	TC-G01	Control Name	Minimize personal data collection
Applicable Components	☑Management ☑Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Assessment of Sensitive Information
Description	The amount of personal data that is processed should be restricted to the minimal amount possible according to the operating environment of the IoT.		

G2

Control Number	TC-G02	Control Name	Hide personal data
Applicable Components	☑Management ☑Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Assessment of Sensitive Information
Description	Secure personal data storage structure should be implemented to make sure personal data, and their interrelationships, be hidden from plain view during storage and access.		

G3

Control Number	TC-G03	Control Name	Separate personal data
Applicable Components	☑Management ☑Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Assessment of Sensitive Information
Description	Secure personal data storage structure should be implemented to make sure personal data is processed in a distributed fashion, in separate compartments whenever possible.		

G4

Control Number	TC-G04	Control Name	Data deletion right protection
Applicable Components	☑Management ☑Architecture ☑Edge Client ☑Gateway ☑Cloud	Security Requirement	Assessment of Sensitive Information
Description	Data deletion right protection should be implemented to allow users to delete their stored personal data.		

Bibliographic Citations

[1] European Union Agency For Network And Information Security, *Baseline Security Recommendations for IoT*, November 2017. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport (accessed September 4, 2018)

[2] National Institute of Standards and Technology, *Federal Information Processing Standards Publication 140-2: Security Requirements for Cryptographic Modules*, December 2002. https://csrc.nist.gov/publications/detail/fips/140/2/final (accessed September 4, 2018)

[3] Open Web Application Security Project, *Internet of Things Top Ten*, 2014. https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf (accessed September 4, 2018)