ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T F.748.35 (06/2024)

SERIES F: Non-telephone telecommunication services

Multimedia services

Requirement and framework of trustworthy federated machine learning based service

ITU-T F-SERIES RECOMMENDATIONS

Non-telephone telecommunication services

TELEGRAPH SERVICE	F.1-F.109
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	F.110-F.159
Mobile services and multidestination satellite services	F.110-F.159
TELEMATIC SERVICES	F.160-F.399
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	F.550-F.599
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.748.35

Requirement and framework of trustworthy federated machine learning based service

Summary

Federated machine learning (FML) is an emerging distributed machine learning paradigm that enables collaborative model training, learning, utilization and construction from a large number of distributed datasets on the basis of ensuring data security and legal compliance. In FML, computing takes place where the data are, and although the data are available, neither the data computing nor the data are visible. There are some challenges for FML-based services in aspects of trust as they perform in distributed or decentralized environments. All the challenges are often brought about by a lack of trust in the multiple participants of FML-based services, usually in the processes of model training and utilization, such as data indexing, data computing, parameter exchanging, etc.

Specific functional components are needed to enhance the trustworthiness of FML-based services, such as enhancing dataset indexing, data computing, parameter exchange and model utilization. The distributed ledger technology (DLT) system is one type of trustworthy shared data system that can be used to also store FML-based service data. The FML-based service can take advantage of the convergence between FML and those components, especially to help address trust-related challenges for FML-based services.

Recommendation ITU-T F.748.35 provides a trustworthy FML-based service, and specifies its concept, general characteristics and requirements, and reference framework.

History[*]

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T F.748.35	2024-06-13	16	11.1002/1000/15914

Keywords

Distributed ledger technology (DLT), federated machine learning (FML), framework, trustworthiness.

[*] 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/.

Table of Contents

Recommendation ITU-T F.748.35

Requirement and framework of trustworthy federated machine learning based service

1 Scope

This Recommendation provides the requirements and framework of trustworthy federated machine learning (FML) based services.

The scope includes:

– Concept, general characteristics and requirements of trustworthy FML-based services;

– Reference framework of trustworthy FML-based services.

Use cases of trustworthy FML-based service are provided in an appendix.

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 distributed ledger [b-ITU-T X.1400]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

3.1.2 distributed ledger technology (DLT) [b-ITU-T X.1400]: Technology that enables the operation and use of distributed ledgers.

3.1.3 federated machine learning (FML) [b-IEEE P3652.1]: A framework or system that enables multiple participants to collaboratively build and use machine learning models without disclosing the raw and private data owned by the participants while achieving good performance.

3.1.4 federated machine learning model (FMLM) [b-IEEE P3652.1]: The result of the model-training process of a federated machine learning system. The learned model can be used in order to make certain machine-learning inference tasks on new data, e.g., classification, recognition, prediction, and recommendation.

3.1.5 ledger [b-ITU-T X.1400]: Information store that keeps final and definitive (immutable) records of transactions.

3.1.6 trust [b-ITU-T Y.3052]: The measurable belief and/or confidence which represents accumulated value from history and the expecting value for the future.

NOTE – Trust is quantitatively and/or qualitatively calculated and measured. Trust is used to evaluate values of entities, value-chains among multiple stakeholders and human behaviours, including decision making.

3.1.7 trustworthy [b-ISO/TR 15801]: Ability to demonstrate authenticity, integrity and availability of electronically stored information over time.

3.1.8 trusted system [b-ISO/TR 15801]: Information technology system with the capability of managing electronically stored information in a trustworthy manner.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 federated machine learning coordinator: A party who composes and manages tasks for federated machine learning (FML) model training and utilization through coordination with FML participants.

3.2.2 federated machine learning participant: A party who provides datasets and computing resources to participate the activities of a federated machine learning (FML)-based service, such as data pre-processing, model training, model utilization, etc.

3.2.3 federated machine learning model training dataset: A dataset to be used to train federated machine learning (FML) models.

3.2.4 federated machine learning model training module: An executable program to be used to train federated machine learning (FML) models with FML model training datasets.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DLT	Distributed Ledger Technology
FML	Federated Machine Learning
FMLM	Federated Machine Learning Model
FMLS	Federated Machine Learning-based Service
ML	Machine Learning
RMCT	Robust Model Compression Training
T-FMLS	Trustworthy FML-based Service
TSS	Trustworthy Shared Storage

5 Conventions

This Recommendation uses the following conventions:

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

– The keywords "is recommended" indicate a requirement that is recommended, but which is not absolutely required to claim conformance with this Recommendation.

6 Overview of trustworthy FML-based services

Federated machine learning (FML) is an emerging distributed machine learning (ML) paradigm that enables collaborative model training, learning, utilization and construction from a large number of distributed datasets on the basis of ensuring data security and legal compliance. In FML, computing takes place where the data are, and although the data are available, neither the data computing nor the data are visible.

In traditional FML-based services (see Figure 6-1), FML coordinators and FML participants exchange information directly. FML coordinators coordinate and manage dataset indexes, model training and utilization progress, and store and manage full data of the entire lifecycle for dataset indexes, model training and utilization. FML coordinators usually act as trust points for traditional FML-based services. There are some challenges for traditional FML-based service for it works in distributed or decentralized environments, trusted or untrusted. The main challenges are listed in Appendix I. All those challenges are often brought about by a lack of trust in the multiple distributed or decentralized participants of the traditional FML-based service. Appendix I also provides more information about impact factors for trustworthiness of FML-based services.

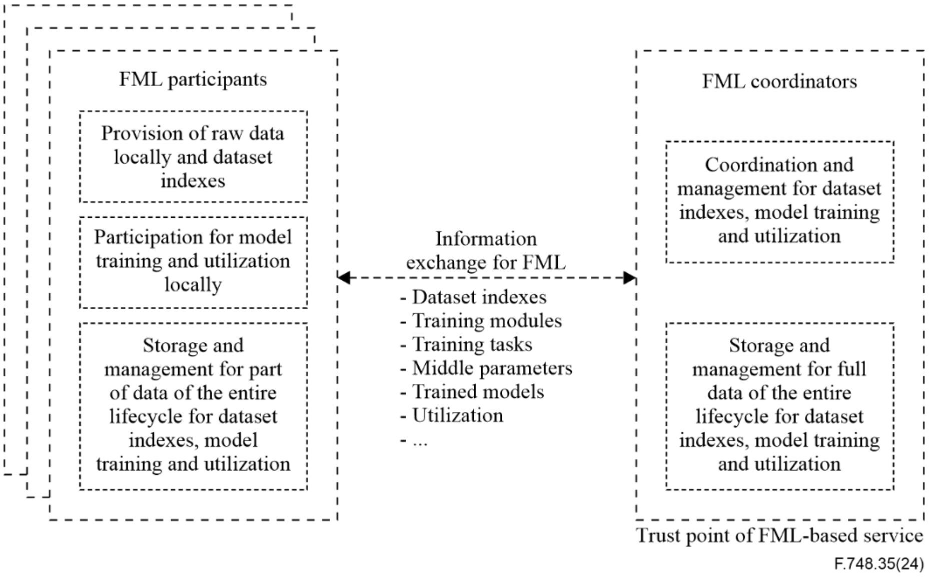
FML participants
Provision of raw data locally and dataset indexes
Participation for model training and utilization locally
Storage and management for part of data of the entire lifecycle for dataset indexes, model training and utilization
Information exchange for FML
- Dataset indexes
- Training modules
- Training tasks
- Middle parameters
- Trained models
- Utilization
- ...
FML coordinators
Coordination and management for dataset indexes, model training and utilization
Storage and management for full data of the entire lifecycle for dataset indexes, model training and utilization
Trust point of FML-based service
F.748.35(24)

Figure 6-1 – Overview of traditional FML-based service

Distributed ledger technologies (DLT) have inherent advantages to leverage data management and sharing, such as peer to peer communication, decentralization, immutability, openness, crowd consensus and smart contract support and automatization. The FML-based service can benefit from the convergence between FML and DLT , especially in addressing the challenges mentioned above.

Figure 6-2 gives an overview of a trustworthy FML-based service (T-FMLS). In this paradigm, FML coordinators and FML participants exchange information through a trustworthy shared storage (TSS), not directly with each other. The TSS is used to store and manage the information of the entire lifecycle for dataset indexes, model training and utilization for the T-FMLS.

NOTE – T-FMLS is independent from TSS. TSS may be based on a DLT system. TSS and DLT are out of the scope of this Recommendation.

In T-FMLS, FML participants store their training datasets (sets of raw data) locally and provide indexes of the training datasets in the TSS. The TSS keeps the data indexes to prevent tampering. An index of raw data includes descriptions of the raw data, information on accessing the raw data, and a digest of the raw data which is used to validate the relationship between the index and the raw data. The digest in an index can be encrypted by the FML participants.

In T-FMLS, FML coordinators store FML model training modules in the TSS. The TSS keeps the FML model training modules to prevent tampering. FML model training modules are open to relevant FML participants. FML model training modules can be programmed as smart contracts of the TSS. In addition, FML participants can utilize the robust model compression training (RMCT) technique to lighten the model while ensuring the robustness of the compressed model compared to traditional model compression techniques. RMCT technique can be used to reduce the size of models in FML with limited communication and storage resources, and includes adversarial training, differential privacy, quantization-aware training, knowledge distillation, etc.

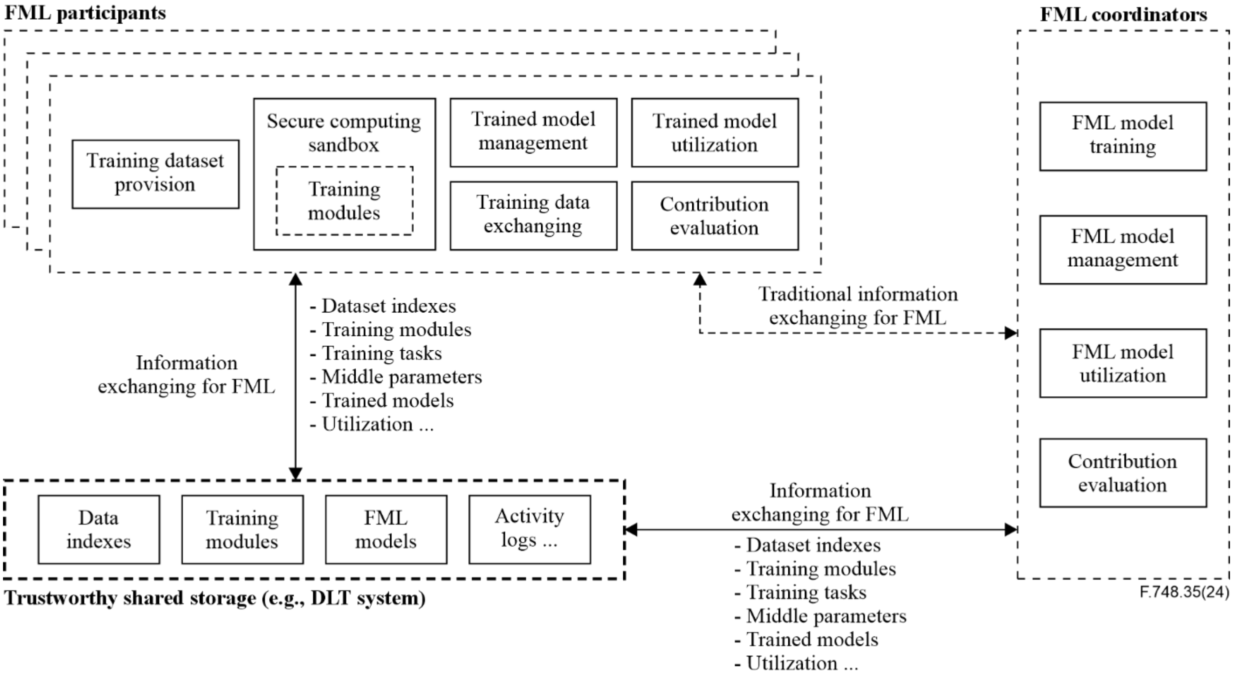

Figure 6-2 – Overview of trustworthy FML-based service

In T-FMLS, by using data indexes and training modules stored in TSS, FML coordinators can compose and manage FML model training tasks. In an FML model training task, data indexes and training modules are selected by the FML coordinator. During an FML model training task, the training modules are performed in a secure computing sandbox of each FML participant, and the training modules can validate the relationship of the indexes provided by FML coordinators with the raw data provided by FML participants. In the meantime, training parameters are exchanged between FML coordinators and FML participants through TSS, and the model training results and relevant activity logs can be stored in TSS as well. TSS provides trust capability to store data indexes, training modules, training result and relevant activity logs. Therefore, this paradigm of trustworthy FML-based services can enhance their trustworthiness and data security.

7 General characteristics and requirements of trustworthy FML-based services

7.1 General characteristics of trustworthy FML-based services

7.1.1 Trustworthy full-lifecycle management for FML model training tasks

T-FMLS provides trustworthy full-lifecycle management of FML model training tasks, including at least:

– Creating and managing of FML model training tasks;

– Managing of FML model training progresses;

– Managing and utilizing relevant trained FML models;

– Tracing and tracking FML model training and result management.

Relevant information of FML model training is stored in TSS, which prevents information tampering.

7.1.2 Trustworthy module provision for FML model training

T-FMLS improves the following distinct characteristic of FML-based services: "computing is available but it is not visible".

FML model training modules are usually transparent and stored in TSS. T-FMLS participants can check and validate the FML model training modules independently. They can also trace and track the utilization of the FML model training modules.

Typically, each T-FMLS participant provides secure computing sandbox and performs the FML model training modules in the secure computing sandbox to guarantee security of computing environment of each FML participant.

7.1.3 Trustworthy data provision and computing for FML model training

T-FMLS improves another distinct characteristic of the FML-based service, "data are available but not visible". Where the data are is where is the computing takes place, and data are not moved out of their secure domain.

In T-FMLS, FML participants keep raw data in their secure domains and share data indexes through TSS. The FML coordinators select and use the data indexes and FML model training module(s) to compose FML model training tasks.

When FML participants perform an FML model training task, they provide raw data that match relevant data indexes. The FML model training module of the FML model training task can validate the relationship between the raw data and the relevant data indexes. Furthermore, more it may measure quality and quantity of the dataset to be used to train the FML model. All the information of activities of data provisioning and computing can be stored in TSS. FML participants and coordinators can then trace and track the whole progresses of the FML model training task and evaluate their relevant contributions to the FML model training and utilization.

7.1.4 Trustworthy parameters exchange for FML model training

T-FMLS guarantees that no sensible information and no row data are leaked when exchanging training parameter for FML model training. The exchanged information is stored in TSS and can be traced and tracked.

7.1.5 Trustworthy model management for trained FML model

T-FMLS improves the following distinct characteristic of the FML-based service: "the trained model is available, but it is not visible". The trained FML models can be distributed to be stored by the FML participants and coordinators. T-FMLS guarantees trustworthy storage and management of the trained FML models and guarantee that the participants can follow the utilization of their trained FML models.

7.1.6 Compliance with national and regional data regulations

T-FMLS is compliant with national and regional data regulations when FML coordinators deploy FML model training tasks to FML participants and when FML coordinators and participants perform trained FML models.

7.1.7 Robustness and scalability for FML model training

T-FMLS guarantees the robustness and scalability of FML model training, including reducing negative impacts of failures from a single or several of the FML participants.

T-FMLS guarantees RMCT, which ensures that FML models trained on multiple FML participants are robust against adversarial attacks. In T-FMLS, multiple FML participants can jointly train FML models while keeping their data decentralized and private. Adversarial attacks are a type of security threat where an attacker manipulates the input data to deceive the model into producing incorrect outputs. FML model training tasks are working in distributed or decentralized environments which may become vulnerable to adversarial attacks. RMCT ensures model robustness by allowing the compressed model to perform normal inference under various conditions, such as when dealing with noisy or perturbed data.

7.2 General requirements of trustworthy FML-based services

7.2.1 Requirements for task management of FML model training

- It is required to provide TSS to allow FML participants and FML coordinators to save and retrieve information (such as data indexes, parameters, modules and activity logs), respectively and independently.
- It is required that each FML model training task of T-FMLS has a global unique identity which is used in its full lifecycle.
- It is required to allow activity logs of management of FML model training tasks in full lifecycle to be stored in the TSS, including at least:
  - That of creating and managing of FML model training tasks;
  - That of managing of FML model training progresses;
  - That of managing and utilizing relevant trained FML models;
  - That of tracing and tracking FML model training and result management.
- It is required that information of FML model training tasks is stored in the TSS.
- It is required to be compliant with national and regional data regulations when FML coordinators deploy FML model training tasks to FML participants.

7.2.2 Requirements for module provision for FML model training

- It is required to allow FML model training modules to be stored in the TSS.
- It is required to provide a mechanism to allow FML participants to check and validate FML model training modules independently when they are used to train FML models, according to FML model training tasks.
- It is required to provide mechanism to allow each FML participant to provide a secure computing sandbox and to perform FML model training modules in the secure computing sandbox to guarantee security of the computing environment.
- It is required to provide a mechanism to allow FML model training modules being performed to store activity logs to the TSS, according to relevant FML model training tasks and the rules of FML participants.
- It is recommended to allow FML participants and FML coordinators to trace and track the utilization of the FML model training modules independently.

7.2.3 Requirements for data provision and computing for FML model training

- It is required to provide s mechanism to allow FML participants to share data indexes that match corresponding raw data and allow FML coordinators to create FML model training tasks according to the shared data indexes.
- It is required to provide a mechanism to allow FML participants to avoid raw data to be leaked out of its original domain when performing FML model training.
- It is required to provide a mechanism to allow FML model training modules being performed to check and validate raw data provided by FML participants, according to relevant FML model training tasks.
- It is recommended to allow FML participants and FML coordinators to trace and track the utilization of the data indexes independently.

- It is recommended to provide mechanism to allow FML participants and FML coordinators to measure the quality and quantity of the datasets to be used to train FML models independently.

7.2.4 Requirements for parameter exchanging for FML model training

- It is required that no sensible information and no row data are leaked when exchanging training parameters for FML model training.
- It is recommended to provide a mechanism to allow FML participants and FML coordinators to trace and track the exchanged training parameters independently, if allowed.
- It is required to be compliant with national and regional data regulations when parameters are being exchanged for FML model training.

7.2.5 Requirements for model management for trained FML models

- It is recommended to allow trained FML models to be stored in distributed storage by the FML participants and FML coordinators, according to policies of FML model training tasks.
- It is required to guarantee trustworthy storage and management for trained FML models, and to allow FML participants and FML coordinators to follow the utilization of their trained FML models.
- It is required to be compliant with national and regional data regulations when FML coordinators and participants perform trained FML models.

7.2.6 Requirements for robustness and scalability for FML model training

- It is required to guarantee robust and scalable FML model training, including reducing negative impacts of failures from one or several participants.
- It is required to allow FML participants to perform RMCT, including:
  - Adversarial training to ensure inference integrity by utilizing data perturbation;
  - Differential privacy to prevent models from memorizing training data;
  - Quantization-aware training to be robust against model inversion attacks;
  - Distillation learning to protect local privacy.

7.2.7 Requirements for data security protection

- It is required to provide a mechanism to protect data security, such as raw data, data indexes, FML model training tasks, trained FML models, etc.

8 Reference framework of trustworthy FML-based services

This clause provides a reference framework of the trustworthy FML-based service (T-FMLS) according to the requirements listed in clause 7.

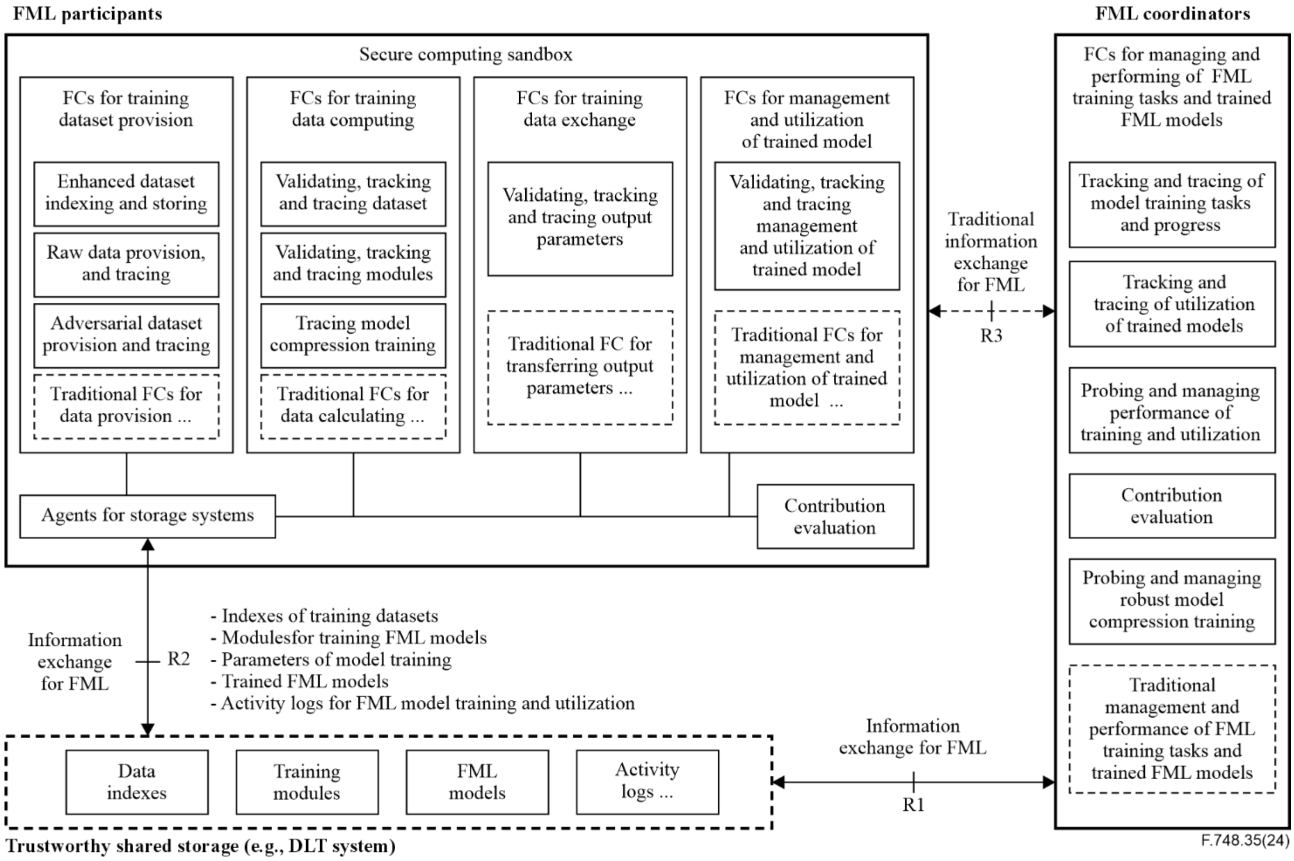
FML participants
FML coordinators
Secure computing sandbox
FCs for training dataset provision
Enhanced dataset indexing and storing
Raw data provision, and tracing
Adversarial dataset provision and tracing
Traditional FCs for data provision ...
FCs for training data computing
Validating, tracking and tracing dataset
Validating, tracking and tracing modules
Tracing model compression training
Traditional FCs for data calculating ...
FCs for training data exchange
Validating, tracking and tracing output parameters
Traditional FC for transferring output parameters ...
FCs for management and utilization of trained model
Validating, tracking and tracing management and utilization of trained model
Traditional FCs for management and utilization of trained model ...
Agents for storage systems
Contribution evaluation
Traditional information exchange for FML
R3
FCs for managing and performing of FML training tasks and trained FML models
Tracking and tracing of model training tasks and progress
Tracking and tracing of utilization of trained models
Probing and managing performance of training and utilization
Contribution evaluation
Probing and managing robust model compression training
Traditional management and performance of FML training tasks and trained FML models
Information exchange for FML
R2
- Indexes of training datasets
- Modulesfor training FML models
- Parameters of model training
- Trained FML models
- Activity logs for FML model training and utilization
Information exchange for FML
R1
Data indexes
Training modules
FML models
Activity logs ...
Trustworthy shared storage (e.g., DLT system)
F.748.35(24)

Figure 8-1 – Diagram of reference framework of trustworthy FML-based services

The T-FMLS mainly consists of three parts, multiple FML coordinators and FML participants, and trustworthy shared storage (TSS). Each of them includes groups of logical functional components (FCs).

Each FML coordinator of the T-FMLS includes groups of FCs for FML training tasks, trained FML models and contribution evaluation, including as least:

– FCs for tracking and tracing model training tasks and progress;

– FCs for tracking and tracing utilization of trained models;

– FCs for probing and managing performance of training and utilization of FML models;

– FCs for contribution evaluation;

– FCs for probing and managing robust model compression training;

– FCs for traditional task composition and management for FML model training and utilization;

– Agents for storage systems.

Each FML participant of the T-FMLS includes groups of FCs for FML training tasks, trained FML models and contribution evaluation, including as least:

– FCs for training dataset provision;

– FCs for training data computing, in secure computing sandboxes;

– FCs for training parameter exchange;

– FCs for management and utilization of trained models;

– FCs of contribution evaluation;

– Agents for storage systems.

The TSS is an entity external to the T-FMLS, with which the FML participants and coordinators store and exchange information for FML model training and trained FML models, such as data indexes, training modules, FML models and activity logs.

An FML coordinator exposes two reference points, R1 and R3. R1 is for information exchange for FML model training and trained FML model utilization by using the TSS. R3 is a traditional reference point through which the traditional FML coordinators and FML participants exchange information for FML model training and trained FML model utilization directly.

An FML participant exposes reference point R2. R2 is for information exchange for FML model training and trained FML model utilization by the TSS.

NOTE – The TSS may be based on DLT systems. The TSS and reference point R3 are out of the scope of this Recommendation.

8.1 Functional components of FML coordinators

8.1.1 FCs for tracking and tracing model training tasks and progress

An FML coordinator of a given T-FMLS supports tracking and tracing FML model training tasks and progress.

8.1.2 FCs for tracking and tracing utilization of trained models

An FML coordinator of a given T-FMLS supports tracking and tracing the utilization of trained FML models.

8.1.3 FCs for probing and managing performance of training and utilization

An FML coordinator of a given T-FMLS supports probing and managing the performance of FML model training and utilization.

8.1.4 FCs for contribution evaluation

An FML coordinator of a given T-FMLS supports evaluation of its contribution to each task of the FML model training and utilization.

8.1.5 FCs for probing and managing robust model compression training

An FML coordinator of a given T-FMLS supports probing and managing robust model compression training.

8.1.6 FCs for traditional task composition and management for FML model training and utilization

An FML coordinator of a given T-FMLS supports traditional task composition and management for FML model training and utilization.

8.1.7 Agents for storage systems

Agents for storage systems of an FML coordinator of a given T-FMLS is to connect to trustworthy shared storage to support exchanging information for FML model training and utilization.

8.2 Functional components of FML participants

8.2.1 FCs for training dataset provision

An FML participant of a given T-FMLS supports training dataset provision related functional components of traditional FML-based service. Besides, it supports enhanced functionalities for dataset indexing and storing, raw data providing and tracing, adversarial dataset provision and tracing.

8.2.2 FCs for training data computing

An FML participant of a given T-FMLS supports training data computing related functional components of traditional FML-based service. Besides, it supports enhanced functionalities for validating, tracking and tracing dataset, and validating, tracking and tracing training modules, and tracing model compression training. Data computing is performed in secure computing sandboxes of FML participants.

8.2.3 FCs for training data exchange

An FML participant of a given T-FMLS supports exchanging training parameters related functional components of traditional FML-based service. Besides, it supports enhanced functionalities for validating, tracking and tracing the parameters to be exchanged for FML model training.

8.2.4 FCs for management and utilization of trained machine learning (ML) models

An FML participant of a given T-FMLS supports management and utilization of trained ML models of traditional FML-based service. Besides, it supports enhanced functionalities for validating, tracking and tracing management and utilization of trained models.

8.2.5 FCs for contribution evaluation

An FML participant of a given T-FMLS supports evaluation of its contribution to each task of the FML model training and utilization.

8.2.6 Agents for storage systems

Agents for storage systems of an FML participant of a given T-FMLS is to connect to trustworthy shared storage to support exchanging information for FML model training and utilization.

8.3 External entities

8.3.1 Trustworthy shared storage

The trustworthy shared storage (e.g., a DLT system) is an entity external to a T-FMLS, with which the FML participants and coordinators store and exchange information for FML model training and trained FML models.

8.4 Reference points

An FML coordinator exposes reference point R1 for information exchange for FML model training and trained ML model utilization by using trustworthy shared storage.

An FML participant exposes reference point R2 for information exchange for FML model training and trained ML model utilization by using trustworthy shared storage.

An FML coordinator exposes traditional reference point R3 with which the traditional FML coordinator and FML participants to exchange information for FML model training and trained FML model utilization directly.

Appendix I

Challenges and impact factors for trustworthiness of FML-based services

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

There are some challenges for the traditional FML-based service as it works in distributed or decentralized environments, trusted or untrusted, mainly as given below:

– In the model training phase of the traditional FML-based service:

  - Computing: Because computing environments are diverse and managed by different participants, the challenges include to guarantee that computing environments are trusted, to guarantee that the training modules performed by each participant are consistent and secure, etc.
  - Dataset provision: Because the dataset and the relevant data computing are available but are not visible, the challenges include how to have other participants trust the provided data.
  - Data exchange: Because training parameters should be exchanged for model training, the challenges include how to guarantee that the raw data are not leaked during model training, etc.
  - Model management: Relevant challenges include where to store the trained model, whether using one integrated model or using distributed model slices stored by different participants. How to guarantee that a trained model can be used if it is stored in distributed storage, etc.
  - Robust of training: Relevant challenges include how to protect model training from interruption and disturbance by a part of the participants, etc.

– In the model utilization phase of traditional the FML-based service:

  - Model utilization: Relevant challenges include how to identify a trained model to be used, and how the participants can obtain continuous benefits from the trained models if they had contributed to the training.

According to the challenges for traditional FML-based services mentioned above, there are some important impact factors to the trustworthiness of FML-based services as given below.

I.1 Dataset provision for FML model training

FML-based service has a distinct characteristic that is "data are available but they are not visible". That means that "computing takes place where the data are". Because the data used for FML model training are not visible, there are some impact factors for each participant to let other participants and the coordinator accept the dataset, including:

– The quality and quantity of the dataset provided for model training are valuable;

– The actual calculated dataset for model training matches the pre-declared dataset, etc.

I.2 Computing for FML model training

FML-based service has another distinct characteristic that is "computing is available, but it is not visible". Because the computing in FML model training progress is not visible, there are some impact factors as shown below (but not limited):

– Whether the training modules performed by each FML participant are consistent;

– Whether the training modules performed are secure for executing environment;

– Whether the training modules performed are secure for the raw data;

- Whether the training modules can validate and guarantee the dataset provided by each FML participant to match to pre-declared dataset;
- Whether the computing capability of each FML participant is valuable, etc.

I.3 Communication for FML model training

It is necessary to exchange parameters when training FML models in FML-based services. Therefore, there are some risks related to the leaking of sensitive data when parameters for FML model training are exchanged. There is at least the following relevant impact factor:

- How to guarantee that the sensible information of raw data of FML participants is not leaked when model training parameters are exchanged, etc.

I.4 Model utilization of FML model

There is another distinct characteristic of FML-based service, "the trained model of FML is available, but it is not visible". Each participant contributes part of raw data provision and computing, and then usually only stores part of the trained FML model. Therefore, at least the following relevant impact factors exist:

- Who and how is the trained model to be stored;
- Who can use the trained model, and how to can all the FML participants benefit according to their real contribution, etc.

Because of the important impact factors for trustworthiness of FML-based services mentioned above, it is needed to provide technical mechanisms to improve trustworthiness among FML participants and coordinators when they collaborate to provide FML-based services.

Appendix II

Use cases of trustworthy FML-based services

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

II.1 Trustworthy FML-based services in an autonomous driving environment

The FML-based autonomous driving service consists of three entities: an autonomous driving terminal (FML participant), a trustworthy shared data storage (DB) system, and an autonomous driving system (FML coordinator).

The autonomous driving terminal (FML participant) provides federated machine learning and inference functions in autonomous vehicle. The autonomous driving terminal may be a personal or a shared autonomous driving terminal. The autonomous driving terminal enables machine learning and inference function for user preference service. The autonomous driving terminal transfers the learning models to an autonomous driving system through communication networks.

The communication network can utilize the existing edge network environment. For example, it supports wireless local area network (LAN), etc. The communication network provides a function of transmitting a result of processing an autonomous driving service between the autonomous driving terminal (FML participant) and the autonomous driving system (FML coordinator).

The autonomous driving system (FML coordinator) may consist of edge communication network and shared data storage system, handles learning models from the autonomous terminal and learns from information of the surrounding environment. The system contains three functions, namely, autonomous service management function, user information management function and service information management function. The autonomous service management function supports an autonomous driving service from the surrounding environment of the user terminal. The user information management function is responsible for user registration and storage service related to autonomous driving information. The service information management function supports artificial intelligence learning on autonomous driving terminals with surrounding environment information to manage machine-based learning models.

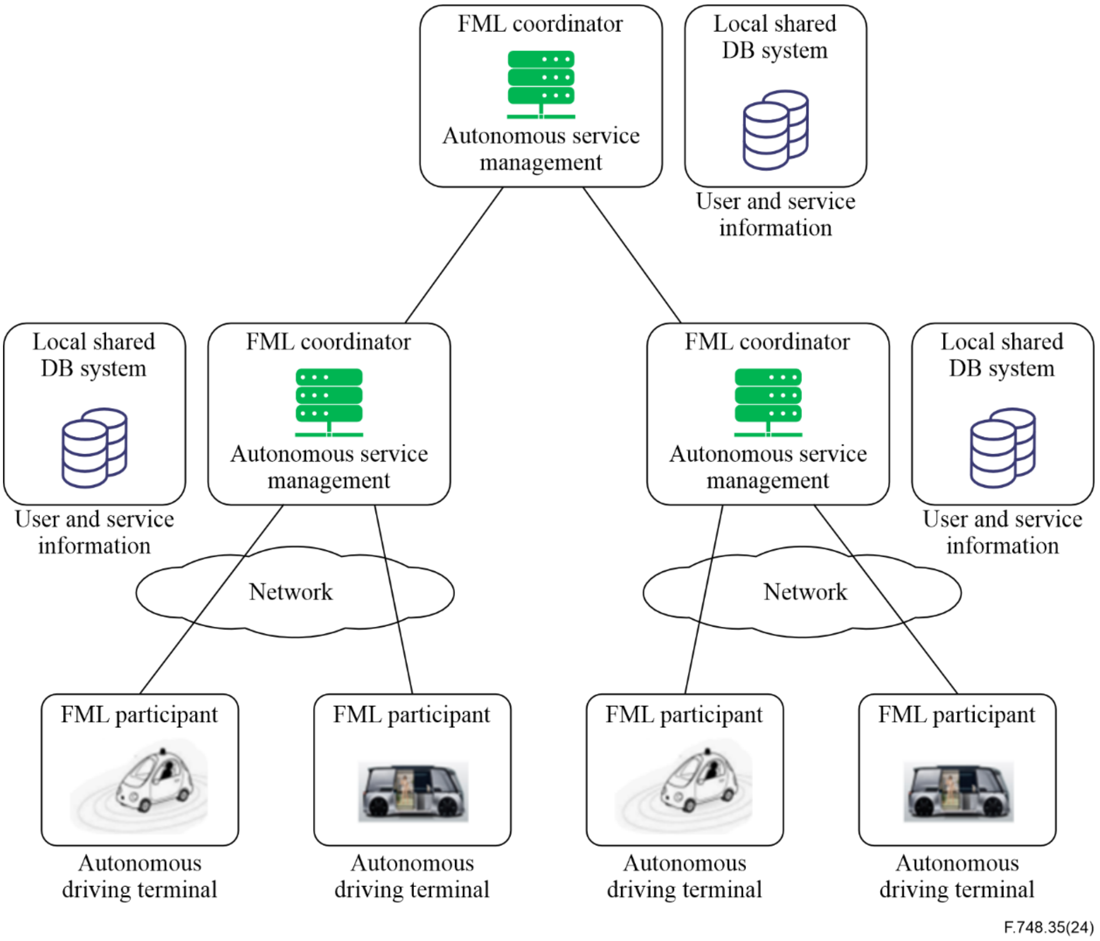
FML coordinator
Autonomous service management
Local shared DB system
User and service information
Local shared DB system
User and service information
FML coordinator
Autonomous service management
FML coordinator
Autonomous service management
Local shared DB system
User and service information
Network
Network
FML participant
Autonomous driving terminal
FML participant
Autonomous driving terminal
FML participant
Autonomous driving terminal
FML participant
Autonomous driving terminal
F.748.35(24)

Figure II.1 – Trustworthy FML based service in autonomous vehicle environment

Bibliography

[b-ITU-T X.1400]	Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.
[b-ITU-T Y.3052]	Recommendation ITU-T Y.3052 (2017), *Overview of trust provisioning in information and communication technology infrastructures and services*.
[b-IEEE P3652.1]	IEEE Standard P3652.1 (2020), *IEEE Guide for Architectural Framework and Application of Federated Machine Learning*.
[b-ISO/TR 15801]	ISO/TR 15801:2017, *Document management – Electronically stored information – Recommendations for trustworthiness and reliability*.

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

Published in Switzerland
Geneva, 2024