International Telecommunication Union

# 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 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 multidestination 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/.

## Table of Contents

# 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.

For decentralized mode, it uses multi-party computation methods to exchange data or parameters to complete the training tasks. It can be applied to scenarios where participants need strict data privacy protection or in scenarios where participants have a large amount of local data since different parties' exchange parameters, but not real data when the machine learning model is training. Multi-party computation is suitable for simple calculations since it can support fewer algorithms compared to the trusted execution environment solution.

## 7 Roles in the shared machine learning system

### 7.1 Overview

The shared machine learning system is described in Figure 1.

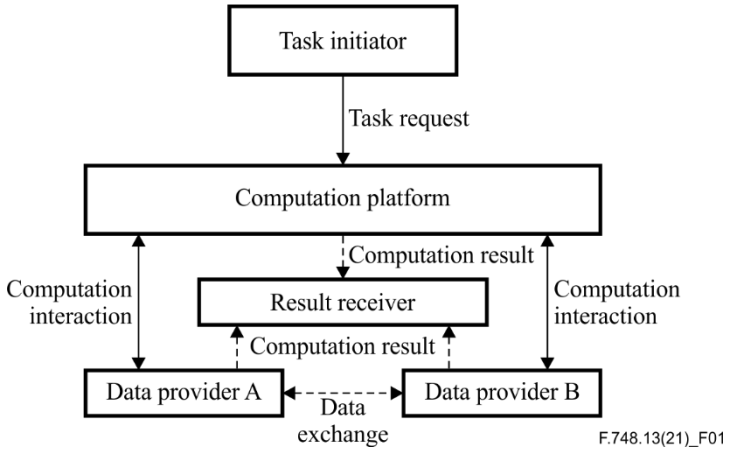


**Figure 1 – Roles in the shared machine learning system**

In a shared machine learning system, there are several roles, including task initiator, data provider, computation platform, and result receiver. Note that Figure 1, only shows two data providers, but in the real deployment, it can have multiple data providers. A party can act as multiple roles. For example, one of the data providers can be a task initiator and / or result receiver.

### 7.2 Data provider

A data provider owns the data and provides the data as input to the computation platform or the other data provider. Note that the data providers also have computation capabilities.

In the centralized mode, the data is encrypted and transmitted from the data provider to the computation platform.

In the decentralized mode, the data is processed as secret or parameters and then exchanged between the data providers, under the coordination of the computation platform.

In any mode, the exchanged data is in a form of a calculation factor, not the original data itself. And the computation platform or the data providers shall not infer any information about the original data from the calculation factors.

### 7.3 Computation platform

The computation platform receives the task request from the task initiator and sends the encrypted result to the result receiver. It interacts with the data providers to perform the computation tasks.

In the centralized mode, the computation platform receives the encrypted data from the data providers, decrypts the encrypted data, and performs the computation in the trusted execution environment.

In the decentralized mode, the computation platform divides the computation task and coordinates the data providers to exchange parameters or secrets between each other and perform computation tasks individually.

The computation platform integrates computation algorithms.

### 7.4 Result receiver

In the centralized mode, when a computation task is completed, the computation platform will send the encrypted result to the result receiver, which can decrypt and get the final result.

In the decentralized mode, the data providers send the computation results to the result receiver, and the result receiver merges the received computation results and gets the final result.

The result receiver can be run by the data providers, or the task initiator, or the computation platform.

### 7.5 Task initiator

The task initiator initiates the computation task with the computation platform.

The task initiator can be run by the computation platform or the data providers.

## 8 Technical requirements of the shared machine learning system

### 8.1 Basic functional requirements

#### 8.1.1 Data management functional requirements

The data management functional requirements for the shared machine learning system include:

– The shared machine learning system is required to support the management and display of metadata information.

– The shared machine learning system is required to support data usage authorization function.

– The shared machine learning system is required to support data alignment function.

– The shared machine learning system is recommended to support data usage behaviour auditing.

– The shared machine learning system is recommended to support encrypted data storage.

#### 8.1.2 Algorithm management functional requirements

The algorithm management functional requirements for the shared machine learning system include:

– The shared machine learning system is required to support at least one mainstream machine learning training and prediction algorithm that can achieve privacy protection, such as linear regression, logistic regression, tree model, deep neural network, graph neural network.

– The shared machine learning system is required to support the parameter adjustment function to obtain better training results.

– The shared machine learning system is required to support at least one data segmentation method of horizontal segmentation or vertical segmentation and is recommended to support both data segmentation methods at the same time.

– The shared machine learning system is required to support the model of resisting semi-honest attacks.

– The shared machine learning system is recommended to support the data privacy intersecting function to ensure that the samples can be aligned when the data is segmented vertically.

– The shared machine learning system is recommended to support secure data analysis functions, such as maximum and minimum statistics, mean variance statistics.

– The shared machine learning system is recommended to support machine learning pre-processing and algorithm effect evaluation functions, including data set division, missing value filling, weight of evidence (WOE), feature correlation evaluation, and other capabilities to improve the performance of machine learning models.

### 8.1.3 Computation management functional requirements

The computation management functional requirements for the shared machine learning system include:

– The shared machine learning system is required to provide basic task management capabilities, such as task creation and cancellation.

– The shared machine learning system is recommended to provide rich task management capabilities, such as task progress monitoring, task queuing, historical task information tracking.

– The shared machine learning system is recommended to support distributed resource management and task scheduling capabilities.

## 8.2 Scalability requirements

The scalability requirements for the shared machine learning system include:

– The shared machine learning system is recommended to have good scalability and to allow new functional components to be added according to business needs.

– The shared machine learning system is recommended to support users to access the system through application programming interface (API).

## 8.3 Reliability requirements

The reliability requirements for the shared machine learning system include:

– The shared machine learning system is required to guarantee the system availability and to avoid being shut down by incorrect input data.

– The shared machine learning system is required to have the ability to perform automatic disaster recovery after failures (such as server failure, hard disk failure, network failure, shutdown, restart), including data backup and restore, etc.

– The shared machine learning system is recommended to support clustering of training and prediction and support cross-computer room disaster recovery, so that the service has failover and disaster tolerance capabilities, thereby improving the system availability.

– The shared machine learning system is recommended to provide operational and maintenance capabilities such as grayscale release, monitoring and alarm, and link tracking, to improve system reliability.

### 8.4 Compatibility requirements

The compatibility requirements for the shared machine learning system include:

– The shared machine learning system is required to be compatible with the other machine learning algorithms.

– The shared machine learning system is recommended to achieve backward compatibility during the upgrade process, including compatibility between system modules, and compatibility between systems and files.

– The shared machine learning system is recommended to support the deployment requirements of different environments, such as cloud environment, virtual machine, physical machine.

– The shared machine learning system is recommended to support normal operation on a variety of mainstream trusted execution environments for the trusted execution environment solution.

### 8.5 Performance requirements

The performance requirements for the shared machine learning system include:

– The shared machine learning system is recommended to support distributed training to increase the amount of data supported by system training and reduce training time.

– The shared machine learning system is recommended to have the capability to improve prediction queries per second (QPS) through horizontal expansion.

### 8.6 Usability requirements

The usability requirements for the shared machine learning system include:

– The shared machine learning system is required to provide complete deployment and operation instructions to facilitate users to understand, access, and use the system.

– The shared machine learning system is recommended to provide a platform interface to reduce the cost of user learning and usage.

– The shared machine learning system is recommended to provide an algorithm development framework so that users can develop custom algorithms that meet security constraints based on the framework.

– The shared machine learning system is recommended to adopt a system design to reduce the interruption to users during system upgrades.

## 9 Security requirements of the shared machine learning system

### 9.1 Authentication requirements

The authentication requirements for the shared machine learning system include:

– The shared machine learning system is required to support identity authentication functions for the users who access the shared machine learning system. Users include data providers, system users, and result receivers.

– The shared machine learning system is required to support certificate authentication for the data providers and result receivers.

– The shared machine learning system is recommended to support two or more combinations of technologies (password verification, mailbox verification, short messaging service (SMS) verification, etc.) to achieve user identity authentication for system users.

### 9.2 Access control requirements

The access control requirements for the shared machine learning system include:

– The shared machine learning system is required to support authorization mechanism for the data users to guarantee authorization of their data to participate in the shared machine learning.

– The shared machine learning system is recommended to support complete roles and authorization systems. The shared machine learning system is required to give explicit roles and access rights after the system user logs in the system.

– The shared machine learning system is recommended to require the user to re-authenticate or reactivate the session when the session is idle according to the training policy.

### 9.3 Security auditing requirements

The security auditing requirements for the shared machine learning system include:

– The shared machine learning system is required to support functions of log recording and log auditing for the data operations when users access the shared machine learning system.

– The shared machine learning system is recommended to support the history backtracking and auditing function for the main operations to the system.

### 9.4 Data security requirements

The data security requirements for the shared machine learning system include:

– The shared machine learning system is required to support the function of encrypted transmission and storage of important data.

– The processed data is required not to contain sensitive data required by relevant regulation.

– The shared machine learning system is required to support the limiting of transmission of data.

– The shared machine learning system is required to support secure transmission protocols or secure transmission channels to ensure the security and reliability of data transmission links and prevent being attacked.

– The shared machine learning system is required to ensure the confidentiality, integrity, and availability of data characteristics and samples, and the data is prohibited from being obtained illegally by unauthorized users.

– The shared machine learning system is required to destroy the trusted execution environment after completing the computation tasks in the centralized mode.

### 9.5 Privacy protection requirements

The privacy protection requirements for the shared machine learning system include:

– The shared machine learning system is required to ensure that data related to user privacy is not leaked to other data providers, coordinators, or users.

– The shared machine learning system is required to provide a mechanism to avoid being located or roughly located to an individual in any form from the information exchanged between the data providers.

– The shared machine learning system is required to allow data providers to use reasonable encryption methods in order to ensure that other parties other than the recipient can infer user privacy data from the encrypted interactive data to prevent possible attacks, such as brute force cracking, reasoning attacks, and so on.

– In the secure multi-party computing solution, the shared machine learning system is required to ensure that the user privacy-related data does not go out from the local storage, and only random numbers or parameters are exchanged between different data providers.

## 10 Technical architecture, functional components, and processing procedure of the shared machine learning system in centralized mode

### 10.1 Technical architecture of the shared machine learning system in the centralized mode

In a centralized mode of a shared machine learning system, local data from multi-party participants is processed, encrypted, and transmitted to a trusted execution environment to train the shared model. Since the data in each party is encrypted, the data cannot be seen by the platform or other participants. When multi-party participants or others have the authorization to access the shared model, they can get access to it by using application programming interfaces (APIs) to input information and to get outputs or predictions based on shared values.

Before providing data, participants (data providers) verify the correctness and validity of the software running in the trusted execution environment through remote attestation. After that, an encryption mechanism is negotiated between the participants and the trusted execution environment. Then, participants encrypt data using negotiated mechanism and send the ciphertext to the trusted execution environment. The encryption mechanism can be a symmetric encryption mechanism or asymmetric encryption mechanism.

To ensure the computed model will not be leaked, the trained model should be encrypted after the whole computation is completed.

The technical architecture is described in Figure 2.

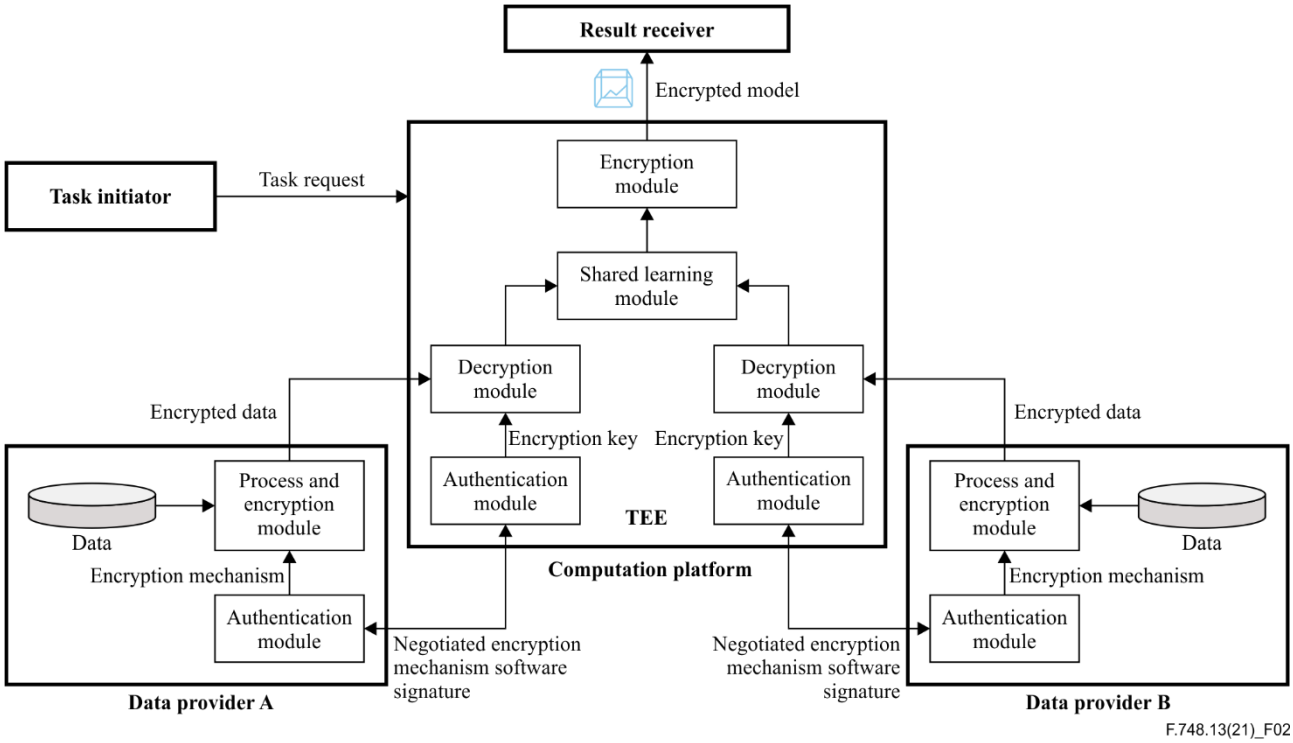


**Figure 2 – Technical architecture of the shared machine learning system in the centralized mode**

The technical architecture of the shared machine learning system in the centralized mode is mainly composed of a computation platform and multiple data providers. The computation platform is composed of authentication modules, decryption modules, encryption modules and a shared learning module. Each data provider consists of a process and encryption module, an authentication module, and data. The modules in the technical architecture are functional components.

The data of each data provider is processed and encrypted by the encryption key obtained from the authentication module, then the encrypted data is uploaded to the trusted execution environment of the computation platform. The authentication module of the computation platform decrypts the encrypted data by using the decryption key, and then sends the decrypted data to the shared learning module. The shared learning module performs the shared machine learning operation on the decrypted data from multiple data providers.

## 10.2 Functional components of the shared machine learning system in the centralized mode

The computation platform is mainly composed of authentication modules, decryption modules, encryption modules, and a shared learning module, all of which exist in a trusted execution environment (TEE).

– Authentication module: this module is responsible for negotiating the encryption mechanism with each data provider and providing the decryption key to the decryption module. The decryption key is used for decrypting the encrypted data uploaded by the data provider to the platform. The authentication module of the computation platform is responsible for signing the software code running in the trusted execution environment and supporting the data provider to check the software code.

– Decryption module: this module is responsible for decrypting the encrypted data uploaded by the data provider based on the decryption key. The decryption key can be an asymmetric key or a symmetric key.

– Shared learning module: this module is responsible for data training based on the decrypted data from multiple data providers to output a shared model.

– Encryption module: this module is responsible for encrypting the computed model after the whole computation is completed.

The data provider is mainly composed of data, process and encryption modules, and authentication modules. There are at least two data providers.

– Data: the data provided by the data provider can be processed, encrypted, and uploaded to the computation platform. The encrypted data can be encrypted raw data, calculation factors, or any other data needed to be protected when transmitting among participants and the computation platform.

– Process and encryption module: this module is used to process and encrypt the data based on the encryption mechanism negotiated with the computation platform, and then the encrypted data is uploaded to the computation platform.

– Authentication module: the authentication module of the data provider is used to realize remote authentication of the data provider and the computation platform, including negotiating the encryption mechanism with the computation platform, and checking the code signature.

The task initiator sends the computation task request to the computation platform and initiates the computation task.

The result receiver receives the encrypted result from the computation platform and gets the final result.

## 10.3 Processing procedures of the shared machine learning system in the centralized mode

In the centralized mode, any data provider or the computation platform can initialize computational tasks, then the computation platform creates a trusted execution environment. The local data provided by each data provider can be processed, encrypted, and uploaded to the computation platform. The platform decrypts the received encrypted data sent by each data provider in the trusted execution environment and performs model training based on the decrypted data to obtain a shared model. The data processing, encryption, decryption, and training steps can be repeated multiple times. Finally, the trusted execution environment is destroyed to ensure data security and privacy.

The processing procedures are described in Figure 3, and the processing procedures are recommended:

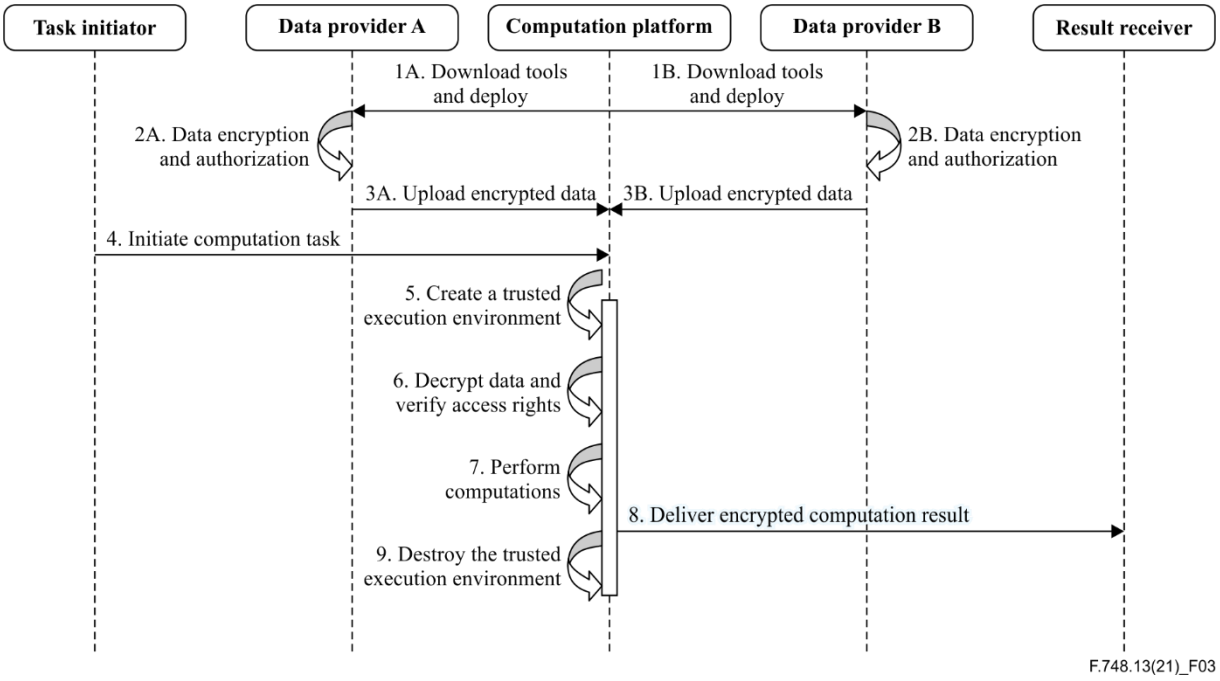


**Figure 3 – Processing procedures of the shared machine learning system in the centralized mode**

The technical process procedure of the shared machine learning system in the centralized mode are as follows:

– Step 1: data providers download tools from the computation platform and deploy the tools.

– Step 2: data providers perform the data preparation, including data encryption, data authorization.

– Step 3: data providers upload the encrypted data to the computation platform.

– Step 4: task initiator initiates computation tasks on the computation platform, including the model to be trained, and the algorithms.

– Step 5: the computation platform creates a trusted execution environment.

– Step 6: the computation platform decrypts the encrypted data in the trusted execution environment.

– Step 7: the computation platform performs computations with the decrypted data in the trusted execution environment to obtain a computation result.

– Step 8: the computation platform delivers the computation result to the result receiver.

– Step 9: the computation platform destroys the trusted execution environment and the data in it.

Note that the processing procedures above are normal procedures. In the real deployment, the orders and details of each procedure can be different. For example, the task initiator can initiate the computation in the first step. The data providers can upload encrypted data to the computation platform repeatedly. The modelling data or trained model can also be sealed up and stored outside the computation platform to be re-used later.

## 11 Technical architecture, functional components, and processing procedure of the shared machine learning system in decentralized mode

### 11.1 Technical architecture of the shared machine learning system in the decentralized mode

In the decentralized mode of the shared machine learning system, each party needs to deploy a learning module locally and transmit data to the local learning module. Learning modules among different data providers exchange parameters by using different encryption methods to achieve data sharing without exchanging raw data to protect data privacy. Computation platform assists to trigger the update of the learning module for each participant and coordinate relationships among different parties.

The technical architecture is described in Figure 4.

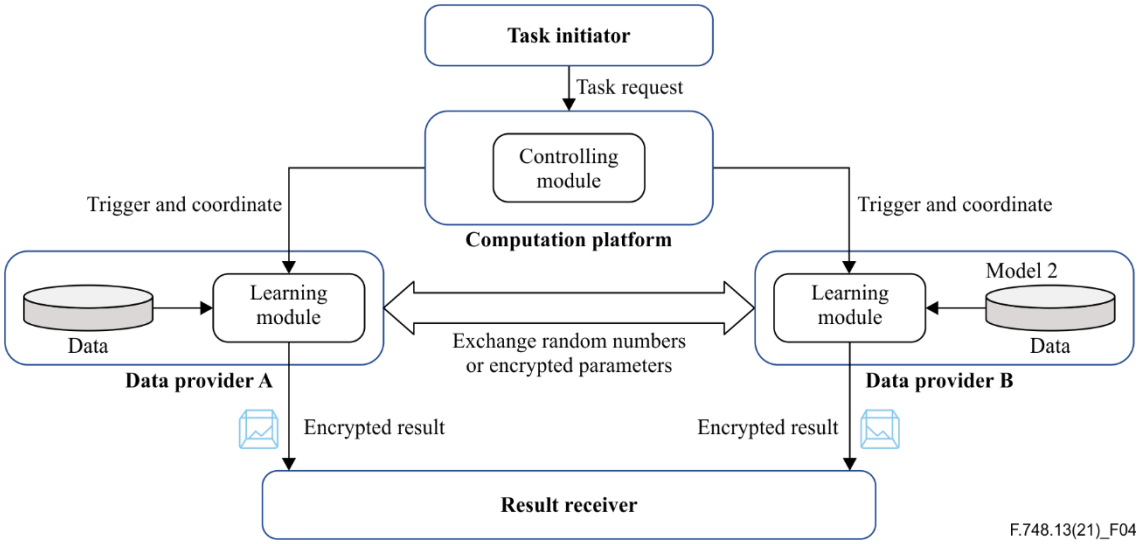


**Figure 4 – Technical architecture of the shared machine learning system in the decentralized mode**

The technical architecture of the shared machine learning system in the decentralized mode is mainly composed of a computation platform, a result receiver, a task initiator, and multiple data providers.

### 11.2 Functional components of the shared machine learning system in the decentralized mode

The computation platform mainly includes a controlling module, which divides computation tasks to different data providers, and coordinates with the learning modules in the data providers. Then the learning modules in each data provider exchange random numbers or encrypted parameters to perform the shared machine learning operation.

The data provider is mainly composed of data and learning modules. There are at least two data providers.

– Data: the data in the data provider is provided to the local learning module for machine learning. The data provider ensures that the users' privacy is not leaked.

– Learning module: this module is used to receive machine learning tasks issued by the computation platform and performs the shared machine learning operation based on the local data and random numbers or encrypted parameters exchanged from other data providers.

The result receiver receives the encrypted result from the data providers and gets the final result.

The task initiator sends the task request to the computation platform.

## 11.3 Processing procedures of the shared machine learning system in the decentralized mode

In the decentralized mode, data providers perform shared learning operations by exchanging information that would not leak the users' privacy based on an established multi-party computation protocol.

The recommended processing procedures of the decentralized solution are described in Figure 5.

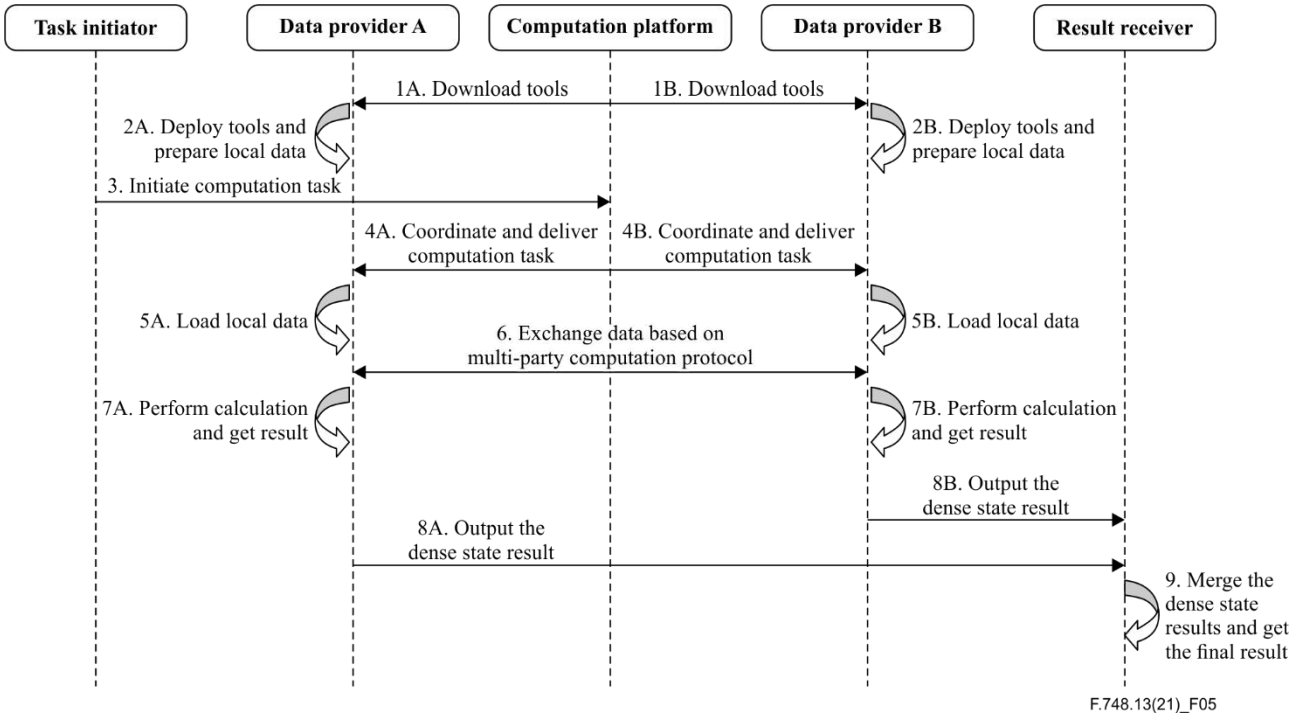


**Figure 5 – Processing procedures of the shared machine learning system in the decentralized mode**

The technical processing procedures of shared machine learning system are as follows:

– Step 1: each data provider downloads tools from the computation platform.

– Step 2: each data provider deploys the downloaded tools and prepares the local data.

– Step 3: the task initiator initiates computation tasks to the computation platform.

– Step 4: the computation platform coordinates and delivers the computation tasks to the data providers.

– Step 5: the data providers load local data for computation.

– Step 6: the data providers exchange random numbers or encrypted parameters through multiple interactions based on multi-party computation protocol.

– Step 7: the data providers perform dense state calculation and get dense state results.

– Step 8: the data providers output the dense state result to the result receiver.

– Step 9: the result receiver merges the dense state results and gets the final result.

# Appendix I

## Use cases for shared machine learning systems

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

Shared machine learning can be used in different types of services that need data sharing to train shared models and need data security as well.

This appendix describes use cases for shared machine learning systems to illustrate its concept and technical architectures.

### I.1 Use case: Improving modules for recognizing telecom frauds using data from multiple networks

It is valuable and important to detect and prevent telecom frauds in time and automatically. Usually, deceivers and being-deceived people may be in the same or different communication networks when they are in communication. Therefore, to train modules in recognizing telecom frauds would require close cooperation between multiple network operators, but based on the laws and regulations, the data of the communication networks are protected, separated, and are not allowed to be opened and exchanged.

The training mode of the shared machine learning can help overcome data access restrictions of multiple networks. In this training mode, the communication networks keep their raw data and just upload necessary desensitized information (such as data labels and index, not the data itself) to the model controlling platform (see Figure I.1). Without loss of generality, the model controlling platform can use the desensitized information to arrange the module training tasks to the local training platforms in the communication networks respectively. The module training tasks are performed by the module training executors in the local training platforms with the local raw data. As the training progresses, the local training platform can exchange and synchronize the parameters of the being-trained modules with that in the model controlling platform.

The trained modules for detecting telecom frauds can be deployed and performed in multiple communication networks respectively.

In this case, the network operators can use shared machine learning mechanisms and relevant systems to train and perform modules for detecting telecom frauds, and without directly sharing their raw data.

The overall framework for detecting telecom frauds using data from multiple networks is described in Figure I.1.

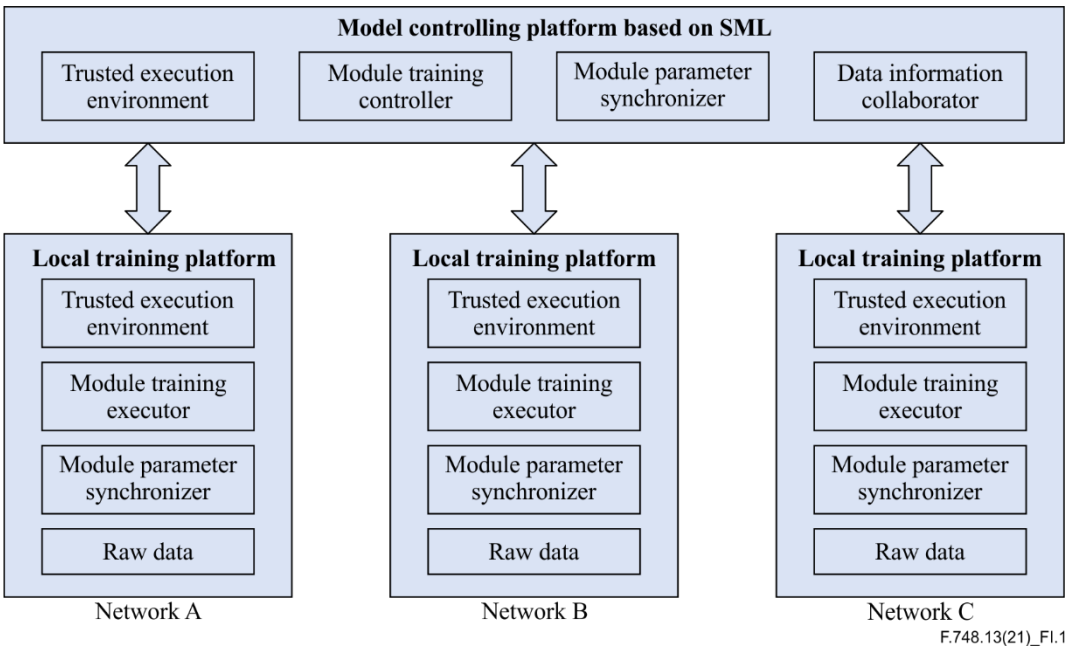


**Figure I.1 – Overall framework for detecting telecom fraud using data from multiple networks**

## I.2 Intelligent credit and risk control use case

Shared machine learning can be used in intelligent credit scenarios in the financial field. Encrypted users' credit data from different parties are gathered to train a shared risk control model by a trusted third party. Therefore, data providers, such as banks, financial institutions, and other related parties can use the shared model to check the credit qualification of individuals to determine the credit amount. The shared learning technology promotes the intelligent checking process and assists to reduce on-line human credit checking costs. Additionally, shared machine learning in this scenario can support user-side authorization and privacy data protection to realize better risk control.

## I.3 Intelligent marketing use case

Shared learning can provide a precise users' equity strategy and a secure sharing environment that improves risk identification. For example, in a car insurance scenario, shared machine learning can significantly improve the differentiated equity of car insurance. It can assist insurance companies to develop better sales strategies before users purchasing insurance under the conditions of users' authorization. Through the car owners' information, users with different risk levels can be subdivided. Further, accurate image and risk analysis can be carried out for the owners to realize the precise users' equity strategy.

# Bibliography

[b-ITU-T J.1201] Recommendation ITU-T J.1201 (2019), *Functional requirements of a smart TV operating system*.

[b-ITU-T Y.3172] Recommendation ITU-T Y.3172 (2019), *Architectural framework for machine learning in future networks including IMT-2020*.

## SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series D | Tariff and accounting principles and international telecommunication/ICT economic and policy issues |
| 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 | Telephone transmission quality, telephone installations, local line networks |
| Series Q | Switching and signalling, and associated measurements and tests |
| 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, next-generation networks, Internet of Things and smart cities |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2021