

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1750

(09/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Data security – Big Data Security

Guidelines on security of big data as a service for big data service providers

Recommendation ITU-T X.1750

ITU-T

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1750

Guidelines on security of big data as a service for big data service providers

Summary

Big data as a service (BDaaS) is a cloud service category that provides cloud service customers with capabilities to collect, store, analyse, visualize and manage big data, as specified in Recommendation ITU-T Y.3600. With remarkable growth of data volumes and rapid development of big data business, big data infrastructure has become the central facility to provide BDaaS. Consequently, significant security issues arise for BDaaS. For example, open source big data software design sometimes fails to take security into consideration from the beginning. New technologies introduced by big data analytics can also result in failure of traditional security protection measures. Recommendation ITU-T X.1750 analyses security challenges BDaaS faces, identifies security roles and responsibilities for provision of BDaaS, as well as a security framework for a big data infrastructure. It also specifies security protection measures that should be satisfied for services and components related to BDaaS.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1750	2020-09-03	17	11.1002/1000/14266

Keywords

Big data as a service, security guidelines, security measures.

* 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/>.

© ITU 2021

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

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Security threats and challenges to big data as a service	3
	6.1 Security challenges to a big data infrastructure.....	4
	6.2 Security challenges to big data applications.....	4
	6.3 Security challenges to data	4
	6.4 Security challenges to big data as a service ecosystem.....	4
7	High-level concepts of big data as a service – security considerations and role of BDSPs.....	5
8	Security measures of big data as a service.....	5
	8.1 Security measures for a big data infrastructure	5
	8.2 Security measures for big data applications	8
	8.3 Security measures for interface	11
	8.4 Security measures for big data as a service ecosystem	12
	Bibliography.....	21

Recommendation ITU-T X.1750

Guidelines on security of big data as a service for big data service providers

1 Scope

This Recommendation analyses security challenges faced by big data as a service (BDaaS) and provides guidelines for big data service providers (BDSPs) to secure BDaaS. It identifies security roles and responsibilities of BDaaS components and specifies a security framework for a big data infrastructure, including platforms, applications, analytics, interfaces and the BDaaS ecosystem. This Recommendation also specifies security protection measures that should be taken for activities or components related to BDaaS.

This Recommendation is a high-level description of security requirements for BDaaS implementation that focuses on BDaaS. BDaaS involves big data infrastructure providers (BDIPs) and big data application providers (BDAPs). Guidelines for BDIPs and BDAPs, as well as detailed guidance on BDaaS implementation lie outside the scope of this Recommendation.

2 References

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

- | | |
|-------------------|---|
| [ITU-T X.1601] | Recommendation ITU-T X.1601 (2015), <i>Security framework for cloud computing</i> . |
| [ITU-T X.1631] | Recommendation ITU-T X.1631 (2015), <i>Information technology – Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services</i> . |
| [ITU-T X.1641] | Recommendation ITU-T X.1641 (2016), <i>Guidelines for cloud service customer data security</i> . |
| [ITU-T Y.3600] | Recommendation ITU-T Y.3600 (2015), <i>Big data – Cloud computing based requirements and capabilities</i> . |
| [ISO/IEC 27000] | ISO/IEC 27000:2018, <i>Information technology – Security techniques – Information security management systems – Overview and vocabulary</i> . |
| [ISO/IEC 27036-3] | ISO/IEC 27036-3:2013, <i>Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security</i> . |
| [ISO 28000] | ISO 28000:2007, <i>Specification for security management systems for the supply chain</i> . |

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 big data [ITU-T Y.3600]: A paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics.

NOTE – Examples of datasets characteristics include high-volume, high-velocity, high-variety, etc.

3.1.2 big data as a service (BDaaS) [ITU-T Y.3600]: A cloud service category in which the capabilities provided to the cloud service customer are the ability to collect, store, analyse, visualize and manage data using big data.

3.1.3 big data provenance [b-ITU-T Y.3602]: Information that records the historical path of data according to the data lifecycle operations in a big data ecosystem.

3.1.4 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.

3.1.5 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.6 metadata [b-ITU-T M.3030]: Data that describes other data.

3.1.7 security challenge [ITU-T X.1601]: A security "difficulty" other than a direct security threat arising from the nature and operating environment of cloud services, including "indirect" threats.

3.1.8 threat [ISO/IEC 27000]: Potential cause of an unwanted incident, which can result in harm to a system or organization.

3.1.9 vulnerability [b-NIST SP 800-30]: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 data asset: An electronically recorded data resource, owned or controlled by an organization.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
ABAC	Attribute-Based Access Control
BDaaS	Big Data as a Service
BDAP	Big Data Application Provider
BDIP	Big Data Infrastructure Provider
BDSN	Big Data Service partner
BDSP	Big Data Service Provider
BDSU	Big Data Service User
CSC	Cloud Service Customer
DP	Data Provider
IT	Information Technology
PII	Personally Identifiable Information
PKI	Public Key Infrastructure

SAML	Security Assertion Markup Language
SDK	Software Development Kit
SSL	Secure Socket Layer
TLS	Transport Layer Security
USB	Universal Serial Bus

5 Conventions

In this Recommendation:

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

The phrase "**is recommended**" indicates a requirement that is recommended, but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The phrase "**is prohibited from**" indicates a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

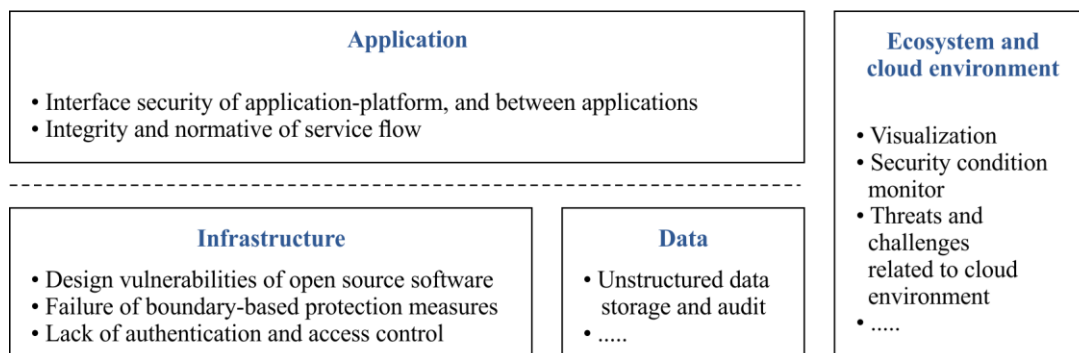
The phrase "**can optionally**" indicates an optional requirement that is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator or service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

6 Security threats and challenges to big data as a service

This clause describes security threats and challenges to BDaaS. Cloud computing-based BDaaS is specified in [ITU-T Y.3600]. Security challenges relevant to cloud computing environments as described in clause 8 of [ITU-T X.1601] should be taken into consideration for BDaaS. This Recommendation, then, describes security threats and challenges to specific capabilities and services of BDaaS, i.e., big data platform as a service and big data-related software as a service (recognizing that the BDaaS ecosystem includes data providers (DPs), BDAPs and BDIPs), including:

- vulnerabilities of big data infrastructure and failure of security measures;
- storage and audit problems incurred by unstructured data;
- security and regulation of interface between applications, platforms and service flow;
- other security concerns, e.g., trust, authentication and visualization.

Figure 6-1 shows an architecture of BDaaS security challenges.



X.1750(20)_F6-1

Figure 6-1 – Big data as a service security challenges