International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2068

(03/2015)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

Functional framework and capabilities of the Internet of things

Recommendation ITU-T Y.2068

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

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
Network control architectures and protocols	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.3999

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

Recommendation ITU-T Y.2068

Functional framework and capabilities of the Internet of things

Summary

Recommendation ITU-T Y.2068 provides a description of the basic capabilities of the Internet of things (IoT), based on the functional view, the implementation view and the deployment view of the IoT functional framework described in this Recommendation, in order to fulfil the IoT common requirements specified in Recommendation ITU-T Y.2066.

This Recommendation also describes additional capabilities of the IoT for the integration of cloud computing and big data technologies with the IoT.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2068	2015-03-22	13	11.1002/1000/12419

Keywords

Capability, deployment view, functional component, functional entity, functional framework, functional group, functional view, implementation view, Internet of things, IoT, IoT basic capabilities.

[*] 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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.2068

Functional framework and capabilities of the Internet of things

1 Scope

This Recommendation describes the functional framework of the Internet of things (IoT) in three different views, the IoT basic capabilities, and additional capabilities for the integration of cloud computing and big data technologies with the IoT.

The scope of this Recommendation includes:

- concepts of the IoT functional framework;
- the functional view, the implementation view and the deployment view of the IoT functional framework;
- the IoT basic capabilities fulfilling the common requirements of the IoT specified in [ITU-T Y.2066];
- additional IoT capabilities for the integration of cloud computing and big data technologies with the IoT.

All capabilities of the IoT specified in this Recommendation are numbered and summarized in Annex A.

Appendix I provides an analysis of all capabilities of the IoT specified in this Recommendation in terms of matching with the common requirements of the IoT specified in [ITU-T Y.2066].

NOTE – The detailed specification of the capabilities identified in this Recommendation is outside the scope of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through references 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.2012]	Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.
[ITU-T Y.2060]	Recommendation ITU-T Y.2060 (2012), *Overview of the Internet of things*.
[ITU-T Y.2066]	Recommendation ITU-T Y.2066 (2014), *Common requirements of the Internet of things*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.2 device [ITU-T Y.2060]: 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, data capture, data storage and data processing.

3.1.3 functional entity [ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.1.4 Internet of things (IoT) [ITU-T Y.2060]: 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.

3.1.5 next generation network (NGN) [b-ITU-T Y.2001]: A packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.1.6 thing [ITU-T Y.2060]: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

IoT	Internet of Things
MMCF	Mobility Management and Control Functions
NACF	Network Attachment Control Functions
NGN	Next Generation Network
QoS	Quality of Service
RACF	Resource and Admission Control Functions
TaaS	Things as a Service

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**can optionally**" and "**may**" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Concepts of the IoT functional framework

6.1 Openness and interoperability of the IoT capabilities

The openness of the IoT capabilities refers to opening the networking and service-provisioning functionalities of the IoT to stimulate the innovation ability for IoT technologies and applications development. Through an open, shared, collaborative approach, IoT applications can be developed effectively for business, industry, and social community.

The openness of IoT capabilities can be realized by encapsulating IoT capabilities into service-provisioning interfaces.

The "open IoT capabilities" refer to the set of the IoT capabilities that are required to be opened to IoT applications or users. These IoT capabilities should have open interfaces that can be accessed by IoT applications or users.

The interoperability of the IoT capabilities can be realized by specifying the service-provisioning interfaces in a standardized way.

The "interoperable IoT capabilities" refer to the set of the IoT capabilities that are required to interact between different IoT functional elements, especially when deployed by different service providers. These IoT capabilities are distributed across different functional elements, and collaboration between these different functional elements fulfils their functionalities.

6.2 Completeness, implementability and applicability of the IoT capabilities

The completeness of the IoT capabilities refers to the fact that the whole set of IoT capabilities can fulfil all the common requirements of the IoT [ITU-T Y.2066].

NOTE – There may not be one-to-one mapping between IoT common requirements and IoT capabilities (i.e., one common requirement may involve multiple capabilities).

The implementability of the IoT capabilities refers to the set of the IoT capabilities that can be implemented in the functional elements described in, or reasonably derived from, specifications of existing networks.

The applicability of the IoT capabilities refers to the set of the IoT capabilities that can be deployed in the functional elements of the IoT implementations.

The IoT capabilities specified in this Recommendation should fulfil the requirements of completeness, implementability and applicability. These characteristics of the IoT capabilities specified in this Recommendation are validated by the IoT functional framework.

6.3 The different views of the IoT functional framework

The IoT functional framework consists of the IoT functional elements and their relations. In this Recommendation, the IoT functional framework can be described via three distinct views, i.e., the functional view, the implementation view and the deployment view.

NOTE 1 – The three views reflect three different phases of development of the IoT, namely the design phase, implementation phase, and deployment phase. Each view describes IoT capabilities aiming to fulfil the requirements encountered in different phases of development of the IoT.

NOTE 2 – The IoT functional elements in the functional view are named "functional groups". The IoT functional elements in the implementation view are named "functional entities". The IoT functional elements in the deployment view are named "functional components".

The functional view identifies functional groupings of IoT capabilities. The functional view of the IoT functional framework consists of the IoT "functional groups", and their relations. The functional view of the IoT functional framework is used to describe the completeness of the IoT capabilities by establishing the relations of the IoT capabilities with the common requirements of the IoT.

NOTE 3 – Functional groupings help to simplify the specification and analysis of the IoT capabilities.

The implementation view identifies capabilities of the IoT when implementation of functional groupings is realized. The implementation view of the IoT functional framework consists of the IoT "functional entities", and their relations. The implementation view of the IoT functional framework is used to describe the implementability of the IoT capabilities by establishing the relations of the IoT capabilities with the functional entities described in, or reasonably derived from, specifications of existing networks.

The deployment view identifies capabilities of the IoT when deployment of functional entities is realized. The deployment view of the IoT functional framework consists of the IoT "functional components" (such as gateway for IoT as specified in [b-ITU-T Y.2067]) and their relations. The deployment view of the IoT functional framework is used to describe the applicability of the IoT capabilities by establishing the relations of the IoT capabilities with the functional components deployed in concrete IoT implementations.

The capabilities identified via the three views are the "basic IoT capabilities" which fulfil the common requirements of the IoT [ITU-T Y.2066] (see clause 8). Additional capabilities which fulfil some common requirements of the IoT [ITU-T Y.2066] are identified for the integration of cloud computing and big data technologies with the IoT (see clause 9).

7 The IoT functional framework

7.1 The IoT functional framework in functional view

The IoT functional framework in functional view is to describe the IoT capabilities at the functional level in order to guarantee that the IoT capabilities can fulfil all common requirements of the IoT specified in [ITU-T Y.2066]. A practical way is to describe the IoT capabilities in groups corresponding to all categories of common requirements of the IoT as specified in [ITU-T Y.2066]. The IoT functional framework in functional view consists of groups of the IoT capabilities and their relationships.

In this Recommendation, the groups of the IoT capabilities are named "IoT functional groups". The classification of the IoT functional groups is based on the following requirement categories specified in [ITU-T Y.2066]: application support requirements, service requirements, data management requirements, device requirements, communication requirements, security and privacy protection requirements, and non-functional requirements.

IoT functional group names correspond to those of the requirement categories as follows: application support group, service provision group, data management group, connectivity group, communication group, security and privacy protection group and management group.

7.1.1 The IoT functional groups

The application support group is defined as a group of the IoT capabilities that can fulfil the requirements specified in the category of application support requirements [ITU-T Y.2066].

NOTE 1 – Based on the specifications of the category of application support requirements in [ITU-T Y.2066], this group of capabilities cannot be used directly by IoT users, but can be used by service providers.

NOTE 2 – IoT user, service provider, data manager and thing are the four IoT actors as described in clause 6 of [ITU-T Y.2066]. In this Recommendation, the term "thing" refers to "physical thing" as noted in clause 6.2.1 of [ITU-T Y.2066].

The service provision group is defined as a group of the IoT capabilities that can fulfil the requirements specified in the category of service requirements [ITU-T Y.2066].

NOTE 3 – Based on the specifications of the category of service requirements in [ITU-T Y.2066], this group of capabilities can be used by IoT users, service providers and things.

The data management group is defined as a group of the IoT capabilities that can fulfil the requirements specified in the category of data management requirements [ITU-T Y.2066].

NOTE 4 – Based on the specifications of the category of data management requirements in [ITU-T Y.2066], this group of capabilities can be used by data managers.

The connectivity group is defined as a group of the IoT capabilities that can fulfil the requirements specified in the category of device requirements [ITU-T Y.2066].

NOTE 5 – Based on the specifications of the category of device requirements in [ITU-T Y.2066], this group of capabilities can be used by data managers and things.

The communication group is defined as a group of the IoT capabilities that can fulfil the requirements specified in the category of communication requirements [ITU-T Y.2066].

NOTE 6 – Based on the specifications of the category of communication requirements in [ITU-T Y.2066], this group of capabilities can be used by IoT users, service providers and things.

The security and privacy protection group is defined as a group of the IoT capabilities that can fulfil the requirements specified in the category of security and privacy protection requirements [ITU-T Y.2066].

NOTE 7 – Based on the specifications of the category of security and privacy protection requirements in [ITU-T Y.2066], this group of capabilities can be used by IoT users, things, service providers and data managers.

The management group refers to a group of the IoT capabilities that can fulfil some non-functional requirements, such as manageability, reliability, high availability. The management group includes the capabilities for managing the operations related to application support, service provision, data management, connectivity, and communication of the IoT.

NOTE 8 – Based on the specifications of the category of security and privacy protection requirements in [ITU-T Y.2066], this group of capabilities can be used by IoT users, service providers or data managers.

7.1.2 Relations among the IoT functional groups

Figure 7-1 describes the IoT functional framework in functional view constituted by the IoT functional groups and the relations among these groups. The connectivity group is within the device layer defined in [ITU-T Y.2060], the communication, data management, service, and application support groups are within the network layer and the service support and application support layer defined in [ITU-T Y.2060].

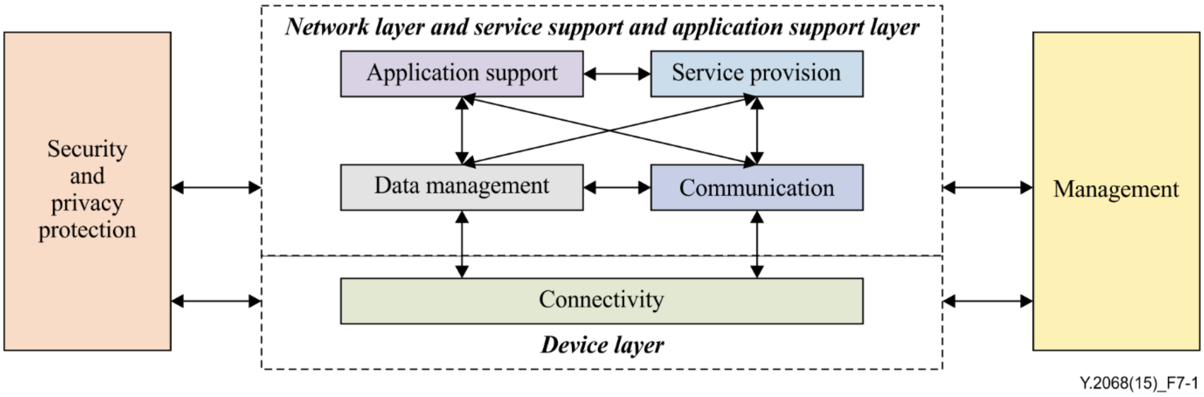

Figure 7-1 – The IoT functional framework in functional view

The connectivity group provides services to the data management group and communication group. The connectivity group can provide services to the communication group and data management group triggered by requests. The security and privacy protection group configures and manages the security and privacy protection aspects of connectivity capabilities, and the management group configures and manages the other aspects of connectivity capabilities.

The communication group provides communication services to the other functional group. The other functional groups use the communication services. The management group configures and manages the communication capabilities. The security and privacy protection group configures and manages the security and privacy protection aspects of communication capabilities.

The data management group provides services to the other functional groups. The other functional groups request and configure the data management services. The management group configures and manages the data management capabilities. The security and privacy protection group configures and manages the security and privacy protection aspects of data management capabilities.

The application support group requests services from the data management group and communication group, and these two groups can provide services to the application support group. The management group configures and manages the application support capabilities. The security and privacy protection group configures and manages the security and privacy protection aspects of application support capabilities.

The service provision group requests services from the data management group and communication group, and these two groups can provide services to the service provision group. The management group configures and manages the service provision capabilities. The security and privacy protection group configures and manages the security and privacy protection aspects of the service provision capabilities.

The security and privacy protection group configures and manages the security and privacy protection aspects of the capabilities in other functional groups.

The management group configures and manages the capabilities, except the security and privacy protection aspects of these capabilities, in other functional groups.

7.2 The IoT functional framework in implementation view

In this Recommendation, the functional entities of the implementation view are only described by their capabilities without mentioning their detailed relationships.

NOTE – There may be different implementation views based on different implementation approaches of the IoT. In this Recommendation, only one implementation view of the IoT functional framework is presented in order to describe and analyse the capabilities of the IoT. It is anticipated that there is no need to cover all possible implementation views of the IoT functional framework: the implementation view of the IoT is in fact only used for showing the implementability of the IoT capabilities, so one implementation view of the IoT is sufficient to show this possibility.

7.2.1 Structure of an implementation view

An implementation view of the IoT functional framework consists of the functional entities of the IoT, and their high level relations. Figure 7-2 illustrates an implementation view of the IoT functional framework based on the IoT reference model specified in [ITU-T Y.2060] and the IoT common requirements specified in [ITU-T Y.2066], and building over functional entities described in the NGN functional architecture [ITU-T Y.2012].

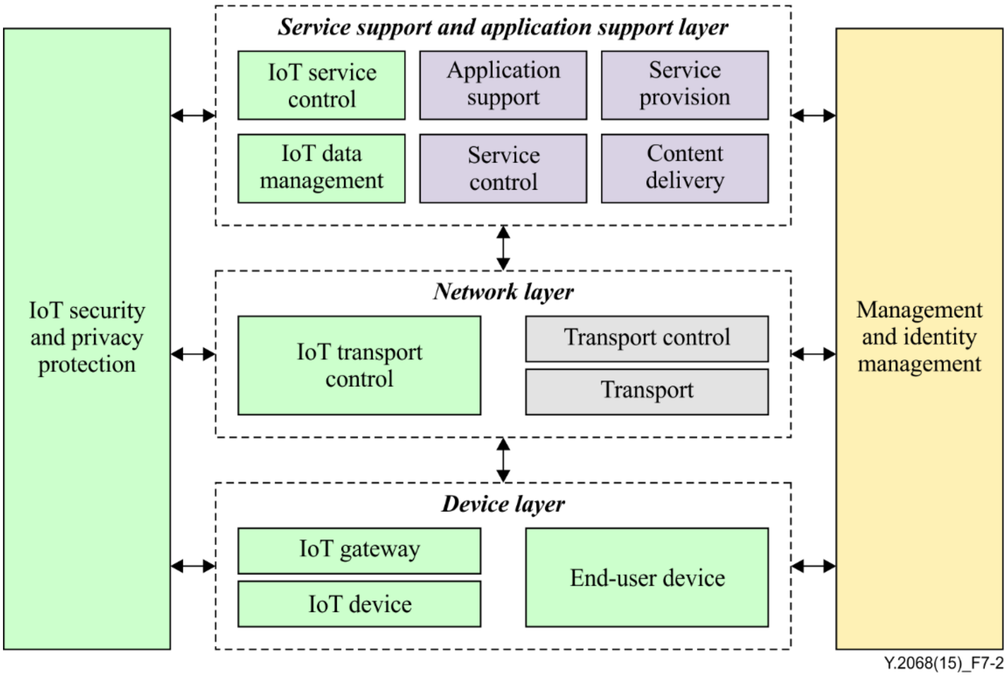

Figure 7-2 – Implementation view of the IoT functional framework building over the NGN functional architecture

There are two classes of functional entities in this implementation view of the IoT functional framework, one is for the functional entities already specified for the NGN [ITU-T Y.2012], and another is for the functional entities specific to the IoT.

The functional entities that are illustrated by green boxes in Figure 7-2 are the functional entities specific to the IoT (to be specified in this Recommendation), while the functional entities illustrated by differently coloured boxes are the functional entities described in [ITU-T Y.2012]. Among the functional entities described in [ITU-T Y.2012], the functional entities illustrated by the same colour belong to a single functional layer except the Management and Identity Management functional entity that crosses all functional layers of the IoT reference model [ITU-T Y.2060].

Even if some end-user functions are already mentioned in NGN Recommendations, these Recommendations only cover specifications on interactions between end-user functions and other NGN functions. There is no specification of end-user functions. In the implementation view, the end-user functions are needed to be described in order to cover the possibility that the IoT device capabilities are implemented in end-user functional entities. The "End-User" functional entity of NGN Recommendations enhanced with some IoT device capabilities is named as "End-User Device" functional entity in this Recommendation.

NOTE 1 – A smart phone configured with sensors and associated application software is an implementation of the End-User Device functional entity.

With respect to the functional entities already specified for the NGN, the Transport and Transport Control functional entities are in the network layer, and the Application Support, Service Provision, Service Control and Content Delivery functional entities are in the service support and application support layer. The Management and Identity Management functional entity crosses all functional layers.

With respect to the functional entities specific to the IoT, the IoT Device, the IoT Gateway and the End-User Device functional entities are in the device layer, the IoT Transport Control functional entity in the network layer, the IoT Data Management and the IoT Service Control functional entities in the service support and application support layer. The IoT Security and Privacy Protection functional entity crosses all functional layers.

NOTE 2 – The functional entities described in this Recommendation located in the service support and application support layer are only related with the generic support capabilities specified in [ITU-T Y.2060].

7.2.2 Functional entities of an implementation view

The Transport functional entity illustrated in Figure 7-2 includes the access network functions, edge functions, core transport functions, gateway functions, and media handling functions as specified in [ITU-T Y.2012].

The Transport Control functional entity illustrated in Figure 7-2 includes resource and admission control functions (RACF), network attachment control functions (NACF), and mobility management and control functions (MMCF) as specified in [ITU-T Y.2012].

The Service Provision functional entity and the Application Support functional entity illustrated in Figure 7-2 include functions such as the gateway, registration, authentication and authorization functions at the application level as specified in [ITU-T Y.2012].

The Service Control functional entity illustrated in Figure 7-2 includes resource control, registration, and authentication and authorization functions at the service level for both mediated and non-mediated services as specified in [ITU-T Y.2012].

The Content Delivery functional entity illustrated in Figure 7-2 receives content from the Application Support functional entity and Service Provision functional entity, stores, processes, and delivers it to the End-User Device functional entity using the capabilities of the Transport functional entity, under control of the Service Control functional entity as specified in [ITU-T Y.2012].

The Management and Identity Management functional entity illustrated in Figure 7-2 includes management functions and identity management functions as specified in [ITU-T Y.2012].

The IoT Device functional entity contains the capabilities of connecting and monitoring things, or controlling things that fulfil the device requirements of the IoT specified in [ITU-T Y.2066].

The IoT Gateway functional entity contains the capabilities of interconnecting devices with networks, buffering and transferring data, and configuring and monitoring devices that fulfil some device requirements and some data management requirements of the IoT specified in [ITU-T Y.2066] and [b-ITU-T Y.2067].

The End-User Device functional entity contains the capabilities of time synchronization, collaboration among services or among devices, reliable and secure human body connectivity, automatic service, intelligent communication, and device mobility to fulfil some application support requirements, service requirements, communication requirements, and device requirements of the IoT specified in [ITU-T Y.2066].

NOTE – As the above capabilities can be distributed in different functional entities, the capabilities contained in the End-User Device functional entity are named by prefixing them with the term "end-user" in order to distinguish them from capabilities residing in other functional entities.

The IoT Data Management functional entity contains the capabilities of semantic annotating, aggregating, storing, and transporting data of things that fulfil the data management requirements of the IoT specified in [ITU-T Y.2066].

The IoT Transport Control functional entity contains the capabilities of configuring and monitoring communication modes, autonomic networking, content-aware communication, and location-based communication that fulfil some communication requirements specified in [ITU-T Y.2066].

The IoT Service Control functional entity contains the capabilities of group management, time synchronization, collaboration among services, configuring and monitoring the semantic based services, autonomic services, location-based and context-aware services that fulfil some service requirements of the IoT specified in [ITU-T Y.2066].

The IoT Security and Privacy Protection functional entity contains the capabilities of performing the operations of security and privacy protection in communication, data management, and service provisioning. These capabilities fulfil some security and privacy protection requirements of the IoT specified in [ITU-T Y.2066].

7.3 The IoT functional framework in deployment view

In this Recommendation, the functional components specified in the deployment view of the IoT functional framework are only described by their capabilities without mentioning their detailed relationships.

NOTE – There may be different deployment views based on different deployment approaches of the IoT. In this Recommendation, only one deployment view of the IoT functional framework is presented in order to describe and analyse the capabilities of the IoT. It is anticipated that there is no need to cover all possible deployment views of the IoT functional framework in the Recommendation: the deployment view of the IoT is in fact only used for showing the applicability of the IoT capabilities, so one deployment view of the IoT is enough to show this possibility.

7.3.1 Structure of a deployment view

A deployment view of the IoT functional framework consists of its functional components and their high level relations. Figure 7-3 illustrates a deployment view of the IoT functional framework based on the IoT reference model specified in [ITU-T Y.2060], the IoT common requirements specified in [ITU-T Y.2066], and the NGN components described in the NGN functional architecture [ITU-T Y.2012].

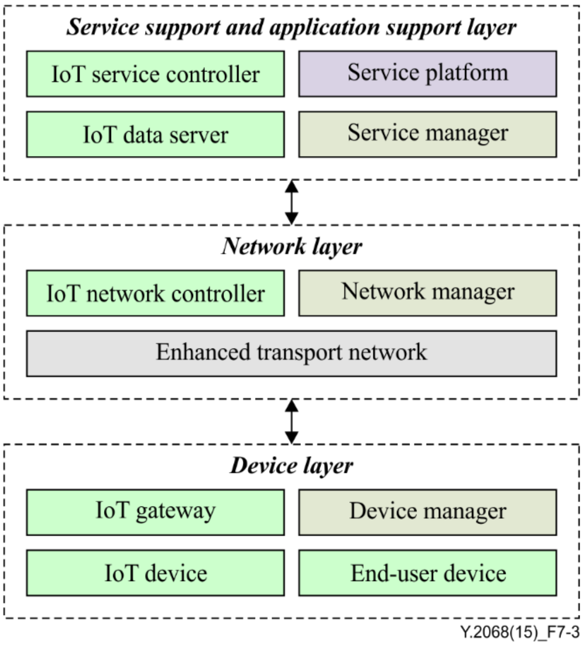

Figure 7-3 – Deployment view of the IoT functional framework building over the NGN components

The functional components that are illustrated by green boxes in Figure 7-3 are the functional components specific to the IoT (to be specified in this Recommendation), while the functional components illustrated by differently coloured boxes are the functional components described or partially described in [ITU-T Y.2012].

The deployment view of the IoT functional framework is only a logical approach for deploying IoT capabilities, and the functional components described in the deployment view can be mapped to physical components of some practical IoT deployments.

The functional components of this deployment view are classified respectively into device layer, network layer, and service support and application support layer as specified in [ITU-T Y.2060]. The cross-layer capabilities specified in [ITU-T Y.2060] are assigned to different functional components (such as Device Manager, Network Manager and Service Manager), distributed in each functional layer, in order to simplify the description and analysis of the IoT capabilities.

The IoT Device, IoT Gateway, End-User Device, and Device Manager functional components belong to the device layer. The Enhanced Transport Network, IoT Network Controller, and Network Manager functional components belong to the network layer. The IoT Data Server, IoT Service Controller, Service Platform, and Service Manager functional components belong to the service support and application support layer.

NOTE – The functional components described in this Recommendation in the service support and application support layer are solely related to generic support capabilities specified in [ITU-T Y.2060].

7.3.2 Functional components of a deployment view

The IoT Device functional component includes the capabilities of the IoT Device functional entity, capabilities of autonomic management and energy management, and capabilities of security and privacy protection.

The IoT Gateway functional component includes capabilities of interconnecting IoT Devices with Enhanced Transport Network, capabilities of aggregating and transferring data of things as well as capabilities of the IoT Device functional component.

The End-User Device functional component includes capabilities of existing networking terminal, and capabilities of the IoT Device functional components.

The Device Manager functional component includes capabilities of identifying and managing devices within a defined domain, and capabilities of autonomic management.

The Enhanced Transport Network functional component includes capabilities of transport and transport control as specified in [ITU-T Y.2012], and enhanced capabilities to fulfil some communication requirements specified in [ITU-T Y.2066].

The IoT Transport Controller functional component includes capabilities of configuring, monitoring, and controlling functionalities of the IoT related communication performed in the Enhanced Transport Network to fulfil communication requirements specified in [ITU-T Y.2066].

The Network Manager functional component includes capabilities of managing the Enhanced Transport Network, and capabilities of security and privacy protection in the Enhanced Transport Network.

The IoT Data Server functional component includes capabilities of storing, querying and managing data of things, and contains database and data management related with data of things.

The IoT Service Controller functional component includes capabilities of configuring, monitoring, and controlling functionalities of IoT application support and service provision performed in Service Platform to fulfil some application support requirements and service requirements of the IoT specified in [ITU-T Y.2066].

The Service Platform functional component includes capabilities of Application Support, Service Provision, Content Delivery, Service Control, and other enhanced capabilities to fulfil some application support requirements and service requirements specified in [ITU-T Y.2066].

The Service Manager functional component includes capabilities of managing both Service Platform and the IoT Service Controller, and capabilities of Security and Privacy Protection for Service Platform and for the IoT Service Controller.

8 The IoT basic capabilities

The IoT basic capabilities in this Recommendation refer to the capabilities that fulfil the common requirements of the IoT as specified in [ITU-T Y.2066].

Clauses 8.1 to 8.7 describe the IoT basic capabilities. These same capabilities are numbered and summarized in Annex A.

NOTE – In clauses 8.1 to 8.7, the capability numbers, as shown in Annex A, appear between square brackets at the end of the description of the corresponding capability.

8.1 Service provision capabilities

Service provision capabilities include service prioritization, semantic based service, service composition, mobility service, autonomic service, location-based and context-aware service, service management, service discovery, service subscription, naming and addressing, virtual storage and processing capabilities, adaptable service provision, and service provision acknowledgement.

- Service prioritization capability involves the abilities of providing services in different priorities, such as querying data or transferring data in different priorities [C-1-1].
- Semantic based service capability involves the abilities of semantically annotating data or service, semantically querying data or semantically requesting services [C-1-2].

NOTE – Semantic based service capability enables the description and exchange of semantics between services in order to support, for example, automatic service customization.

- Service composition capability involves the abilities of creating new services or customized services based on existing capabilities and user specific requirements [C-1-3].
- Mobility service capability involves the abilities of remote access to the IoT, and remote authentication of users [C-1-4].
- Autonomic service capability involves the abilities of automatic capturing, transferring, and analysing data of things, and automatic service provisioning based on predefined rules or policies [C-1-5].
- Location-based and context-aware service capability involves the abilities of automatically provisioning services based on location and context information, and predefined rules or policies [C-1-6].
- Service discovery capability involves the abilities of discovering IoT users, services, devices and things [C-1-7].
- Service subscription capability involves the abilities of subscribing the needed services and associated data of things by IoT users [C-1-8].
- Naming and addressing capability involves the abilities of creating, updating, deleting, querying names and addresses of users, devices and things [C-1-9].
- Virtual storage and processing capability involves the abilities of providing storage and processing resources in a scalable way [C-1-10].
- The capability of adaptable service provision involves the abilities of extending service configurations to provide new services as required by applications or users of the IoT in order to be adaptable to different applications or users of the IoT [C-1-11].

- The capability of service provision acknowledgement involves the abilities of acknowledging the correct service provision requested by applications or users of the IoT in order to support reliable service provision in the IoT [C-1-12].

8.2 Communication capabilities

The communication group includes event-based communication, periodic communication, self-configuring for networking, self-healing for networking, self-optimizing for networking, self-protection for networking, multicast communication, unicast communication, broadcast communication, anycast communication, error control for communication, Quality of Service enabling communication, content-aware communication, location-based communication, transport acknowledgement and adaptable networking capabilities.

- Event-based communication capability enables IoT devices and service provider to initiate communication based on predefined events [C-2-1].
- Periodic communication capability enables IoT devices and service provider to periodically initiate communication based on predefined rules [C-2-2].

NOTE 1 – In the perspective of network performance, it is required that the usage of event-based or periodic communication capabilities be avoided, unless there is a specific reason to communicate using these capabilities.

- Unicast communication capability enables the IoT to transfer messages from the source entity to single destination entity [C-2-3].
- Multicast communication capability enables the IoT to transfer messages from the source entity to a group of destination entities simultaneously [C-2-4].
- Broadcast communication capability enables the IoT to transfer messages to all destination entities of a given domain [C-2-5].
- Anycast communication capability enables the IoT to transfer messages to any of the destination entities of a given domain [C-2-6].
- The capability of error control for communications involves the abilities of ensuring correct message transfer from source entity to destination entity [C-2-7].
- Quality of Service enabling communication capability provides mechanisms to enable support of Quality of Service for message transfer from source entity to destination entity [C-2-8].
- The capability of self-configuring for networking involves the abilities of automatically configuring networking parameters based on discovered network interfaces and predefined rules [C-2-9].
- The capability of self-healing for networking involves the abilities of automatically recovering from fault status of networking based on monitoring and predefined rules [C-2-10].
- The capability of self-optimizing for networking involves the abilities of automatically optimizing networking operations based on monitoring and predefined rules [C-2-11].
- The capability of self-protecting for networking involves the abilities of automatically protecting networking entities from harmful operations based on predefined rules [C-2-12].
- Content-aware communication capability involves the abilities of selecting path and routing of messages based on content and predefined rules [C-2-13].

NOTE 2 – This capability can be used to block messages based on the specified content and predefined rules.

- The capability of location-based communication involves the abilities of identifying locations and initiating communication control based on identified locations and predefined rules [C-2-14].

- The capability of transport acknowledgement involves the abilities of acknowledging the correct message delivery to support reliable communications as required by IoT applications [C-2-15].
- The capability of adaptable networking involves the abilities of extending networking configurations for connecting to emerging communication networks of the IoT [ITU-T Y.2060] in order to be adaptable to different networking technologies [C-2-16].

8.3 Application support capabilities

The application support group includes programmable interface provision, group management, time synchronization, orchestration, user management, and application operation acknowledgement capabilities.

- The capability of programmable interface provision involves the abilities of supporting new services or customized services based on existing capabilities and application specific requirements [C-3-1].
- The capability of group management involves the abilities of creating, modifying, deleting, and querying IoT groups, and adding, modifying, deleting and querying IoT group members [C-3-2].
- The capability of time synchronization involves the abilities of synchronizing the time among related functional components in a reliable way, in order to support global or local time stamping for applications [C-3-3].
- Orchestration capability involves the abilities of automatic arrangement and coordination of service provisioning or device operations in order to fulfil application specific requirements [C-3-4].
- User management capability involves the abilities of creating, querying, updating and deleting IoT user profiles, and authenticating, authorizing, registering and auditing IoT users [C-3-5].
- The capability of application support operation acknowledgement involves the abilities of acknowledging the correct operations requested by applications in order to support reliable application operations in the IoT [C-3-6].

8.4 Data management capabilities

The data management group includes data storage, data processing, data querying, data access control, open information exchange, semantic data operation and autonomic data operation capabilities.

- The capability of data storage involves the ability of storing data of things based on predefined rules and policies [C-4-1].
- The capability of data processing involves the ability of data fusion and mining based on predefined rules and policies [C-4-2].

NOTE 1 – Data processing refers to a set of data operations in order to fulfil the application requirements. Data processing in the IoT includes collecting, representing, fusing, mining, and interpreting the data of things. From an application perspective, data processing can be regarded as data analysis that consists of data fusing and data mining. From an implementation perspective, the operation of data fusing includes data collection and data representation, and the operation of data mining includes data interpretation.

- The capability of data querying involves the ability of querying information about things connected to the IoT [C-4-3].
- The capability of data access control involves the abilities of controlling and monitoring data access operations by the owners of the data [C-4-4].

- The capability of open information exchange involves the abilities of sending data to or receiving data from external data sources, e.g., data centres and data servers outside the IoT [C-4-5].
- The capability of semantic data operation involves the abilities of semantic annotating, semantic discovering, semantic storing, and semantic composing data of things to fulfil the requirements of IoT users or applications [C-4-6].
- The capability of autonomic data operation involves the abilities of automatically collecting, aggregating, transferring, storing, analysing data of things, and automatically managing these data operations for support of operating data of things in a scalable way [C-4-7].

NOTE 2 – This capability can be used to face the impact of big data in the IoT.

8.5 Management capabilities

The management group includes capabilities fulfilling the IoT interoperability requirements, capabilities fulfilling the IoT scalability requirements, capabilities fulfilling the IoT reliability requirements, capabilities fulfilling the IoT high availability requirements, and capabilities fulfilling the IoT manageability requirements.

NOTE – The abilities involved in the management capabilities specified in this Recommendation may be operated in a remote way. Remote operation can be disabled based on security or other policy considerations.

8.5.1 Capabilities fulfilling IoT interoperability requirements

The capabilities fulfilling the IoT interoperability requirements specified in [ITU-T Y.2066] include managing data models for exchanging data of things, managing service description, managing network configuration, managing device configuration, managing security policy, and managing privacy protection policy capabilities.

- The capability of managing data models for exchanging data of things involves the abilities of creating, querying and updating data models for support of interoperability among IoT applications. This capability also includes the abilities of creating and updating data models for support of semantic interoperability among IoT applications [C-5-1].
- The capability of managing service description involves the abilities of creating, querying and updating service description for support of service interoperability [C-5-2].
- The capability of managing network configuration involves the abilities of creating, querying and updating network configuration for support of network interoperability [C-5-3].
- The capability of managing device configuration involves the abilities of creating, querying and updating network configuration for support of device interoperability [C-5-4].
- The capability of managing security policy involves the abilities of creating, querying and updating security policy for support of interoperability between different implementations of security policy [C-5-5].
- The capability of managing privacy protection policy involves the abilities of creating, querying and updating privacy protection policy for support of interoperability between different implementations of privacy protection policy [C-5-6].

8.5.2 Capabilities fulfilling the IoT scalability requirements

The capabilities fulfilling the IoT scalability requirements specified in [ITU-T Y.2066] include managing distributed processing and managing multiple domains.

- The capability of managing distributed processing involves the abilities of managing IoT functional components in a distributed way for support of IoT scalability [C-5-7].
- The capability of managing multiple domains involves the abilities of managing IoT functional components in multiple domains for support of IoT scalability [C-5-8].

8.5.3 Capabilities fulfilling the IoT reliability requirements

The capabilities fulfilling the IoT reliability requirements specified in [ITU-T Y.2066] include redundant deployment enablement capability.

- The capability of redundant deployment enablement involves the abilities of enabling deployment of redundant functional components of the IoT to guarantee reliability required in communication, service provision and data management [C-5-9].

8.5.4 Capabilities fulfilling the IoT high availability requirements

The capabilities fulfilling the IoT high availability requirements specified in [ITU-T Y.2066] include service integrity check, data integrity check, device integrity check, security integrity check and user integrity check capabilities.

- The capability of service integrity check involves the abilities of checking the service lifetime, the available resources required to provide the service in order to guarantee the high availability of service provisioning [C-5-10].
- The capability of data integrity check involves the abilities of checking the data lifetime, the available attributes of the data, and the consistency of data in order to guarantee the high availability of data management [C-5-11].
- The capability of device integrity check involves the abilities of checking the status of all functions of device to guarantee the high availability of IoT devices [C-5-12].
- The capability of security integrity check involves the abilities of checking the consistency of security policies deployed in all functional components of the IoT to guarantee the high availability of security in the IoT [C-5-13].
- The capability of user profile integrity check involves the abilities of checking the lifetime, subscription, privacy protection and availability of services subscribed to by users to guarantee the high availability of service provisioning and privacy protection for users [C-5-14].

8.5.5 Capabilities fulfilling the IoT manageability requirements

The capabilities fulfilling the IoT manageability requirements specified in [ITU-T Y.2066] include managing devices, managing networks, managing services, managing data operations, managing security operations, managing privacy protection, managing user operations, and plug and play capabilities.

- The capability of managing devices involves the abilities of configuring, monitoring, diagnosing and recovering devices of the IoT, and updating device software to enhance capabilities of devices of the IoT [C-5-15].
- The capability of managing networks involves the abilities of configuring, monitoring, accounting and charging, optimizing, diagnosing and recovering networks of the IoT [ITU-T Y.2060], and updating network software to enhance capabilities of networks of the IoT [C-5-16].
- The capability of managing services involves the abilities of describing, configuring, monitoring, accounting and charging, optimizing, recovering, and updating services of the IoT [C-5-17].
- The capability of managing data operations involves the abilities of configuring, monitoring, accounting and charging, optimizing and recovering data operations, and updating software related with data operations to enhance capabilities of the IoT [C-5-18].
- The capability of managing security operations involves the abilities of configuring, monitoring, auditing, diagnosing and recovering security operations, and updating software related with security operations to enhance capabilities of the IoT [C-5-19].

- The capability of managing privacy protection involves the abilities of configuring, monitoring, auditing and recovering privacy protection, and updating software related with privacy protection to enhance capabilities of the IoT [C-5-20].
- The capability of managing user operations involves the abilities of configuring, monitoring, accounting and charging, optimizing, diagnosing and recovering operations of IoT users, and updating software related with operations of IoT users to enhance capabilities of IoT [C-5-21].
- Plug and play capability involves the abilities of automatic configuring, connecting and activating devices of the IoT to enable on-the-fly semantic-based configuration and activation of IoT devices [C-5-22].

8.6 Connectivity capabilities

The connectivity group includes identification-based connectivity, things' status notification device mobility capability, and adaptable connectivity capabilities.

- The capability of identification-based connectivity involves the abilities of establishing the connectivity based on the identification of things [C-6-1].
- The capability of things' status notification involves the abilities of automatic notification of the status of things and its changes based on predefined rules [C-6-2].
- The capability of device mobility involves the abilities of keeping the connectivity with the IoT when a device moves [C-6-3].
- The capability of adaptable connectivity involves the abilities of extending connectivity configurations to enable connectivity of new types of devices to the IoT in order to be adaptable to different device technologies [C-6-4].

8.7 Security and privacy protection capabilities

The security and privacy protection group includes communication security capability, data management security capability, service provision security capability, security integration capability, mutual authentication and authorization capability, and security audit capability.

- Communication security capability involves the abilities of supporting secure, trusted and privacy-protected communication [C-7-1].
- Data management security capability involves the abilities of providing secure, trusted and privacy-protected data management [C-7-2].
- Service provision security capability involves the abilities of providing secure, trusted and privacy-protected service provision [C-7-3].
- Security integration capability involves the abilities of integrating different security policies and techniques related to the variety of IoT functional components [C-7-4].
- Mutual authentication and authorization capability involves the abilities of authenticating and authorizing each other before a device accesses the IoT based on predefined security policies [C-7-5].
- Security audit capability involves the abilities of monitoring any data access or attempt to access IoT applications in a fully transparent, traceable and reproducible way based on appropriate regulation and laws [C-7-6].

NOTE – These security and privacy protection capabilities include also the ability of coping with the security and privacy protection issues for operations across different domains.

9 IoT capabilities for integration of key emerging technologies

The following clauses describe the IoT capabilities for integration of some key emerging technologies, in alignment with the IoT capabilities list provided in Annex A. In the following clauses, the capability numbers, as shown in Annex A, are put between square brackets "[ ]" and inserted at the end of each paragraph describing the corresponding capability.

Clauses 9.1 and 9.2 describe the additional IoT capabilities for integration of cloud computing technologies and big data technologies.

NOTE – This Recommendation does not prevent more additional capabilities for integration with the IoT of other emerging technologies, such as network function virtualization and software-defined networking, to be considered further.

9.1 Capabilities for integration of cloud computing technologies

Owing to the high scalability, energy efficiency and deployment efficiency requirements of the IoT, there are some great challenges in the deployment of the IoT. Some key features of cloud computing technologies, such as virtualization and resource sharing, can help to improve scalability, energy efficiency (i.e., reduce the energy consumption) and deployment efficiency (e.g., reduce the memory and bandwidth usage) for the IoT. Additional capabilities for the integration of cloud computing technologies with the IoT are required.

With the integration of cloud capabilities of the infrastructure capabilities type [b-ITU-T Y.3500] into the IoT, the IoT infrastructure can be deployed utilizing these cloud capabilities. In this way, the IoT infrastructure can increase its scalability for computing, data storage and other aspects, and also increase energy efficiency. The capability of accessing virtual processing resources and the capability of accessing virtual storage resources are required in order to integrate with cloud capabilities of the infrastructure capabilities type.

- The capability of accessing virtual processing resources involves the abilities of adopting the capabilities specified in infrastructure capabilities type of cloud to use processing resource deployed in cloud [C-8-1].
- The capability of accessing virtual storage resources involves the abilities of adopting the capabilities specified in infrastructure capabilities type of cloud to use storage resource deployed in cloud [C-8-2].

With the integration of cloud capabilities of the platform capabilities type [b-ITU-T Y.3500] into the IoT, the IoT can deploy its platform according to this type of cloud capability. In such a way, the IoT can provide flexibility for the usage of IoT application support and service support capabilities, e.g., IoT application providers can more easily deploy IoT applications based on the platform of the IoT.

With the integration of cloud capabilities of the application capabilities type [b-ITU-T Y.3500] into the IoT, the IoT can deploy IoT applications according to this type of capability. In such a way, IoT applications can be used more flexibly.

Things as a Service (TaaS) can be considered as a cloud service category whose things-related services (e.g., accessing, subscription and notification of things-related data, and management and control of things-related devices) are provided to cloud service customers. TaaS offers cloud capabilities of the platform capabilities type and/or application capabilities type based on the IoT infrastructure. Via TaaS, IoT applications and/or IoT users can easily use the desired things-related services (e.g., get the desired things-related data, and control the desired things-related devices).

In order to integrate cloud computing technologies for implementation of TaaS, the additional capabilities of publishing things as services, summarizing data of things, and synchronizing data with things are required.

- The capability of publishing things as services involves the abilities of adopting the capabilities specified in the platform capabilities type of cloud to deploy things-related services [C-8-3].
- The capability of summarizing data of things involves the abilities of collecting and aggregating in the service support and application support layer of the IoT reference model [ITU-T Y.2060] the data of things related with the required things-related services for their provision to cloud users [C-8-4].
- The capability of synchronizing data with things involves the abilities of creating, deleting, and updating the data of things just in time with respect to application requirements, based on the updated status of sensed things in order to guarantee the quality of TaaS [C-8-5].

NOTE – The above identified capabilities of publishing things as services, summarizing data of things and synchronizing data with things are additional capabilities that are required for the integration of cloud computing technologies with the IoT in order to provide TaaS, they are not part of the IoT basic capabilities specified in clause 8 of this Recommendation.

9.2 Capabilities for integration of big data technologies

The development of the IoT causes rapid growth of IoT data. As there will be a large number of devices connected with the IoT and a large number of IoT services will flourish, there will be a large amount of IoT data created and used in the IoT.

Major characteristics of IoT data relevant for the integration of big data technologies into the IoT are:

a) Massive quantity (volume): the IoT infrastructure connects countless physical things and virtual things. These interactions and data aggregations produce huge data in the information world [ITU-T Y.2060], including not only the data collected by sensors, but also other data of the IoT infrastructure, e.g., other data concerning devices and data concerning networks, platforms and applications.

b) Heterogeneity (variety): IoT data are heterogeneous (data types and sources). For instance, IoT data related to healthcare applications usually differ from those related to transportation applications, not only from a structure (i.e., format) point of view but also from a semantic point of view.

c) Coexistence of structured and un-structured data (variety): structured data and un-structured data coexist in the IoT. Structured data are generally more efficient than un-structured data for data management.

d) High speed of data generation and processing (velocity): the collection and aggregation at the IoT device layer of data from a huge number of data sources form constantly large and high speed flows; the support of IoT application requirements may require processing of the data of things at high speed, e.g., for applications requiring real-time decision making.

e) Frequent update or change of the values of data (volatility): the values of data of things are changed or updated frequently over a period of time as they have to reflect the status of things, and update the services related with things, just in time as required by IoT applications.

f) Contextualization: a lot of IoT data are meaningful only if they are collected and integrated with related contextual data in order to provide context-aware services.

Data management capability of the IoT can be enhanced by big data technologies for transferring, storing, processing, validating and querying IoT data more efficiently, as well as for extracting information and actionable knowledge from IoT data. Besides, additional capabilities for the integration of big data technologies are also required.

The required additional capabilities for the integration of big data technologies are the capabilities of adopting big data collection, adopting big data aggregation, adopting big data storage, adopting big data integration, adopting big data query, and adopting big data analysis.

- The capability of adopting big data collection involves the abilities of adopting the technologies of big data collection [C-9-1].
- The capability of adopting big data aggregation involves the abilities of adopting the technologies of big data aggregating from different sources in the device layer of the IoT reference model as specified in [ITU-T Y.2060] [C-9-2].
- The capability of adopting big data storage involves the abilities of adopting the technologies of big data storing [C-9-3].
- The capability of adopting big data integration involves the abilities of adopting the technologies of big data summarizing from different sources in the service support and application support layer of the IoT reference model as specified in [ITU-T Y.2060] [C-9-4].
- The capability of adopting big data query involves the abilities of adopting the technologies of big data query [C-9-5].
- The capability of adopting big data analysis involves the abilities of adopting the technologies of big data analysis [C-9-6].

10 Security considerations

Security is a fundamental aspect to be considered in IoT technical specifications. The security issues in IoT can be divided into two groups: one is about the usual security threats, and another is about privacy protection that is particularly significant in IoT. This Recommendation considers the security issues from both the IoT functional framework perspective and the IoT basic capabilities perspective.

In the functional view of the IoT functional framework described in clause 7.1, the security and privacy protection functional group is specified. In the implementation view of the IoT functional framework described in clause 7.2, the IoT security and privacy protection functional entity is specified. In the deployment view of the IoT functional framework described in clause 7.3, the functional components of device manager, network manager, and service manager are specified to contain the capabilities of security and privacy protection.

Among the IoT basic capabilities described in clause 8, the capabilities of security and privacy protection are described in clause 8.7, and the management capabilities related with security and privacy protection are described in clause 8.5. These capabilities fulfil the IoT common requirements on security and privacy protection specified in [ITU-T Y.2066].

Annex A

The IoT capabilities list

(This annex forms an integral part of this Recommendation.)

Tables A.1 to A.9 list and number the capabilities identified in this Recommendation.

Tables A.1 to A.9 have similar formats.

The first column is headed "capability number" and assigns a number to each IoT capability. The numbering rule for each IoT capability is as follows: C-<the sub-clause number of clause 8 or 7+sub-clause number of clause 9>-<the sequence number of each IoT capability in each sub-clause>. For example, the first IoT capability described in clause 8.1 is numbered C-1-1.

The second column is headed "capability name" and gives the name of each IoT capability.

The third column is headed "capability summary" and briefly describes what the capability does.

The fourth column is headed as "related requirement(s)" and describes the common requirement(s) specified in [ITU-T Y.2066] to be fulfilled by the capability.

NOTE – One IoT capability may fulfil several requirements, and several IoT capabilities may fulfil the same single requirement.

The fifth column is headed "associated component(s)" and lists the functional components (from clause 7.3) associated with the IoT capability. This column can be used to validate that the IoT capability can be implemented and deployed.

Table A.1 – List of service provision capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-1-1	Service prioritization	Service prioritization involves the abilities of providing services in different priorities, such as querying data or transferring data in different priorities.	Prioritization of services is required to fulfil the different service requirements of different groups of IoT users.	Service platform, IoT service controller
C-1-2	Semantic based service	Semantic based service involves the abilities of semantic annotating data or service, semantic querying data, or semantic requesting services.	Semantic based services are required to support autonomic service provisioning.	Service platform, IoT data server
C-1-3	Service composition	Service composition involves the abilities of creating customized services based on existing capabilities.	Service composition is required to support flexible service creation.	Service platform, service manager

Table A.1 – List of service provision capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-1-4	Mobility service	Mobility service involves the abilities of remote accessing service platform, remote authenticating users, and remote requesting services.	Mobility services are required to support service mobility, user mobility and device mobility.	Service platform, service manager
C-1-5	Autonomic service	Autonomic service involves the abilities of automatic capturing, transferring, and analysing data of things, and automatic providing services based on predefined rules or policies.	Autonomic services are required to enable automatic capture, communication and processing of data of things.	Service platform, service manager, IoT service controller
C-1-6	Location-based and context-aware service	Location-based and context-aware service involves the abilities of automatic providing services based on the location information and related context and predefined rules or policies.	Location-based and context-aware services are required to enable flexible, user customized and autonomic services based on the location information and/or related context.	Service platform, service manager, IoT service controller
C-1-7	Service discovery	Service discovery involves the abilities of discovering IoT users, services, devices and data of things.	Discovery services are required to support discover IoT users, services, devices and data of things.	Service manager, IoT data server, device manager
C-1-8	Service subscription	Service subscription involves the abilities of subscribing the needed services and associated data of things by IoT users.	Service subscription support is required to allow the IoT user to subscribe the needed services and associated data of things.	Service manager, IoT data server
C-1-9	Standardized naming and addressing	Standardized naming and addressing involves the abilities of creating, updating, deleting, querying names and addresses of users, devices and things.	Standardized naming and addressing is required to support interoperability among different domains.	Service manager, network manager, device manager

Table A.1 – List of service provision capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-1-10	Virtual storage and processing	Virtual storage and processing involves the abilities of providing storage and processing resources in a scalable way.	Virtual storage and processing capabilities are required to support storing and processing a large amount of data (big data).	Service platform, IoT data server
C-1-11	Adaptable service provision	The capability of adaptable service provision involves the abilities of extending service configurations to provide new services as required by applications or users of the IoT in order to be adaptable to different applications or users of the IoT.	Adaptability to the new technologies emerging in the future is required in the IoT.	Service platform, service manager
C-1-12	Service provision acknowledgement	The capability of service provision acknowledgement involves the abilities of acknowledging the correct service provision requested by applications or users of the IoT to support reliable service provision in the IoT.	Reliability in capabilities of the IoT, such as reliability in communication, service and data management capabilities of the IoT, is required.	Service platform

Table A.2 – List of communication capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-2-1	Event-based communication	Event-based communication capability enables IoT devices and service provider to initiate communication based on predefined events.	Event-based communication between devices or between IoT users is required to be supported.	IoT device, IoT gateway, end-user device, service platform
C-2-2	Periodic communication	Periodic communication capability enables IoT devices and service provider to periodically initiate communication based on predefined events.	Periodic communication between devices or between IoT users is required to be supported.	IoT device, IoT gateway, end-user device, service platform

Table A.2 – List of communication capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-2-3	Unicast communication	Unicast communication capability enables transport network to transfer messages from the source entity to single destination entity.	The support of the unicast communication mode between IoT users or devices is required.	Enhanced transport network
C-2-4	Multicast communication	Multicast communication capability enables transport network to transfer messages from the source entity to a group of destination entities simultaneously	The support of the multicast communication modes is required to provide communication services within a group of IoT users or devices.	Enhanced transport network
C-2-5	Broadcast communication	Broadcast communication capability enables transport network to transfer messages to all nodes of a given network area	The support of the broadcast communication modes is required to support the collaboration among IoT users or devices.	Enhanced transport network
C-2-6	Anycast communication	Anycast communication capability enables transport network to transfer messages to any one node of a given network area.	The support of the anycast communication modes is required to support the collaboration among IoT users or devices.	Enhanced transport network
C-2-7	Error control for communications	Error control for communications capability involves the abilities of ensuring to transfer data correctly from end to end.	Error control for communications is required to be supported.	IoT device, IoT gateway, end-user device, IoT network controller
C-2-8	Quality of Service enabling communication	Quality of Service enabling communication capability provides some mechanisms to guarantee the delivery and processing of time-critical messages	Time-critical communications are required to be supported.	IoT device, IoT gateway, end-user device, IoT network controller

Table A.2 – List of communication capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-2-9	Self-configuring for networking	The capability of self-configuring for networking involves the abilities of automatically configuring networking parameters based on discovered networking interfaces and predefined rules.	Autonomic networking is required.	IoT device, IoT gateway, end-user device, network manager
C-2-10	Self-healing for networking	The capability of self-healing for networking involves the abilities of automatically recovering from fault status of networking based on monitoring results and predefined rules.	Autonomic networking is required.	IoT device, IoT gateway, end-user device, network manager
C-2-11	Self-optimizing for networking	The capability of self-optimizing for networking involves the abilities of automatically optimizing networking operations based on monitoring results and predefined rules.	Autonomic networking is required.	IoT device, IoT gateway, end-user device, network manager
C-2-12	Self-protecting for networking	The capability of self-protecting for networking involves the abilities of automatically protecting entities of networking from harmful operations based on predefined rules.	Autonomic networking is required.	IoT device, IoT gateway, end-user device, network manager
C-2-13	Content-aware communication	Content-aware communication capability involves the abilities of identifying content and selecting path and routing messages based on content, or blocking messages based on content.	Content-aware communication is required for support of path selection and routing of communications based on content.	IoT device, IoT gateway, end-user device, IoT network controller
C-2-14	Location-based communication	The capability of location-based communication involves the abilities of identifying locations and initiating communication based on predefined rules.	Location-based communication is required.	IoT device, IoT gateway, end-user device, IoT network controller

Table A.2 – List of communication capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-2-15	Transport acknowledgement	The capability of transport acknowledgement involves the abilities of acknowledging correctly received messages to support reliable communications as required by IoT applications.	Reliability in capabilities of IoT, such as reliability in communication, service and data management capabilities of the IoT, is required.	Enhanced transport network, IoT device, IoT gateway, end-user device
C-2-16	Adaptable networking	The capability of adaptable networking involves the abilities of extending networking configurations to connect with emerging IoT to be adaptable to different networking technologies.	Adaptability to the new technologies emerging in the future is required in the IoT.	Enhanced transport network, network manager, IoT device, IoT gateway, end-user device, device manager

Table A.3 – List of application support capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-3-1	Programmable interface provision	The capability of programmable interface provision involves the abilities of supporting new services or customized services based on existing capabilities and application specific requirements.	Programmable interfaces are required to be standardized to provide open access to application support capabilities.	Service platform
C-3-2	Group management	The capability of group management involves the abilities of creating, modifying, deleting, and querying IoT groups, and adding, modifying, deleting and querying IoT group members.	Group management is required.	Service platform

Table A.3 – List of application support capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-3-3	Time synchronization	The capability of time synchronization involves the abilities of synchronizing the time among related functional components in reliable way, in order to support global or local time stamping for applications.	Reliable time synchronization is required.	Service platform
C-3-4	Orchestration	Orchestration capability involves the abilities of automatic arrangement and coordination of service provisioning or device operations to fulfil application specific requirements.	Collaboration is required.	IoT device, IoT gateway, end-user device, service platform
C-3-5	User management	User management capability involves the abilities of creating, querying, updating and deleting IoT user profiles, and authenticating, authorizing, registering and auditing IoT users.	User management is required.	Service platform
C-3-6	Application support operation acknowledgement	The capability of application support operation acknowledgement involves the abilities of acknowledging correct operations requested by applications to support reliable application operations in the IoT.	Reliability in capabilities of the IoT, such as reliability in communication, service and data management capabilities of the IoT, is required.	IoT data server, IoT gateway

Table A.4 – List of data management capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-4-1	Data storage	The capability of data storage involves the ability of storing data of things based on predefined rules and policies.	Storing data of things is required to be supported.	IoT data server, IoT gateway

Table A.4 – List of data management capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-4-2	Data processing	The capability of data processing involves the ability of data fusion and mining based on predefined rules and policies.	Processing data of things is required to be supported.	IoT data server
C-4-3	Data querying	The capability of data querying involves the ability of querying historical information about things	Querying historical data of things is required to be supported.	IoT data server
C-4-4	Data access control	The capability of data access control involves the abilities of controlling and monitoring the data access operations by the owners of data.	Data access control by the data owners is required.	IoT data server
C-4-5	Open information exchange	The capability of open information exchange involves the abilities of sending data to or receiving data from external data sources, e.g., data centres and data servers outside the IoT.	Data exchange with entities outside the IoT is required to be supported.	IoT data server
C-4-6	Semantic data operation	The capability of semantic data operation involves the abilities of semantic annotating, semantic discovering, semantic storing and semantic composing data of things to fulfil the requirements of IoT users or applications	Semantic annotation and semantic access to data of things are required. Semantic storage, transfer and aggregation of data of things are required.	IoT data server, IoT gateway
C-4-7	Autonomic data operation	The capability of autonomic data operation involves the abilities of automatically collecting, aggregating, transferring, storing, analysing data of things, and automatically managing these data operations for support of operating data of things in a scalable way.	Scalability is required to be supported in the IoT in order to handle a large amount of devices, applications and users.	IoT device, IoT gateway, end-user device, IoT data server

Table A.5 – List of management capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-5-1	Managing data models for exchanging data of things	The capability of managing data models for exchanging data of things involves the abilities of creating, querying and updating data models for support of interoperability among IoT applications. This capability also includes the abilities of creating and updating data models for support of semantic interoperability among IoT applications.	Interoperability is required to be ensured among heterogeneous IoT implementations.	IoT data server
C-5-2	Managing service description	The capability of managing service description involves the abilities of creating, querying and updating service description for support of service interoperability.	Interoperability is required to be ensured among heterogeneous IoT implementations.	Service manager, service platform
C-5-3	Managing network configuration	The capability of managing network configuration involves the abilities of creating, querying and updating network configuration for support of network interoperability.	Interoperability is required to be ensured among heterogeneous IoT implementations.	Network manager, enhanced transport network
C-5-4	Managing device configuration	The capability of managing device configuration involves the abilities of creating, querying and updating network configuration for support of device interoperability.	Support for heterogeneous device related communication technologies is required.	Device manager, IoT device, IoT gateway, end-user device
C-5-5	Managing security policy	The capability of managing security policy involves the abilities of creating, querying and updating security policy for support of interoperability between different implementations of security policy.	Interoperability is required to be ensured among heterogeneous IoT implementations.	Service manager, network manager, device manager

Table A.5 – List of management capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-5-6	Managing privacy protection policy	The capability of managing privacy protection policy involves the abilities of creating, querying and updating privacy protection policy to support interoperability between different implementations of privacy protection policy.	Interoperability is required to be ensured among heterogeneous IoT implementations.	Service manager, network manager, device manager
C-5-7	Managing distributed processing	The capability of managing distributed processing involves the abilities of managing IoT functional components in a distributed way to support IoT scalability.	Scalability is required to be supported in IoT in order to handle a large number of devices, applications and users.	IoT data server, IoT service controller, service platform, service manager, IoT network controller, network manager, enhanced transport network, IoT gateway, device manager
C-5-8	Managing multiple domains	The capability of managing multiple domains involves the abilities of managing IoT functional components in multiple administrative domains to support of IoT scalability.	Scalability is required to be supported in IoT in order to handle a large number of devices, applications and users.	IoT data server, IoT service controller, service platform, service manager, IoT network controller, network manager, enhanced transport network, device manager
C-5-9	Redundant deployment enablement	The capability of redundant deployment enablement involves the abilities of enabling deployment of redundant functional components of the IoT to guarantee reliability required in communication, service provision and data management.	Reliability in capabilities of IoT, such as reliability in communication, service and data management capabilities of IoT, is required.	IoT data server, IoT service controller, service platform, service manager, IoT network controller, network manager, IoT gateway, device manager

Table A.5 – List of management capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-5-10	Service integrity check	The capability of service integrity check involves the abilities of checking the service lifetime, the available resources required to provide the service in order to guarantee the high availability of service provisioning.	The IoT is required to provide high availability in service provisioning, data management, communication, sensing and actuating things.	Service manager
C-5-11	Data integrity check	The capability of data integrity check involves the abilities of checking the data lifetime, the available attributes of the data, and the consistency of data in order to guarantee the high availability of data management.	The IoT is required to provide high availability in service provisioning, data management, communication, sensing and actuating things.	IoT data server
C-5-12	Device integrity check	The capability of device integrity check involves the abilities of checking the status of all functions of device to guarantee the high availability of IoT devices.	The IoT is required to provide high availability in service provisioning, data management, communication, sensing and actuating things.	Device manager, IoT device, IoT gateway, end-user device
C-5-13	Security integrity check	The capability of security integrity check involves the abilities of checking the consistency of security policies deployed in all functional components of the IoT to guarantee the high availability of security in the IoT.	The IoT is required to provide high availability in service provisioning, data management, communication, sensing and actuating things.	Service manager, network manager, device manager, IoT device, IoT gateway, end-user device
C-5-14	User profile integrity check	The capability of user profile integrity check involves the abilities of checking the lifetime, subscription, privacy protection, and availability of services subscribed by users to guarantee the high availability of service provisioning and privacy protection for users.	The IoT is required to provide high availability in service provisioning, data management, communication, sensing and actuating things.	Service manager, network manager, device manager, IoT device, IoT gateway, end-user device

Table A.5 – List of management capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-5-15	Managing devices	The capability of managing devices involves the abilities of configuring, monitoring, diagnosing, and recovering devices of the IoT, and updating software to enhance capabilities of devices of the IoT.	Manageability is required to be supported in IoT in order to ensure normal operations.	Device manager
C-5-16	Managing networks	The capability of managing networks involves the abilities of configuring, monitoring, accounting and charging, optimizing, diagnosing, and recovering networks of the IoT, and updating network software to enhance capabilities of networks of the IoT.	Manageability is required to be supported in IoT in order to ensure normal operations.	Network manager
C-5-17	Managing services	The capability of managing services involves the abilities of describing, configuring, monitoring, accounting and charging, optimizing, recovering, and updating services of the IoT.	Manageability is required to be supported in IoT in order to ensure normal operations.	Service manager
C-5-18	Managing data operations	The capability of managing data operations involves the abilities of configuring, monitoring, accounting and charging, optimizing, and recovering data operations, and updating software related with data operations to enhance capabilities of the IoT.	Manageability is required to be supported in IoT in order to ensure normal operations.	IoT data server
C-5-19	Managing security operations	The capability of managing security operations involves the abilities of configuring, monitoring, auditing, diagnosing, and recovering security operations, and updating software related with security operations to enhance capabilities of the IoT.	Manageability is required to be supported in IoT in order to ensure normal operations.	Service manager, network manager, device manager

Table A.5 – List of management capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-5-20	Managing privacy protection	The capability of managing privacy protection involves the abilities of configuring, monitoring, auditing, and recovering privacy protection, and updating software related with privacy protection to enhance capabilities of the IoT.	Manageability is required to be supported in IoT in order to ensure normal operations.	Service manager, network manager, device manager
C-5-21	Managing user operations	The capability of managing user operations involves the abilities of configuring, monitoring, accounting and charging, optimizing, diagnosing, recovering operations of IoT users, and updating software related with operations of IoT users to enhance capabilities of the IoT.	Manageability is required to be supported in IoT in order to ensure normal operations.	Service manager, network manager, device manager
C-5-22	Plug and play capability	Plug and play capability involves the abilities of automatic configuring, connecting and activating devices of the IoT to enable on-the-fly semantic-based configuration and activation of IoT devices.	Plug and play capability is required.	IoT device, IoT gateway, end-user device, network manager, service manager

Table A.6 – List of connectivity capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-6-1	Identification-based connectivity	The capability of identification-based connectivity involves the abilities of establishing the connectivity based on the identification of things.	Identification-based connectivity between a thing and the IoT is required.	IoT device, IoT gateway, end-user device, network manager
C-6-2	Things' status notification	The capability of things' status notification involves the abilities of automatic notification of the status of things and its changes based on predefined rules.	Monitoring things in timely manner is required.	IoT device, IoT gateway, end-user device

Table A.6 – List of connectivity capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-6-3	Device mobility	The capability of device mobility involves the abilities of keeping the connectivity with the IoT when a device moves.	Device mobility is required.	IoT device, IoT gateway, end-user device, network manager
C-6-4	Adaptable connectivity	The capability of adaptable connectivity involves the abilities of extending connectivity configurations to connect with new types of devices of the IoT in order to be adaptable to different technologies in devices of IoT.	Adaptability to the new technologies emerging in the future is required in IoT.	IoT device, IoT gateway, end-user device, device manager

Table A.7 – List of security and privacy protection capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-7-1	Communication security	The capability of communication security involves the abilities of supporting secure, trusted and privacy-protected communication.	Communication security is required.	IoT device, IoT gateway, end-user device, device manager, network manager, enhanced transport network
C-7-2	Data management security	The capability of data management security involves the abilities of providing secure, trusted and privacy-protected data management.	Data management security is required.	IoT data server, IoT gateway
C-7-3	Service provision security	The capability of service provision security involves the abilities of providing secure, trusted and privacy-protected service provision.	Service provision security is required.	Service platform, service manager
C-7-4	Security integration	The capability of security integration involves the abilities of integrating different security policies and techniques related to the variety of IoT functional components.	Integration of different security policies and techniques is required.	Device manager, network manager, service manager

Table A.7 – List of security and privacy protection capabilities

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-7-5	Mutual authentication and authorization	The capability of mutual authentication and authorization involves the abilities of authenticating and authorizing each other before a device accesses IoT based on predefined security policies.	Mutual authentication and authorization is required.	Device manager, network manager
C-7-6	Security audit	The capability of security audit involves the abilities of monitoring any data access or attempt to access IoT applications in a fully transparent, traceable and reproducible way based on appropriate regulation and laws.	Security audit is required to be supported in IoT.	Device manager, network manager, service manager, IoT data server

Table A.8 – List of capabilities for integration of cloud computing technologies

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-8-1	Accessing virtual processing resources	The capability of accessing virtual processing resources involves the abilities of adopting the capabilities specified in infrastructure capabilities type of cloud to use processing resource deployed in cloud.	Integration with cloud computing technologies is required.	IoT data server, IoT gateway
C-8-2	Accessing virtual storage resources	The capability of accessing virtual storage resources involves the abilities of adopting the capabilities specified in infrastructure capabilities type of cloud to use storage resource deployed in cloud.	Integration with cloud computing technologies is required.	IoT data server, IoT gateway
C-8-3	Publishing things as services	The capability of publishing things as services involves the abilities of adopting the capabilities specified in platform capabilities type of cloud to deploy the services of things.	Integration with cloud computing technologies is required.	IoT data server, service platform

Table A.8 – List of capabilities for integration of cloud computing technologies

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-8-4	Summarizing data of things	The capability of summarizing data of things involves the abilities of collecting and aggregating the data of things related with the required services to provide the service of things to cloud users.	Integration with cloud computing technologies is required.	IoT data server, service platform, IoT device, IoT gateway, end-user device
C-8-5	Synchronizing data with things	The capability of synchronizing data with things involves the abilities of creating, deleting, and updating the data of things just in time with respect to application requirements, based on the updated status of sensed things in order to guarantee the quality of TaaS.	Integration with cloud computing technologies is required.	IoT data server, service platform, IoT device, IoT gateway, end-user device

Table A.9 – List of capabilities for integration of big data technologies

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-9-1	Adopting big data collection	The capability of adopting big data collection involves the abilities of adopting the technologies of big data collection.	Integration with big data technologies is required.	IoT data server, IoT gateway
C-9-2	Adopting big data aggregation	The capability of adopting big data aggregation involves the abilities of adopting the technologies of summarizing big data from different sources in device layer.	Integration with big data technologies is required.	IoT device, IoT gateway, end-user device
C-9-3	Adopting big data storage	The capability of adopting big data storage involves the abilities of adopting the technologies of storing big data.	Integration with big data technologies is required.	IoT data server

Table A.9 – List of capabilities for integration of big data technologies

Capability number	Capability name	Capability summary	Related requirement(s)	Associated component(s)
C-9-4	Adopting big data integration	The capability of adopting big data integration involves the abilities of adopting the technologies of summarizing big data from different sources in server support and application support layer.	Integration with big data technologies is required.	IoT data server, IoT gateway
C-9-5	Adopting big data query	The capability of adopting big data query involves the abilities of adopting the technologies of big data query.	Integration with big data technologies is required.	IoT data server
C-9-6	Adopting big data analysis	The capability of adopting big data analysis involves the abilities of adopting the technologies of big data analysis.	Integration with big data technologies is required.	IoT data server

Appendix I

Matching analysis between requirements and capabilities of the IoT

(This Appendix does not form an integral part of this Recommendation.)

Tables I.1 to I.7 provide matching analyses between requirements and capabilities of the IoT. The following provides a legend for the structure of these tables.

The two columns headed "Requirement number" and "Requirement summary" are copied from the corresponding columns in the table in Annex A of [ITU-T Y.2066].

The column headed "Capability number" contains one or multiple capability numbers provided in Annex A whose corresponding capabilities support the requirement listed in the same row.

The column headed "Capability name" contains the name of the capabilities associated with the "Capability number" provided in the same row. These capabilities are described in clause 8 and support the requirement listed in the same row.

I.1 Matching analysis of non-functional requirements of the IoT

Matching analysis results between non-functional requirements of the IoT and the supported capabilities of the IoT are shown in Table I.1. Results show that all non-functional requirements specified in [ITU-T Y.2066] are fulfilled.

NOTE – There are multiple capabilities associated with each row of Table I.1. These capabilities act together to support the requirement in the same row.

Table I.1 – List of matching analysis of non-functional requirements of the IoT

Requirement number	Requirement summary	Capability number	Capability name
N1	Interoperability is required.	C-5-1, C-5-2, C-5-3, C-5-4, C-5-5, and C-5-6.	Managing data models for exchanging data of things, managing service description, managing network configuration, managing device configuration, managing security policy, and managing privacy protection policy.
N2	Scalability is required.	C-4-7, C-5-7, and C-5-8.	Autonomic data operation, managing distributed processing, and managing multiple domains.
N3	Reliability is required.	C-1-12, C-2-15, C-3-6, and C-5-9.	Service provision acknowledgement, transport acknowledgement, application support operation acknowledgement, and redundant deployment enablement.

Table I.1 – List of matching analysis of non-functional requirements of the IoT

Requirement number	Requirement summary	Capability number	Capability name
N4	High availability is required.	C-5-10, C-5-11, C-5-12, C-5-13, and C-5-14.	Service integrity check, data integrity check, device integrity check, security integrity check, and user profile integrity check.
N5	Adaptability is required.	C-1-11, C-2-16, and C-6-4.	Adaptable service provision, adaptable networking, and adaptable connectivity.
N6	Manageability is required.	C-5-15, C-5-16, C-5-17, C-5-18, C-5-19, C-5-20, and C-5-21.	Managing devices, managing networks, managing services, managing data operations, managing security operations, managing privacy protection, and managing user operations.

I.2 Matching analysis of application support requirements of the IoT

Matching analysis results between application support requirements of the IoT and the capabilities of the IoT that can fulfil those requirements are shown in Table I.2. Results show that all application support requirements specified in [ITU-T Y.2066] are fulfilled.

NOTE – There may be multiple capabilities associated with a single row of Table I.2. Where multiple capabilities are listed, they act together to support the requirement in the same row.

Table I.2 – List of matching analysis of application support requirements of the IoT

Requirement number	Requirement summary	Capability number	Capability name
A1	Standardized programmable interfaces are required.	C-3-1	Programmable interface provision
A2	Group management is required.	C-3-2	Group management
A3	Reliable time synchronization is required.	C-3-3	Time synchronization
A4	Collaboration is required.	C-3-4	Orchestration
A5	User management is required.	C-3-5	User management
A6	Resource usage accounting is required.	C-5-16, C-5-17, and C-5-18	Managing networks, managing services, and managing data operations.

I.3 Matching analysis of service requirements of the IoT

Matching analysis results between service requirements of the IoT and the supported capabilities of the IoT are shown in Table I.3. Results show that all service requirements specified in [ITU-T Y.2066] are fulfilled.

NOTE – There may be multiple capabilities associated with a single row of Table I.3. Where multiple capabilities are listed, they act together to support the requirement in the same row.

Table I.3 – List of matching analysis of service requirements of the IoT

Requirement number	Requirement summary	Capability number	Capability name
S1	Prioritization of services is required.	C-1-1	Service prioritization
S2	Semantic based services are required.	C-1-2	Semantic based service
S3	Service composition is required.	C-1-3	Service composition
S4	Mobility services are required.	C-1-4	Mobility services
S5	Highly reliable and secure human body connectivity services are required.	C-1-12, C-2-15, C-3-6, C-7-1, C-7-2, and C-7-3.	Service provision acknowledgement, transport acknowledgement, application support operation acknowledgement, communication security, data management security, and service provision security.
S6	Autonomic services are required.	C-1-5	Autonomic service
S7	Location-based and context-aware services are required.	C-1-6	Location-based and context-aware service
S8	Service management is required.	C-5-17	Managing services
S9	Discovery services are required.	C-1-7	Service discovery
S10	Service subscription support is required.	C-1-8	Service subscription
S11	Standardized naming and addressing is required.	C-1-9	Standardized naming and addressing
S12	Virtual storage and processing capabilities are required.	C-1-10	Virtual storage and processing

I.4 Matching analysis of communication requirements of the IoT

Matching analysis results between communication requirements of the IoT and the supported capabilities of the IoT are shown in Table I.4. Results show that all communication requirements specified in [ITU-T Y.2066] are fulfilled.

NOTE – There may be multiple capabilities associated with a single row of Table I.4. Where multiple capabilities are listed, they act together to support the requirement in the same row. In the case of the row identified by Requirement number "C3", each of the two identified capabilities can fulfil the requirement.

Table I.4 –List of matching analysis of communication requirements of IoT

Requirement number	Requirement summary	Capability number	Capability name
C1	Event-based, periodic, and automatic communication modes are required to be supported.	C-2-1 and C-2-2.	Event-based communication and periodic communication.
C2	The support of the unicast, multicast, broadcast and anycast communication modes is required.	C-2-3, C-2-4, C-2-5 and C-2-6.	Unicast communication, multicast communication, broadcast communication, and anycast communication.
C3	The support of device initiated communications is required.	C-2-1 or C-2-2.	Event-based communication or periodic communication.
C4	Error control for communications is required to be supported.	C-2-7	Error control for communications
C5	Time-critical communications are required to be supported.	C-2-8	Time-critical communications
C6	Autonomic networking is required.	C-2-9, C-2-10, C-2-11 and C-2-12.	Self-configuring for networking, self-healing for networking, self-optimizing for networking, and self-protecting for networking.
C7	Content-aware communication is required.	C-2-13	Content-aware communication
C8	Location-based communication is required.	C-2-14	Location-based communication
C9	Support for heterogeneous device related communication technologies is required.	C-5-4	Managing device configuration
C10	Support for heterogeneous network related communication technologies is required.	C-5-3	Managing network configuration

I.5 Matching analysis of device requirements of the IoT

Matching analysis results between device requirements of IoT and the supported capabilities of the IoT are shown in Table I.5. Results show that all device requirements specified in [ITU-T Y.2066] are fulfilled.

Table I.5 – List of matching analysis of device requirements of the IoT

Requirement number	Requirement summary	Capability number	Capability name
D1	Identification-based connectivity between a thing and the IoT is required.	C-6-1	Identification-based connectivity
D2	Remote monitoring, control and configuration of devices are required.	C-5-15	Managing devices
D3	Plug and play capability is required.	C-5-22	Plug and play capability
D4	Monitoring things in a timely manner is required.	C-6-2	Things' status notification
D5	Device mobility is required.	C-6-3	Device mobility
D6	Device integrity checking is required.	C-5-12	Device integrity check

I.6 Matching analysis of data management requirements of the IoT

Matching analysis results between data management requirements of the IoT and the supported capabilities of the IoT are shown in Table I.6. Results show that all data management requirements specified in [ITU-T Y.2066] are fulfilled.

Table I.6 – List of matching analysis of data management requirements of the IoT

Requirement number	Requirement summary	Capability number	Capability name
DM1	Storing data of things is required to be supported.	C-4-1	Data storage
DM2	Processing data of things is required to be supported.	C-4-2	Data processing
DM3	Querying historical data of things is required to be supported.	C-4-3	Data querying
DM4	Data access control by the data owners is required.	C-4-4	Data access control
DM5	Data exchange with entities outside the IoT is required to be supported.	C-4-5	Open information exchange
DM6	Integrity checking and life cycle management of data of things is required.	C-5-11	Data integrity check
DM7	Semantic annotation and semantic access to data of things are required.	C-4-6	Semantic data operation
DM8	Semantic storage, transfer and aggregation of data of things are required.	C-4-6	Semantic data operation

I.7 Matching analysis of security and privacy protection requirements of the IoT

Matching analysis results between security and privacy protection requirements of the IoT and the supported capabilities of the IoT are shown in Table I.7. Results show that all security and privacy protection requirements specified in [ITU-T Y.2066] are fulfilled.

Table I.7 – List of matching analysis of security and privacy protection requirements of the IoT

Requirement number	Requirement summary	Capability number	Capability name
SP1	Communication security is required.	C-7-1	Communication security
SP2	Data management security is required.	C-7-2	Data management security
SP3	Service provision security is required.	C-7-3	Service provision security
SP4	Integration of different security policies and techniques is required.	C-7-4	Security integration
SP5	Mutual authentication and authorization is required.	C-7-5	Mutual authentication and authorization
SP6	Security audit is required to be supported in the IoT.	C-7-6	Security audit

Bibliography

[b-ITU-T Y.2001]	Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.
[b-ITU-T Y.2061]	Recommendation ITU-T Y.2061 (2012), *Requirements for support of machine-oriented communication applications in the next generation network environment*.
[b-ITU-T Y.2067]	Recommendation ITU-T Y.2067 (2014), *Common requirements and capabilities of a gateway for Internet of things applications*.
[b-ITU-T Y.3500]	Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.
[b-ETSI TS 102 690]	ETSI TS 102 690 v1.2.1 (2013), *Machine-to-Machine communications (M2M); Functional architecture*, http://www.etsi.org/standards
[b-IoT-A D1.4]	The Internet of things architecture (IoT-A, 2012), *Project Deliverable D1.4 – Converged architectural reference model for the IoT v2.0*, http://www.iot-a.eu/public/public-documents/documents-1

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015