

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

F.748.13

(06/2021)

SERIES F: NON-TELEPHONE TELECOMMUNICATION
SERVICES

Multimedia services

Technical framework for a shared machine learning system

Recommendation ITU-T F.748.13

ITU-T



ITU-T F-SERIES RECOMMENDATIONS
NON-TELEPHONE TELECOMMUNICATION SERVICES

TELEGRAPH SERVICE	
Operating methods for the international public telegram service	F.1–F.19
The gentex network	F.20–F.29
Message switching	F.30–F.39
The international telemessage service	F.40–F.58
The international telex service	F.59–F.89
Statistics and publications on international telegraph services	F.90–F.99
Scheduled and leased communication services	F.100–F.104
Phototelegraph service	F.105–F.109
MOBILE SERVICE	
Mobile services and multideestination satellite services	F.110–F.159
TELEMATIC SERVICES	
Public facsimile service	F.160–F.199
Teletex service	F.200–F.299
Videotex service	F.300–F.349
General provisions for telematic services	F.350–F.399
MESSAGE HANDLING SERVICES	F.400–F.499
DIRECTORY SERVICES	F.500–F.549
DOCUMENT COMMUNICATION	
Document communication	F.550–F.579
Programming communication interfaces	F.580–F.599
DATA TRANSMISSION SERVICES	F.600–F.699
MULTIMEDIA SERVICES	F.700–F.799
ISDN SERVICES	F.800–F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850–F.899
ACCESSIBILITY AND HUMAN FACTORS	F.900–F.999

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

Recommendation ITU-T F.748.13

Technical framework for a shared machine learning system

Summary

Recommendation ITU-T F.748.13 defines the roles, technical and security requirements of a shared machine learning system, and provides technical architectures, functional components, and processing procedures of the shared machine learning system in the centralized and decentralized modes.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T F.748.13	2021-06-13	16	11.1002/1000/14682

Keywords

Encrypted data, multi-party computation, shared machine learning, trusted execution environment.

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© 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.....	1
4	Abbreviations and acronyms	1
5	Conventions	2
6	Overview of the shared machine learning system	2
7	Roles in the shared machine learning system	3
	7.1 Overview	3
	7.2 Data provider	3
	7.3 Computation platform	3
	7.4 Result receiver	4
	7.5 Task initiator.....	4
8	Technical requirements of the shared machine learning system	4
	8.1 Basic functional requirements	4
	8.2 Scalability requirements	5
	8.3 Reliability requirements	5
	8.4 Compatibility requirements	6
	8.5 Performance requirements.....	6
	8.6 Usability requirements.....	6
9	Security requirements of the shared machine learning system.....	6
	9.1 Authentication requirements	6
	9.2 Access control requirements.....	7
	9.3 Security auditing requirements.....	7
	9.4 Data security requirements	7
	9.5 Privacy protection requirements.....	7
10	Technical architecture, functional components, and processing procedure of the shared machine learning system in centralized mode.....	8
	10.1 Technical architecture of the shared machine learning system in the centralized mode.....	8
	10.2 Functional components of the shared machine learning system in the centralized mode.....	9
	10.3 Processing procedures of the shared machine learning system in the centralized mode.....	10
11	Technical architecture, functional components, and processing procedure of the shared machine learning system in decentralized mode.....	11
	11.1 Technical architecture of the shared machine learning system in the decentralized mode	11

	Page
11.2 Functional components of the shared machine learning system in the decentralized mode	11
11.3 Processing procedures of the shared machine learning system in the decentralized mode	12
Appendix I – Use cases for shared machine learning systems	13
I.1 Use case: Improving modules for recognizing telecom frauds using data from multiple networks	13
I.2 Intelligent credit and risk control use case	14
I.3 Intelligent marketing use case	14
Bibliography.....	15

Recommendation ITU-T F.748.13

Technical framework for a shared machine learning system

1 Scope

This Recommendation defines a shared machine learning (SML) system, and provides its roles, technical and security requirements, technical architectures, functional components, and processing procedures of the shared machine learning system in the centralized and decentralized modes. Use cases for shared machine learning systems are provided in the appendix as well.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 machine learning [b-ITU-T Y.3172]: Processes that enable computational systems to understand data and gain knowledge from it without necessarily being explicitly programmed.

3.1.2 trusted execution environment [b-ITU-T J.1201]: A secure area of the main processor in an IBB-capable cable STB and TV to ensure that sensitive data is stored, processed and protected in an isolated and trusted environment. It offers isolated safe execution of authorized security software providing end-to-end security by enforcement of protected execution of authenticated code, confidentiality, authenticity, privacy, system integrity and data access rights.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 shared machine learning: A machine learning paradigm enabling aggregation of multi-party data information and multi-party data privacy protection for scenarios where multiple data providers and the computation platform do not trust each other.

3.2.2 multi-party computation: A subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private.

3.2.3 remote attestation: A method by which a host (client) authenticates its hardware and software configuration to a remote host (server). The goal of remote attestation is to enable a remote system (challenger) to determine the level of trust in the integrity of the platform of another system (attestator).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

API	Application Programming Interface
QPS	Queries Per Second
SML	Shared Machine Learning
SMS	Short Messaging Service
TEE	Trusted Execution Environment
WOE	Weight of Evidence

5 Conventions

The following conventions are used in this Recommendation:

- The keywords "is required to" indicate a requirement that must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.
- The keywords "is prohibited from" indicate a requirement that must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.
- The keywords "is recommended" indicate a requirement that is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.
- The keywords "is not recommended" indicate a requirement that is not recommended but which is not specifically prohibited. Thus, conformance with this Recommendation can still be claimed even if this requirement is present.
- The keyword "functions" is defined as a collection of functionalities.

6 Overview of the shared machine learning system

With shared machine learning (SML) systems, multi-party participants share encrypted data or exchange parameters to protect data security and privacy. The encrypted data or exchanged parameters of each party are gathered to train a shared machine learning model to make the best use of data. Shared machine learning models keep training to achieve self-optimization and multi-party participants or others who have the authorization to access the model, can input information to get outputs or predictions based on shared values. Shared machine learning systems can be applied in media applications but are not limited to media-related applications.

Shared machine learning includes centralized and decentralized modes. The centralized mode is a solution for multi-party data encryption sharing and fusion learning in a trusted execution environment (TEE). The decentralized mode is a solution for sharing and learning by multiple participants based on secure multi-party computing by exchanging non-original data that does not reveal privacy.

For centralized mode, the data is collected and trained in a trusted third party. It can be applied to scenarios where participants would like to share data that does not involve privacy, have low service access costs, and also be applied to complex computing scenarios. It can also support all the algorithms, cluster deployment and centralized computing.