International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4810

(11/2021)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Identification and security

Requirements for data security of heterogeneous Internet of things devices

Recommendation ITU-T Y.4810

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	**Y.4800–Y.4899**
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4810

Requirements for data security of heterogeneous Internet of things devices

Summary

Recommendation ITU-T Y.4810 describes requirements for data security of heterogeneous Internet of things (IoT) devices under specific scenarios to provide a general reference recommendation and to ensure IoT data safety. Deploying existing data security solutions to IoT presents challenges because of limited hardware and software resources, IoT device management and IoT deployment specific scenarios.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4810	2021-11-29	20	11.1002/1000/14820

Keywords

Data security, IoT.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.4810

Requirements for data security of heterogeneous Internet of things devices

1 Scope

This Recommendation specifies requirements for data security of heterogeneous Internet of things (IoT) devices, including, under specific scenarios, a data security threat (DST) and requirement model.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

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

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

3.1.2 application [b-ITU-T Y.2091]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

3.1.3 capability [b-ITU-R M.1224-1]: The ability of an item to meet a service demand of given quantitative characteristics under given internal conditions.

3.1.4 service [b-ITU-T Y.2091]: A set of functions and facilities offered to a user by a provider.

3.1.5 device [ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, date capture, data storage and data processing.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CoAP Constrained Application Protocol

DSR Data Security Requirement

DST Data Security Threat

DTLS Datagram Transport Layer Security

IoT Internet of Things

MCU Microcontroller Unit

MITM Man-In-The-Middle

MQTT Message Queueing Telemetry Transport

NB-IoT Narrowband Internet of Things

OS Operating System

PCB Printed Circuit Board

SE Secure Element

WiFi Wireless Fidelity

5 Conventions

This Recommendation uses the following conventions.

– The phrase "is required to" indicates a requirement that must be strictly followed and from which no deviation is permitted if conformity to this Recommendation is to be claimed.

– The phrase "is recommended" indicates a requirement that is recommended, but which is not absolutely required to claim conformity to this Recommendation.

6 Specific scenarios for data security of heterogeneous IoT devices

Specific scenarios for data security of heterogeneous IoT devices include:

– limited hardware and software resources: low power consumption, low processing capability, long-lived, small amounts of memory and specific operating systems;

– IoT device management considerations: unattended operation and minimal user interactions;

– IoT deployment scenarios: rapidly moving devices and unprotected IoT devices.

Heterogeneous IoT devices under specific scenarios could be critical for attackers or malicious manufacturers and vendors to illegally access the original IoT data including sensitive personal data.

7 Data security threat and requirement model for heterogeneous IoT devices under specific scenarios

According to [ITU-T Y.4000], IoT devices are categorized into four different types according to their communication capabilities and functionality: data-carrying; data-capturing; sensing and actuating; and general.

Based on the categorization in the previous paragraph, the data capabilities of IoT devices can be classified as any or all of the following: data collection; data storage; data query; data transfer; data processing; and data destruction. As for each data capability, a DST and requirement matrix for IoT devices is proposed in Table 1.

Table 1 – Data security threat and requirement matrix for IoT devices

Data capability	Category samples	Details samples	Evaluation reference	Data security threats	Data security requirement clause
Data collection	Data type (non-aggregated data)	Privacy data	Depends on the data leakage impact: the more important the data collected, the greater the impact of the data leak	DST-1; DST-2;	9.1 9.2
		Weather data			
		Public transport data			
		Keys/certification/password			
		Device operation data			
	Data range	Device data			
		Sensor data			
		Converging other device data			
Data storage	Storage types	embedded Flash drives	Depends on the ease of detachable reading: the easier it is to disassemble, the higher the security risk	DST-1; DST-2;	9.1 9.3
		cards			
		Solid state drives			
	Storage capacity	0-100 Mbyte	Depends on the data leakage impact: the greater the amount of data storage, the higher the security risk		
		100 M-1 Gbyte			
		>1 Gbyte			
	Local data cache	Temporary cache only	The security risk of local storage is higher than that of local temporary cache		
		Local storage copy			
Data query and transfer	IP capable	YES	Depends on possibility of a man-in-the-middle (MITM) attack	DST-2; DST-3; DST-4; DST-5; DST-6; DST-7; DST-8;	9.1 9.4 9.5
		NO			
	Communication protocol (application layer)	Message queueing telemetry transport (MQTT) + transport layer security v1.1/v1.2			
		MQTT without TLS			
		Constrained application protocol (COAP) + datagram transport layer security (DTLS) v1.2			
		COAP without DTLS			
		HTTPS			
	Communication protocol (network layer)	WiFi			
		Bluetooth			
		Radio frequency			
		ZigBee			

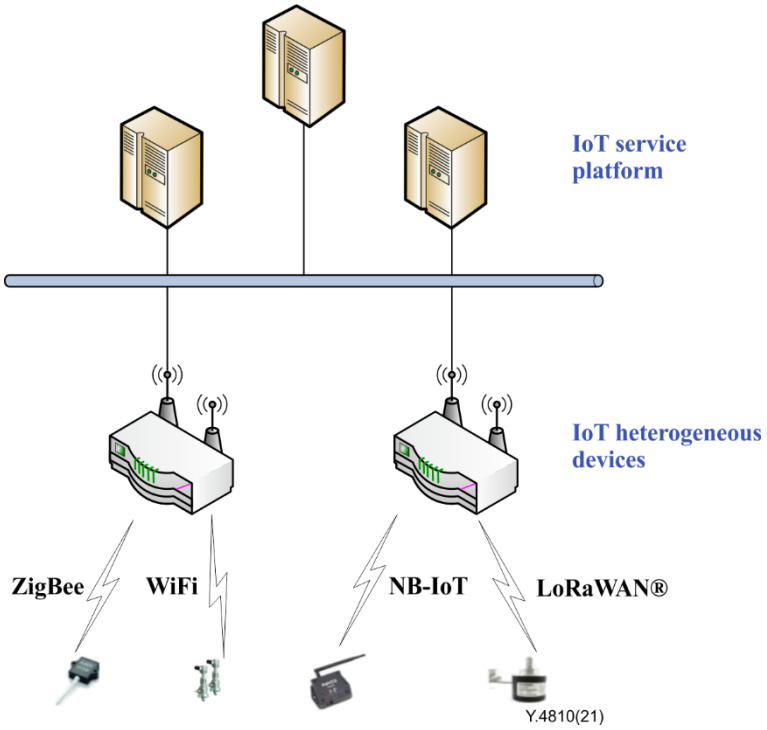
Table 1 – Data security threat and requirement matrix for IoT devices

Data capability	Category samples	Details samples	Evaluation reference	Data security threats	Data security requirement clause
		LoRaWAN®			
		Mobile network			
		KNX			
		Ethernet			
Data processing and destruction	Local computing power	YES	Depends on the ease of detachable reading and the data leakage impact	DST-1;	9.1 9.6 9.7
		NO			

Using the DST and requirement matrix of IoT devices in Table 1, the threats to and corresponding requirements for data security under specific scenarios can be further analysed for each type of data capability of IoT devices. Each type of heterogeneous IoT device contains multiple threats and corresponding requirements based on the matrix.

8 Data security threats in heterogeneous IoT devices under specific scenarios

As shown in Figure 8-1, heterogeneous IoT devices are basic components in the entire IoT system.



NB-IoT: narrowband Internet of things; WiFi: wireless fidelity

Figure 8-1 – Heterogeneous IoT devices in the IoT system

IoT devices are exposed to a variety of DSTs on confidentiality, integrity, availability and underground data leakage, e.g., eavesdropping, MITM attack, illegal message modification, sniffing, physical attack on data storage and unauthorized data leakage. Those threats directly present high threats of data leakage and abuse.

Figure 8-2 shows the following DSTs in heterogeneous IoT devices.

– DST-1: The threat of someone tampering with or spoofing the device (physical interference); it is possible to obtain and tamper with data on all devices. For example, an attacker can read data from the storage and tamper with telemetry data. On the other hand, the IoT device itself presents threats of underground data leakage or sharing with authorized third parties.

– DST-2: The threat of reading data in transit between devices, tampering with transferred data and overloading the device with new connections. For example, an attacker may intercept or partially override a broadcast and send false information.

– DST-3: The threat of someone spoofing the IoT field gateway and stealing data from the IoT service gateway. Also, this threat incorporates the description of DST-1.

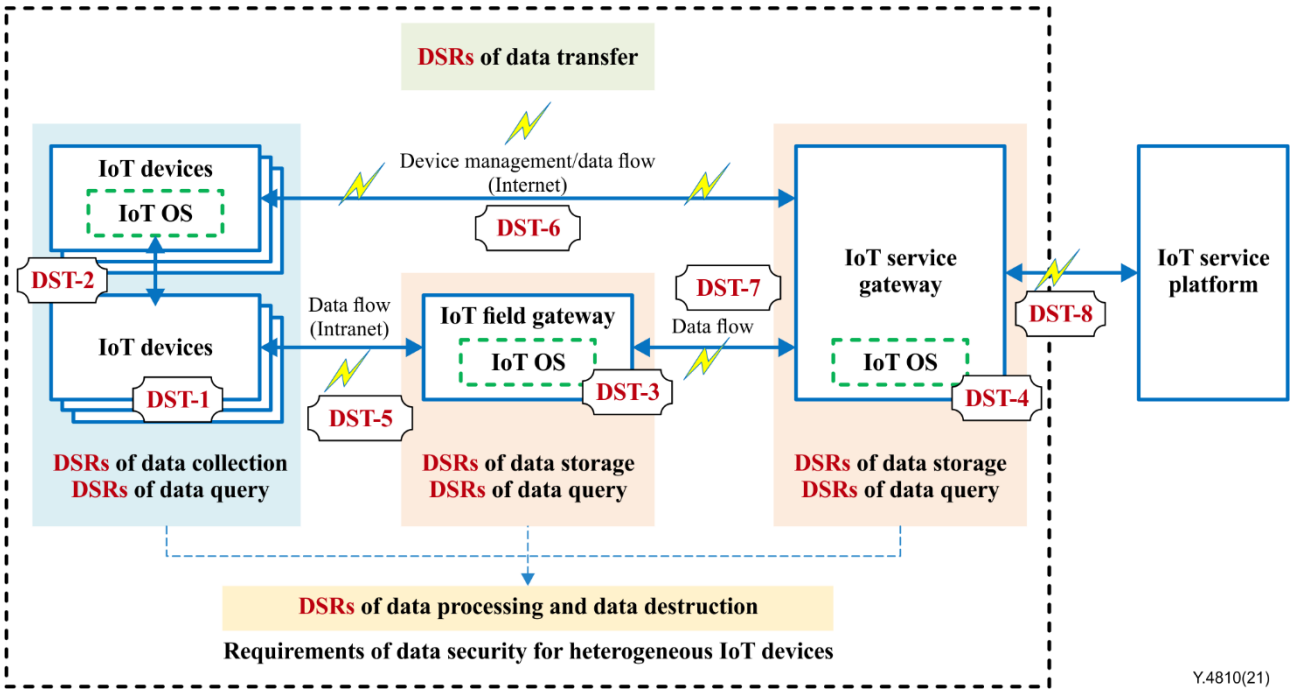
– DST-4: The threat of someone spoofing the IoT service gateway and stealing data from the IoT service platform. Also, this threat incorporates the description of DST-1.

– DST-5: The threat of eavesdropping on or interfering with communication between the device and the field gateway. This threat may also affect data integrity, confidentiality and accessibility. For example, an attacker may leverage extracted key material to intercept and suppress data from the device on the communication path and replace it with false data that is authenticated by stolen key material.

– DST-6: The threat of eavesdropping on or interfering with communication between the device and the service gateway. For example, an attacker may intercept or partially override a broadcast and send false information.

– DST-7: The threat of eavesdropping on or interfering with communication between the field and service gateways. Also, this threat incorporates the descriptions of DST-5 and DST-6.

– DST-8: The threat of eavesdropping on or interfering with the communication between the service gateway and service platform (cloud). Also, this threat incorporates the descriptions of DST-5 and DST-6.



DSR: data security requirement; OS: operating system

Figure 8-2 – Data security threats in heterogeneous IoT devices

9 Requirements for data security of heterogeneous IoT devices under specific scenarios

Requirements for data security of heterogeneous IoT devices include:

– integrity – ensuring that the data available are those expected;

– confidentiality – only authorized individuals can access the data;

– non-repudiation – ensuring that a data transaction cannot be denied;

– availability – maintaining the proper functioning of the data;

– authenticity – the data received must accordingly represent a real-world scene and even if they have probably undergone some processing, the meaning of the scene must not be modified;

– authentication – ensuring that only duly authorized individuals can access the data.

9.1 Common requirements for data security of heterogeneous IoT devices

Common requirements for data security of heterogeneous of IoT devices include:

– the operating system of an IoT device is required to have specific intrusion detection and security protection capabilities;

– whenever feasible, an IoT device operating system is recommended to be correctly configured, such that the system security policy and security update mechanism consider implementation of one or more of the following:

  - trusted boot – IoT devices should enable the function for verifying the boot partition provided by the microcontroller unit (MCU) chip, or implement similar functions by itself,

  - security hardening – it is recommended to enable the system security mechanisms, such as process sandbox, application permission management and full-disk data encryption, be enabled:

        - when the device chip or system supports the trusted execution environment, it is recommended that: a) important data be encrypted; and b) operation and running of trusted applications be performed within it
        - for devices with strong performance, it is recommended to use or develop IoT security products that support system monitoring, log reporting, vulnerability scanning and attack detection to harden the system,
    - update mechanism:
        - software, firmware or software development kit running on IoT devices is required to be secured,
        - it is recommended to update IoT devices securely over the air,
        - any security bugs and vulnerabilities discovered are required to be fixed in a timely fashion,
        - device update packages should be encrypted to avoid firmware reverse attacks,
        - the device should verify the integrity of the update package and the signature – it is recommended to use an asymmetric algorithm for verification;
- an IoT device is required to support the encryption protocols that are efficient and scalable for deployment on IoT devices with limited computational resources;
- an IoT device is recommended to provide the authority control functions, such as ownership control for preventing information leakage and privacy protection;
- it is recommended to apply tamper proof mechanisms to make it difficult to extract keys or other cryptographic material from the IoT device;
- the physical casing of an IoT device is recommended to be equipped with anti-destructive measures to avoid disassembly in a short time, and avoid external exposure of communication interfaces and special control buttons, e.g., non-essential universal serial bus interfaces and debugging serial ports;
- the hardware circuits and chips of an IoT device are recommended to have a secure design that prevents anti-reverse and anti-electromagnetic attacks:
    - the possibility of fire, electrical shock and personal injury involving components is required to be prevented or reduced,
    - human-computer interaction: for special IoT device for public services, which may provide touch screen, keyboard, mouse and other interaction methods, is recommended to enable security verification mechanism such as password verification, which should be applied for operations other than normal functions (such as background management and debugging mode), to prevent the normal business logic of the device from being bypassed; and the IoT device is required to avoid exposing the special permission buttons, such as reset function and system restart function,
    - printed circuit board (PCB) security: after the device is disassembled, its hardware circuits are exposed to security risks, so it is recommended to meet the following security requirements:
        - PCB information – the equipment circuit board should remove sensitive interface screen printing information, such as debugging and burning printed identification of solder joints on the recording interface
        - PCB interface – avoid unnecessary debugging and programming interfaces or solder joints on the device circuit board – if it is necessary to keep the interface, it is recommended to use debugging or burning tools with password protection.

9.2 Specific requirements for data collection of heterogeneous IoT devices

The specific requirements for data collection of heterogeneous IoT devices include:

– it is required to represent the entirety of functions of all types of data collection of an IoT device in an explicit way to end users;

– it is required to limit the function of data collection of an IoT device – the process of a specific type of data collection is required to be initiated only with explicit permission of end users;

– it is required to immediately stop a specific type of data collection if end users choose to disable the corresponding function;

– IoT devices may have a large number of sensors for various forms of data collection; these sensors are required to be protected to meet data security requirements, e.g., in the specific scenario of biometrics and autonomous driving, an IoT device is recommended to meet the following security requirements to ensure data authenticity:

  - microphone – for IoT devices that support voice recognition and voiceprint recognition, the microphone sensor is recommended to only respond to the sound within the recognizable frequency range of the human ear to prevent similar dolphin sound (ultrasonic) attacks,
  - camera – the camera sensor for IoT devices is recommended to choose a model that supports three-dimensional face recognition and live detection to prevent fake face attacks such as photos, videos and face moulds,
  - fingerprint recognition – the fingerprint recognition sensor for IoT devices is recommended to support live detection, prevent forgery fingerprint attacks such as fingerprint film,
  - global navigation satellite system – it is recommended to use satellite-based positioning in addition to other auxiliary positioning solutions (e.g., WiFi/bluetooth low energy/base-station) and mitigate against signal spoofing attacks.

9.3 Specific requirements for data storage in heterogeneous IoT devices

Specific requirements for data storage in heterogeneous IoT devices include:

– it is recommended to secure the data stored in IoT devices with various forms of security software with suitable complexity;

– it is required to encrypt sensitive data such as private information, and securely store these data to prevent information leakage;

– an IoT device is recommended to provide a data integrity verification function to prevent forgery of data;

– it is required to secure device chips embedded into IoT devices:

  - flash chip – the independent flash chip used by the IoT device is recommended to adopt a ball grid array package model with high temperature soldering; for devices with high security requirements, it is recommended to use glue around the flash chip, or use multi-chip stacking packaging technology to stack the flash chip above the central processing unit chip to increase the difficulty of desoldering,
  - MCU and secure element (SE) chip:
    - for MCUs or security chips that support the fuse function, the fuse bit is recommended to be blown during mass production to prevent the internal data of the chip from being read
    - if the device MCU itself supports hardware-level encryption and verification functions, the debugging, reading and writing of the chip is recommended either to

be turned off and the function of Boot mode selection disabled or to enable password protection and the encryption and verification function of the system firmware

- it is recommended to use the SE chip for encryption calculation and key storage.

9.4 Specific requirements for data query of heterogeneous IoT devices

Specific requirements for data query of heterogeneous IoT devices include:

– it is required to use access control policies to govern access to data of IoT devices;

– the principle of minimum authorization is required to be applied to avoid illegal access;

– an external interface is required to verify the legitimacy of URL parameters and user operations;

– it is recommended to audit access logs on all IoT devices.

9.5 Specific requirements for data transfer to and from heterogeneous IoT devices

The specific requirements for data transfer to and from heterogeneous IoT devices include:

– it is required to represent the entirety of functions of all types of data transfer to and from an IoT device in an explicit way to end users;

– it is required to limit the function of data transfer to and from an IoT device – the process of a specific type of data transfer is required to be initiated only with explicit permission of end users;

– it is required to use encryption to secure the data while being transmitted from IoT devices to an IoT service platform;

– IoT devices may use a variety of communication technologies and authentication methods, it is recommended to choose a highly secure communication solution to avoid the common security risks of wireless communication or wired communication within the IoT devices, which may include packet replay, MITM sniffing, cracking and hijacking;

– it is recommended to use the latest version of the encryption protocol and appropriate algorithms to protect the communication security of the specific communication technology;

– high-performance gateway equipment is required to support the function to prevent wireless MITM, distributed denial of service, honeypot and other attacks;

– it is required to have the anti-interference ability between the IoT device and network equipment.

9.6 Specific requirements for data processing by heterogeneous IoT devices

The specific requirements for data processing by heterogeneous IoT devices include:

– it is required to use data fusion, which deals with dynamic environments and large-scale heterogeneous data sources, to ensure data integrity;

– sensitive data calculation and key storage is recommended to be in a trusted execution environment;

– specific IoT devices, such as edge computing gateways, are required to have security capabilities, such as log reporting, authentication, network monitoring and attack protection;

– an IoT device is not allowed to open network ports that listen to unauthorized high-risk services.

9.7 Specific requirements for data destruction by heterogeneous IoT devices

The specific requirements for data destruction by heterogeneous IoT devices include:

– an IoT device is recommended to have a function of data destruction;

– it is required to limit the function of data destruction of an IoT device – the process of a specific type of data destruction is required to be securely initiated only with explicit permission of end users;
– it is required to completely remove the data if end users choose to delete data stored inside an IoT device.

Bibliography

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks.*

[b-ITU-R M.1224-1] Recommendation ITU-R M.1224-1 (2012), *Vocabulary of terms for international mobile telecommunications (IMT) – M Series: Mobile, radiodetermination, amateur and related satellite services.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022