

Recommendation

ITU-T X.1354 (09/2024)

SERIES X: Data networks, open system communications
and security

Secure applications and services (II) – Internet of things
(IoT) security

Security controls for Internet of things systems

ITU-T X-SERIES RECOMMENDATIONS

Data networks, open system communications and security

PUBLIC DATA NETWORKS	X.1-X.199
OPEN SYSTEMS INTERCONNECTION	X.200-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999
INFORMATION AND NETWORK SECURITY	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
Emergency communications	X.1300-X.1309
Ubiquitous sensor network security	X.1310-X.1319
Smart grid security	X.1330-X.1339
Certified mail	X.1340-X.1349
Internet of things (IoT) security	X.1350-X.1369
Intelligent transportation system (ITS) security	X.1370-X.1399
Distributed ledger technology (DLT) security	X.1400-X.1429
Application Security (2)	X.1450-X.1459
Web security (2)	X.1470-X.1489
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METaverse AND DIGITAL TWIN SECURITY	X.2000-X.2199
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

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

Recommendation ITU-T X.1354

Security controls for Internet of things systems

Summary

Recommendation ITU-T X.1354 provides practical security guidelines for three stakeholders, namely providers, developers and users of services in Internet of things (IoT) systems. It also describes the concept, risks and security controls of these systems.

IoT systems present particular challenges for information security because they are highly distributed and involve a large number of diverse entities. This implies that there is a very large attack surface and poses a significant challenge for an information security management system to apply and maintain appropriate security controls across the whole system.

History*

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1354	2024-09-06	17	11.1002/1000/15890

Keywords

IoT security guidelines, IoT systems, IoT risk, security controls.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and 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/>.

© ITU 2024

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	1
4 Abbreviations and acronyms	1
5 Conventions	2
6 Concept and risk of the Internet of things	2
6.1 General	2
6.2 IoT stakeholders	2
6.3 Reference model.....	2
6.4 Risks in IoT systems.....	4
6.5 IoT lifecycle.....	6
7 Security controls	7
7.1 Security controls for developers and providers of IoT services	7
7.2 Security controls for IoT user.....	23
Bibliography.....	25

Recommendation ITU-T X.1354

Security controls for Internet of things systems

1 Scope

This Recommendation provides practical security guidelines for three stakeholders, namely, providers, developers and users of services in Internet of things (IoT) systems. It also describes the concept, risks and security controls of these systems.

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.2069] | Recommendation ITU-T Y.2069 (2012), <i>Terms and definitions for the Internet of things</i> . |
| [ITU-T Y.4000] | Recommendation ITU-T Y.4000/Y.2060 (2012), <i>Overview of the Internet of things</i> . |
| [ISO/IEC 27000] | International Standard ISO/IEC 27000:2018, <i>Information technology – Security techniques – Information security management systems – Overview and vocabulary</i> . |
| [ISO/IEC 30141] | International Standard ISO/IEC 30141:2024, <i>Internet of things – Reference architecture</i> . |

3 Definitions

3.1 Terms defined elsewhere

In this Recommendation, the terms given in [ITU-T Y.2069], [ITU-T Y.4000] and [ISO/IEC 27000] apply.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

- | | |
|-----|-----------------------------------|
| API | Application Programming Interface |
| ID | Identifier |
| IoT | Internet of Things |
| OTA | Over The Air |

5 Conventions

None.

6 Concept and risk of the Internet of things

6.1 General

This clause is a brief introduction to the concept and risks of the IoT, which is useful in the context of security. Detailed information related to clauses 6.2 and 6.3 is provided in [ISO/IEC 30141].

6.2 IoT stakeholders

An IoT domain can have several stakeholders, e.g., providers, developers and users of IoT services.

6.2.1 IoT service provider

The role of service provider is to manage and to operate IoT services. IoT service providers can also provide network connectivity. Security and security credentials of this connectivity need to be addressed and maintained. Additionally, in the case of cloud-based IoT services, depending on the type of service offered from the data centre (software as a service, platform as a service, infrastructure as a service), security management, multi-tenancy and tenant security and separation need be managed at different layers from the hardware up the stack to the application layers.

Common services provided by IoT service providers include connectivity services, data collection and management services, as well as management service for IoT-related assets, such as IoT devices.

6.2.2 IoT service developer

An IoT service developer is responsible for the design, implementation and integration of IoT services. The service developer has multiple roles, namely as device developer or manufacturer, system integrator, as well as developer of the platform and application.

An IoT device developer integrates hardware and software securely into devices and applications, developing and maintaining device firmware that securely connects devices to an IoT-enabled platform.

IoT devices can be used directly by either a user or service provider, and technically similar devices can be used in various use cases. It is important for an IoT device developer to consider the security requirements of potential usage scenarios for the device in the design phase, in order to be able to offer devices that have the right set of functionality and features to fulfil customer needs.

In addition, the IoT service developer needs to collaborate with other stakeholders, such as IoT service provider and system integrators.

6.2.3 IoT user

End-users of IoT services can be categorized into human and digital. IoT users are end-users of services and are categorized as human users and digital users.

A human user is an individual who uses IoT services. A digital user is a non-human user of IoT services including automation services.

6.3 Reference model

The reference model described in this Recommendation is based on the IoT reference architecture [ISO/IEC 30141], with the combination of IoT entities and subsystems shown in Figure 1. The IoT system is consisted of IoT users, application and service subsystems, operations and management subsystems, the resource access and interchange subsystem, physical entities, IoT devices and gateway.

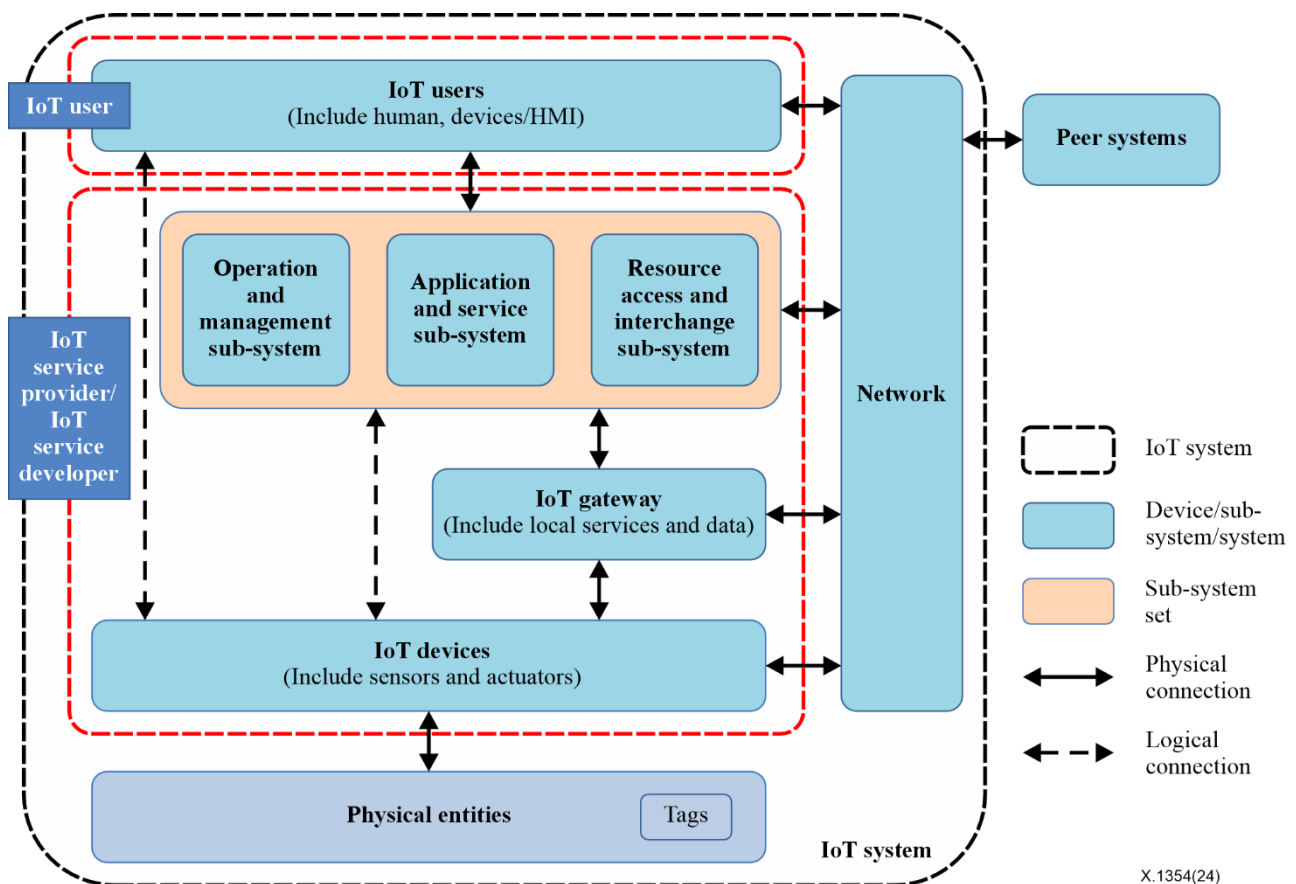


Figure 1 – IoT system reference model (based on Figure 11 of [ISO/IEC 30141])

In Figure 1, the two red dotted rectangles contain IoT users, service providers and developers, respectively, as stakeholders in the IoT system.

A user stakeholder, either human or digital, is the consumer of an IoT service. A provider stakeholder manages and operates IoT services, including network connectivity. A developer stakeholder implements, tests and integrates services on an IoT platform. In the reference model, both provider and developer are related to services with the same IoT entities and are illustrated within a single red dotted rectangle.

IoT entities in Figure 1 are further explained as follows.

The following IoT entities are considered.

- 1) Physical entities are the real-world things that are sensed and acted upon by the IoT devices.
- 2) Tags of various types can be attached to physical entities to aid in their monitoring and identification.
- 3) IoT devices interact with the physical world through sensing and actuation. IoT devices include:
 - a) sensors, which observe a property of a physical entity and convert the observation into digital information;
 - b) actuators, which act on or change some properties of the physical entities based on digital instructions.
- 4) IoT devices communicate via a network. Many IoT devices communicate using a relatively short range and specialized proximity network, due to power and processing limitations.
- 5) Many other devices are able to communicate using wide area networks, such as Internet.

- 6) IoT gateways are commonly used in IoT systems. They form a connection between the local proximity network(s) and the wide area access network. IoT gateways can contain other entities and provide a wider range of capabilities. However, the specific functionality of an IoT gateway can vary depending on its intended use, the types of devices it connects, and the overall architecture of the IoT system it serves. An IoT gateway often contains a management agent, providing remote management capabilities. The IoT gateway can contain a device data store, storing data from the associated IoT devices – this can either support local ("edge" or "fog") processing capabilities or be a means of dealing with intermittent communications networks. One or more analytics services can be supported by the IoT gateway, typically operating on data coming from the IoT devices or from the device data store. The IoT gateway can also contain applications – these can be control applications, where rapid local processing is required to direct actuators based on input from sensors.
- 7) Application and service subsystems of various kinds exist in most IoT systems, with associated data stores. There is often a store containing data derived from IoT devices. There can be a store containing results from analytics services operating on device data and data from other sources. Analytics services of various types are usually present, processing device data and other data to derive insights, for example, monitoring performance. Management of processes associated with the IoT system is usually present. There are applications that reflect the capabilities of the IoT system itself. Finally, there are business services that provide capabilities related to the commercial use of the system, by either end users or other external peer systems. The applications and services communicate with IoT gateways and IoT devices using the access network, while they communicate with each other using the services network.
- 8) The operation and management subsystem includes a device registry data store and an associated device identity service, which provides lookup capabilities for applications and services. There is a device management application, which provides monitoring and administration capabilities for IoT devices in the system. There is an operational support system that provides various capabilities relating to the monitoring and management of the overall IoT system, including the offering of administration capabilities to users.
- 9) Access to the capabilities of the IoT system for users and peer systems is provided by the resource access and interchange subsystem. These subsystems provide controlled interfaces for capabilities of service, administration and business relying on access control capabilities that vary depending on the user. Authentication and authorization are required before the capabilities can be used. Some of the capabilities can be provided through cloud service interfaces by implementation.
- 10) IoT system users can include both human and digital types. Human users typically interact with the IoT system using some kind of device. The user device can take many forms – including a smartphone, personal computer, tablet or a more specialized device. In all cases, some form of application interface is offered to the human user, where the capabilities are supplied by an underlying application that interacts with the rest of the IoT system. Digital users interact with IoT systems by means of service application programming interfaces (APIs) controlled by the resource access and interchange subsystem autonomously. Both user devices and digital users communicate with the rest of the IoT system via the user network. For some IoT systems, user devices can interact directly with IoT devices or IoT gateways.
- 11) Peer systems, whether IoT or non-IoT, can be users of an IoT system or offer services to it. Peer systems interact with the IoT system through the user network – typically Internet.

6.4 Risks in IoT systems

6.4.1 Introduction

This clause provides various risk scenarios associated with IoT systems.

Among widely varied applications of IoT systems, there are different contexts that determine risk scenarios, and hence different risks. A risk scenario is a description of conceivable security incidents, each of which consists of a series of events and consequences. The descriptions are general. These should be used as references in developing the entity's own risk scenarios and risks that are modified and refined to adapt to the business of an organization.

6.4.2 Features of IoT systems

An IoT system senses movement or physical state of equipment or materials. It processes sensed data and actuates to change movement or physical state. Given diversities in applications of IoT systems, it is impracticable to determine a generally applicable set of features that fits to every IoT system. As a practical way to describing features of IoT systems, "common features" and "specific features for application areas" can be identified.

IoT systems have the following common features:

- a) sensors that detect states or movement of equipment or materials;
- b) data acquired by the sensor are securely transmitted over the network to an information system;
- c) the information system processes the data and generates controlling data;
- d) controlling data are securely transmitted to actuators over the network;
- e) actuators translate the controlling data to the states or movement of equipment or materials.

Industrial plant and control systems, an application area of an IoT system, have the following features in addition to the common features previously described.

- a) IoT user is either human or digital ([ISO/IEC 30141]):
 - 1) a human user is an entity within an organization and acts within the scope of the organization's management;
 - 2) a digital user is a device that has interfaces with a sensor or an actuator.
- b) the states or movement of equipment or materials produced through actuators invoke consequences that have impacts on the developers and providers of IoT services and on other entities.

NOTE – IoT systems categorized as industrial plant and control systems include those for:

- monitoring for maintenance of equipment in a plant;
- remote management of leased machines;
- control for goods manufacturing;
- control of critical infrastructure operation, e.g., operation of electric power supply and water plant.

For more technical critical security controls related to IoT use in critical infrastructure environments, guidance can be found in [b-ETSI TR 103 305-3].

Use cases of these IoT systems are provided in [b-ISO/IEC TR 22417].

6.4.3 Risk scenarios and risks in industrial plant and control systems

Risk scenarios of industrial plant and control systems are inherently linked to the complex interplay of their components and the environment in which they operate. These scenarios arise from a series of risk sources, triggering events, and potential consequences that can significantly impact the safety, reliability, and performance of these critical systems.

- a) Circumstances that involve risk sources
 - 1) Operation of an IoT system relies upon or is affected by:
 - quality, configuration and physical environments of information systems, networks and devices and the software stack that constitutes the IoT system;