

Recommendation

ITU-T X.1647 (10/2024)

SERIES X: Data networks, open system communications and security

Cloud computing security – Cloud computing security best practices and guidelines

Security guidelines for selecting computing methods and resources from cloud service providers

ITU-T X-SERIES RECOMMENDATIONS

Data networks, open system communications and security

PUBLIC DATA NETWORKS	X.1-X.199
OPEN SYSTEMS INTERCONNECTION	X.200-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999
INFORMATION AND NETWORK SECURITY	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
Overview of cloud computing security	X.1600-X.1601
Cloud computing security requirements, security capabilities	X.1602-X.1629
Cloud computing security controls	X.1630-X.1639
Cloud computing security best practices and guidelines	X.1640-X.1659
Other cloud computing security	X.1660-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METaverse AND DIGITAL TWIN SECURITY	X.2000-X.2199
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

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

Recommendation ITU-T X.1647

Security guidelines for selecting computing methods and resources from cloud service providers

Summary

With the development of cloud computing, computing tasks can be outsourced to external computing resources for computation. However, computing resources differ in the security levels they offer, and computing tasks differ in their security requirements. To mitigate the security threats introduced by insecure computing resources and satisfy the security requirements of computing tasks, secure computation methods can be applied.

Recommendation ITU-T X.1647 provides guidelines for the selection of secure computation methods and resources from cloud service providers (CSPs) to help service customers or stakeholders to execute outsourcing computation in a way that meets their security requirements.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1647	2024-10-29	17	11.1002/1000/16167

Keywords

Cloud service, computing method, security.

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 2025

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

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	2
5	Conventions	2
6	Background.....	2
	6.1 Overview	2
	6.2 Security challenges.....	4
7	Awareness of security of computing resources, methods and tasks.....	5
	7.1 Overview	5
	7.2 Awareness of security of the computing resources provided by CSPs	5
	7.3 Awareness of security of the secure computing methods	6
	7.4 Awareness of security requirements of computing tasks	8
8	Selection method of secure computing methods and resources	10
	8.1 Overview	10
	8.2 Options of computing resources and methods.....	10
	8.3 Preliminary filtering of computing resources and methods	11
	8.4 Security evaluation of the computing resources and methods	12
	8.5 Resources and methods filtering	13
	8.6 Policy-based computing resources and methods selection.....	13
	Appendix I – Use cases of the selection of secure computing methods and resources for outsourcing computation to CSPs.....	14
	I.1 Use case: A customer performs the computing task with own data.....	14
	I.2 Use case: Customers collaborate to perform the computing task.....	15
	I.3 Use case: CSPs collaborate to perform the computing task	16
	Bibliography.....	18

Recommendation ITU-T X.1647

Security guidelines for selecting computing methods and resources from cloud service providers

1 Scope

This Recommendation provides security guidelines for selecting computing methods and resources from cloud service providers (CSPs). This Recommendation covers:

- Security challenges when outsourcing computations to CSPs, introduced by different security capabilities of computing resources, different security requirements of computing tasks and different secure computing methods;
- Security guidelines are applicable when selecting secure computing methods and resources. These include security-related metrics for resources provided by CSPs, secure computing methods and computing tasks' requirements, and decision-making principles.

2 References

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

[ITU-T Y.3508] Recommendation ITU-T Y.3508 (2019), *Cloud computing – Overview and high-level requirements of distributed cloud*.

[ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 secret sharing [b-ITU-T X.1091]: A method of dividing a key into a number of segmentations and restoring it by assembling the segmentations.

3.1.2 homomorphic encryption [b-ITU-T F.747.13]: Symmetric or asymmetric encryption that allows third parties to perform operations on plaintext data while keeping them in encrypted form.

3.1.3 differential privacy [b-Peter]: A formal framework to quantify to what extent individual privacy in a statistical database is preserved while releasing useful aggregate information about the database.

3.1.4 confidential computing [b-ITU-T F.751.9]: Technology that executes data operations while protecting the confidentiality and integrity of sensitive data.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 secure computing method: Computing method which can provide certain security features (e.g. trusted or verifiable or invisible) for data and computing processes.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AI	Artificial Intelligence
CSC	Cloud Service Customer
CSP	Cloud Service Provider
CPU	Central Processing Unit
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
VR	Virtual Reality

5 Conventions

None.

6 Background

6.1 Overview

Demands for more computing power and faster response speed are increasing day by day. The market for computing-intensive services, such as artificial intelligence (AI)-based services, and delay-sensitive services, such as video and Internet of services, is growing. Large-scale application of computing-intensive and delay-sensitive services across various industries promotes higher requirements for computing resources. With the development of cloud computing technology, and in order to control costs and meet computing requirements, cloud service customers (CSCs) outsource their computing tasks to external cloud computing resources provided by cloud service providers (CSPs). Some typical scenarios of outsourcing computing tasks to CSPs are presented as follows:

Scenario 1: As shown in Figure 1, CSCs can outsource computing tasks to CSPs. In this scenario, CSCs choose one or more CSPs that connect to their devices and send data to the computing resources of the CSPs for computing. The computing resources of the CSPs can be in small or large-scale computing centres and the security capabilities of these computing resources may differ.

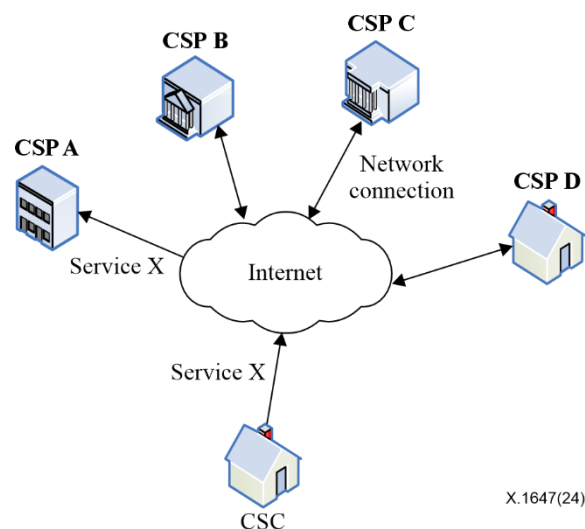


Figure 1 – CSCs outsource computing tasks to traditional CSPs