ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T F.748.24 (04/2024)

SERIES F: Non-telephone telecommunication services

Multimedia services

Trusted contribution evaluation framework on federated machine learning services

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.748.24

Trusted contribution evaluation framework on federated machine learning services

Summary

Federated machine learning (FML) is an emerging distributed framework that enables collaborative machine learning (ML) and model construction across distributed and decentralized datasets. FML service has distinctive features, such as location of data in the calculation, and data availability without visibility. It allows participants to jointly train ML models without sharing raw data, which can technically break data isolation and promote cooperation among data owners.

FML service involves multiple participants who usually perform different contributions to ML model training tasks due to their many impact factors. An effective and trusted contribution evaluation mechanism for FML service is essential to increase participation of the parties involved and can promote sustainable development of FML services.

Recommendation ITU-T F.748.24 introduces a trusted contribution evaluation service for FML service that combines and takes advantage of FML and distributed ledger technology functionalities, and provides relevant concepts, characteristics, requirements and use cases, and specifies a relevant reference framework and common capabilities.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T F.748.24	2024-04-15	16	11.1002/1000/15609

Keywords

Contribution degree, evaluation service federated machine learning.

* 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, 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.748.24

Trusted contribution evaluation framework on federated machine learning services

1 Scope

This Recommendation provides a trusted contribution evaluation service (CES) for federated machine learning (FML) services, and specifies relevant requirements, a reference framework and common capabilities.

This Recommendation includes:

– the concept, characteristics and requirements of a CES for FML services;

– a reference framework and common capabilities of a CES for FML services.

Use cases of trusted a CES for FML services.

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 distributed ledger technology system (DLT system) [b-ITU-T X.1400]: A system that implements a distributed ledger.

3.1.4 federated machine learning (FML) [b-IEEE 3652.1]: Federated machine learning (FML) is 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.

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

3.1.6 service [b-ITU-T Y.2091]: A set of functions and facilities offered to a user by a provider.

3.1.7 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.

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

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CC Contribution Calculator

CES Contribution Evaluation Service

DC Data Collection

DLT Distributed Ledger Technology

FC Functional Component

FML Federated Machine Learning

ML Machine Learning

MMM ML Model Management

PII Personally Identifiable Information

TM Task Management

5 Conventions

This Recommendation uses the following conventions:

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

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

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

6 Overview of a contribution evaluation service for federated machine learning services

FML is an emerging distributed framework that enables collaborative ML and model construction across distributed and decentralized datasets. FML service has distinctive features, such as location of data in the calculation, and data availability without visibility. It allows participants to jointly train ML models without sharing raw data directly, which can technically break data isolation and promote cooperation among data owners.

FML service involves multiple participants who usually perform different contributions to ML model-training tasks due to many impact factors of the participants, such as quantity, quality and

types of datasets, and capabilities of computing and communication. An effective and trusted contribution evaluation mechanism for FML service is essential to increase participation of the parties involved and can promote the sustainable development of FML services.

In the traditional coordination paradigm of FML services, depicted in Figure 6-1-a, FML training coordinators exchange information directly with each FML training participants for ML model training and utilization, in which the exchanged information usually includes modules, parameters and dataset indexes. FML training coordinators can store all exchanged information and final ML models, but FML training participants only can store part of the exchanged information generated by themselves individually. In this paradigm, for an ML model-training task, usually only FML training coordinators have full information to calculate the contribution degree of FML training participants.

Distributed ledger technologies (DLTs) have inherent advantages to leverage data management and sharing, such as peer to peer communication, decentralization, data immutability, openness, crowd consensus, and support and automation of smart contracts. DLT systems can be used as trustworthy shared storage for exchanging data for ML model-training tasks, and also for algorithms and modules to evaluate contributions. In this case, FML training coordinators and FML training participants can calculate contribution degrees for ML model-training tasks independently and consistently.

The trusted CES takes advantages of DLT and enhances contribution evaluation capability on FML services. Figure 6-1-b depicts the relevant enhanced coordination paradigm of FML services for contribution evaluation. In this paradigm, FML training coordinators and FML training participants exchange information for ML model training and utilization through CES and DLT systems. The CES manages ML model-training tasks, and acts as a bridge for FML training coordinators and FML training participants to exchange information for ML model training and utilization. The CES also stores relevant information in DLT systems. DLT systems guarantee the reliability, integrity, consistency, availability and non-tampering of relevant information. The CES, supported by DLT systems, provides a trusted evaluation service to evaluate contribution degree on FML services for each participant.

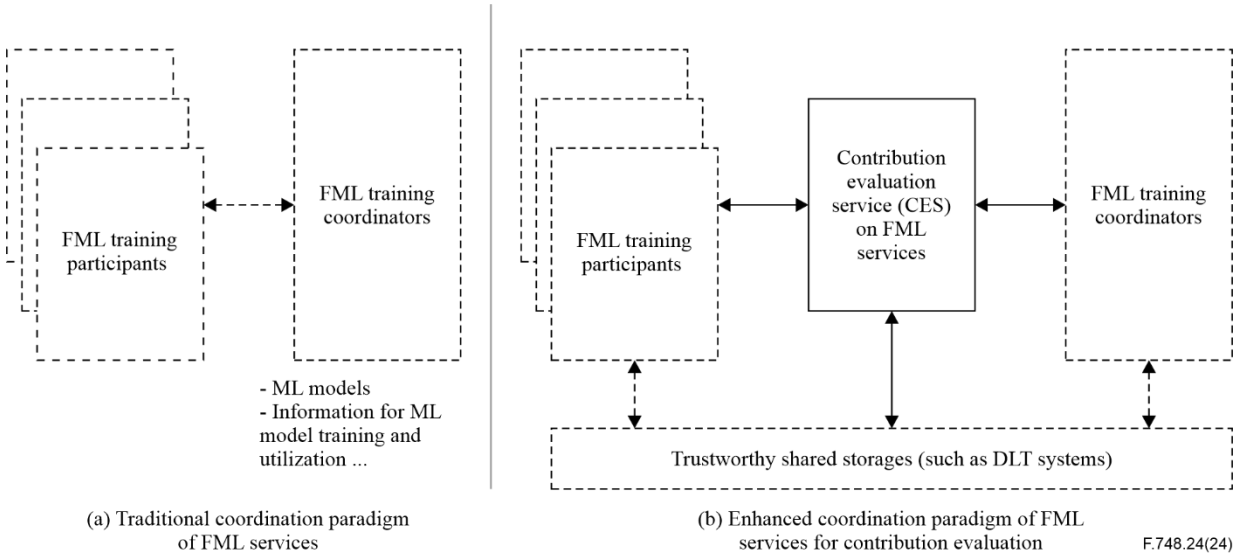

Figure 6-1 – Overview of a trusted contribution evaluation service for FML services

In addition, FML training coordinators can store modules for ML model training and modules for evaluating contributions in DLT systems. FML training participants can store indexes of datasets in DLT systems. Furthermore, FML training coordinators and FML training participants can initiate ML model-training tasks through CES and DLT systems.

7 Characteristics and requirements of a contribution evaluation service for FML services

7.1 Characteristic of contribution evaluation service for FML services

7.1.1 Full-lifecycle data collection and management for FML services

A CES can collect and manage process data for FML services over their full lifecycle, including data concerning, at least:

– creation of ML training tasks;

– management of ML model-training tasks;

– transmission between FML training participants and FML training coordinators;

– ML model training and utilization.

7.1.2 Trustworthy storage for FML services

A CES adopts DLT system(s) as trustworthy storage for exchanged data for ML model-training tasks, and also for algorithms and modules to evaluate contributions. DLT system(s) guarantee(s) the reliability, integrity, consistency, availability and non-tampering of data.

NOTE – A DLT system acts as trustworthy shared storage of CES, but CES is independent of DLT systems. DLT itself lies outside the scope of this Recommendation.

7.1.3 Pluggable modules for contribution degree evaluation

A CES provides pluggable modules to evaluate contribution degree. Pluggable modules are usually transparent and stored in DLT systems. FML training participants and coordinators can use and validate the pluggable modules independently.

NOTE – The model for calculating the contribution degree is jointly formulated and provided by the FML training participants and coordinators, and the CES. Calculation of contribution degree lies outside the scope of this Recommendation.

7.1.4 Independent contribution degree evaluation

An FML service involves multiple participants and allows them to jointly training ML models without sharing raw data directly. A CES provides a decentralized contribution degree evaluation approach to ensure that each participant can calculate their contribution without revealing data.

7.1.5 Consistency in contribution degree calculation

When any participant in and coordinator of FML training uses the same contribution calculation approach provided by the CES to calculate the contribution degree for a FML training task, the result is same.

The results obtained by different contribution calculation approaches are consistent. For example, if the contribution degree of FML training participant A is more than that of B, which is calculated by one approach, the contribution degree is consistent with that obtained by another method.

FML training participants and coordinators are able to evaluate the trustworthiness of the results obtained by the contribution calculation approaches provided by a CES.

7.1.6 Security and personally identifiable information

A CES supports data security and personally identifiable information (PII) protection for data collection (DC) and data storage. A CES exposes the data and capabilities according to its security and PII protection policies.

7.2 Common requirements of a contribution evaluation service for FML services

7.2.1 Requirements for data storage

– A CES is required to support participants in and coordinators of FML training by storing information about FML model-training tasks (such as time, data source, data quantity and data quality) in DLT systems after each round of aggregation of an FML model-training task.

– A CES is required to support participants in and coordinators of FML training by storage of the status of FML model-training tasks (such as model update time, model parameter changes and model result) in DLT systems after each round of aggregation of an FML model-training task.

– A CES is required to support FML training coordinators by storage of operational data of FML model-training tasks in DLT systems after each round of aggregation of an FML model-training task.

– A CES is required to support participants in and coordinators of FML training by retrieval of data from trustworthy shared storages (such as DLT system(s)).

NOTE – DLT systems can be used as trustworthy storage for exchanged data for FML model-training tasks, and also for algorithms and modules to evaluate contributions.

7.2.2 Requirements for collecting data to calculate contribution degree

– A CES is required to support FML training participants and coordinators by collecting data for FML model-training tasks (such as time, data source, data quantity and data quality) from relevant DLT systems to evaluate contribution degree.

– A CES is required to support FML training participants and coordinators by collection of the model update status of FML training tasks (such as model update time, model parameter changes and model result) from relevant DLT systems to evaluate contribution degree.

7.2.3 Requirements for rewarding participants and coordinators

– A CES is recommended to build mechanisms to allow FML training participants and coordinators by obtaining and validating their contribution degree for FML services.

– A CES can optionally incentivize FML training participants by providing feedback on their respective contribution to the overall FML training task.

7.2.4 Requirements for ML model management to calculate contribution degree

– A CES is required to provide an ML model management (MMM) mechanism to ensure ML model security.

– A CES is required to provide pluggable modules for FML training participants and coordinators to evaluate contribution degree.

– A CES is required to provide contribution degree assessment mechanisms to ensure that contribution calculation results are trustworthy.

7.2.5 Requirements for security protection

– A CES is required to provide a security mechanism when up- or downloading data to or from DLT systems.

– A CES is required to provide a PII protection mechanism when up- or downloading data to or from DLT systems.

8 Reference framework of a contribution evaluation service for FML services

A CES consists of six main functional components (FCs), including FML service agents, DC, contribution calculator (CC), model management, DLT agents and task management. Figure 8-1 shows a reference framework of a trusted CES for FML services.

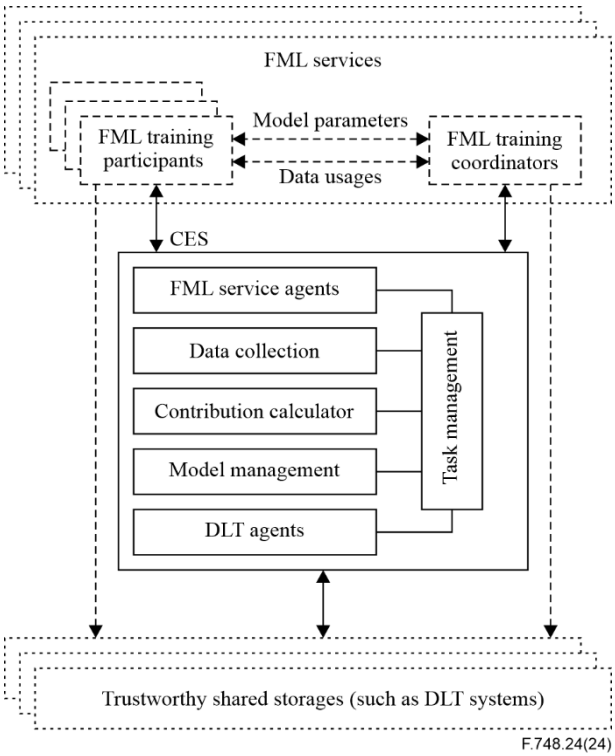

Figure 8-1 – Reference framework of a contribution evaluation service for FML services

8.1 FML service agent

FML service agents interact with external FML services. FML training participants and FML training coordinators connect to FML service agents to exchange information about data usage and model parameters.

FML service agents expose functional interfaces for FML training participants and FML training coordinators to interact with each other.

8.2 Data collection-functional component

A DC-functional component (DC-FC) supports participants in and coordinators of FML training. A DC-FC collects and manages information related to data usage, data exchange, ML model training, model management, etc.

8.3 Contribution calculator-functional component

A CC-functional component (CC-FC) is used to calculate the contribution degree. A CC-FC supports participants in and coordinators of FML training by calculating the contribution degree based on the FML training status, data usage, data quality, data quantity, model-training parameters, etc.

8.4 ML model management-functional component

An MMM-functional component (MMM-FC) provides trustworthy full-lifecycle management of ML model-training tasks. An MMM-FC includes at least:

– initiation or cessation of ML training;

– MMM;

– ML result management;

– management of contribution degree result for FML services.

8.5 DLT agent-functional component

A DLT agent of a CES interacts with DLT systems, which provides capabilities related to trustworthy storage, traceability and their management.

8.6 Task management-functional component

A task management-functional component (TM-FC) provides management mechanism and services policies for FML model-training tasks, including security authentication mechanisms.

9 Common capabilities of a contribution evaluation service for FML services

This clause provides common capabilities and procedures of a trusted CES on FML services, according to the requirements specified in clause 7 and reference framework specified in clause 8.

9.1 Data storage of FML services

See Figure 9-1. FML training coordinators and FML training participants for FML service can store data directly in a DLT system (steps 1 and 4) or store data through a CES (steps 2 and 5). A CES can process data sent by FML services, including checking validity and authority (steps 3 and 6). Data after checking and processing is usually stored in the DLT system (step 7).

FML training participants and FML training coordinators attach identity information when storing data. If information about ab FML training task is stored, its identity is also required. If the relevant data is stored in the DLT system through a CES, the CES attaches its identity-related information to the data stored in the DLT system. Attaching identity is to facilitate further searching, extraction and processing of relevant data.

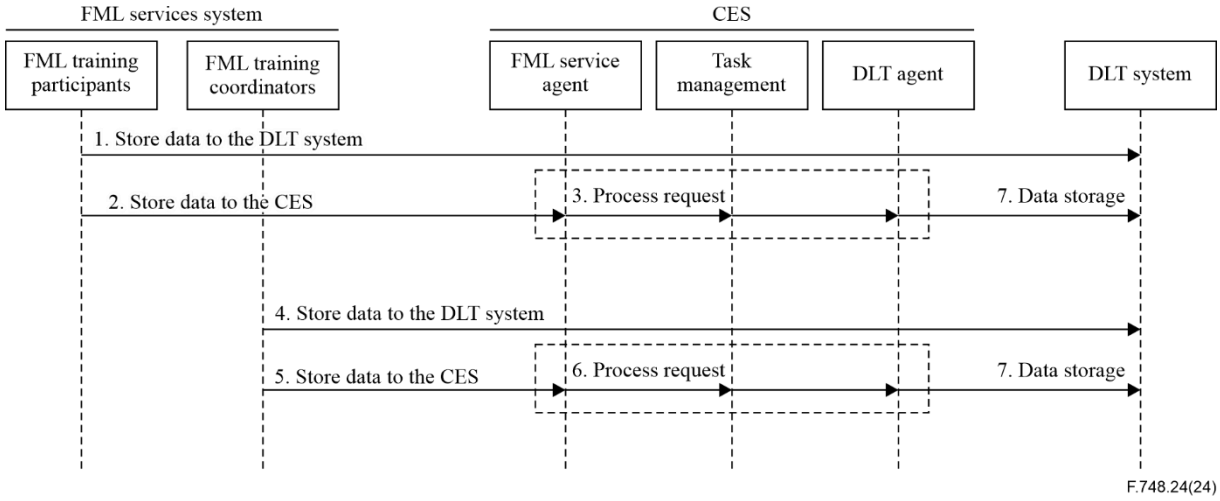

Figure 9-1 – Reference procedures of data storage in FML system

9.2 Identity registration of FML services

FML training coordinators and FML training participants firstly register in a CES before they can organize or participate in FML training tasks. During registration, FML training coordinators and FML training participants need to provide user identity, public key and certificates. FML training coordinators and FML training participants store their private key corresponding to their public key. A CES uses its own private key to sign certificates, store signature information in the corresponding certificates and feeds back to the FML training coordinators and FML training participants. The CES stores registration information about FML training coordinators and FML training participants, and related information can also be stored in the DLT system. See Figure 9-2.

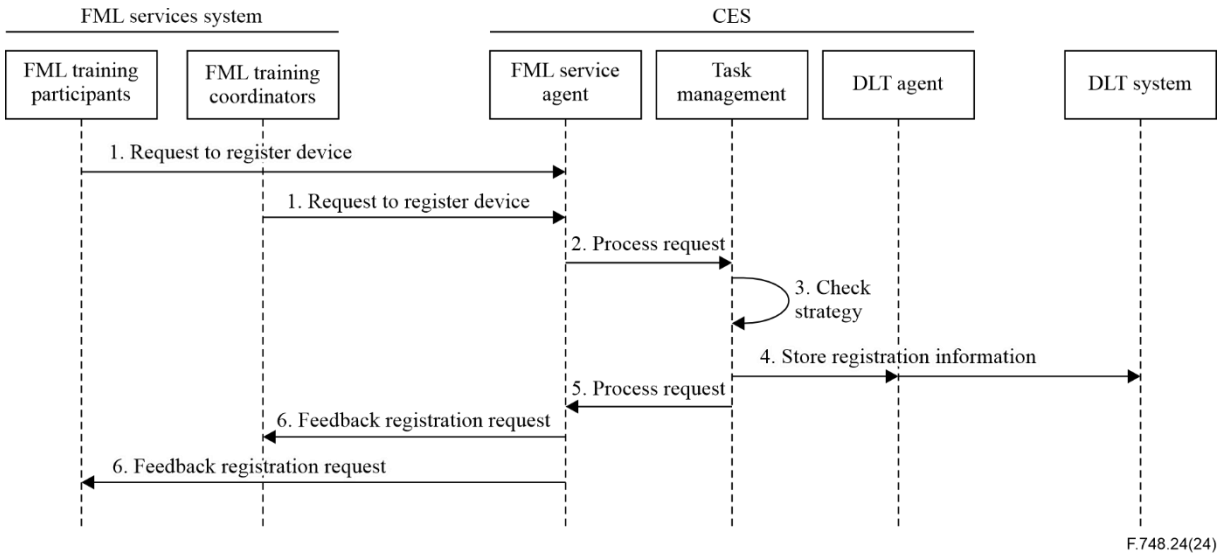

Figure 9-2 – Reference procedures of identity registration in FML system

The relevant steps mainly include the following.

Step 1. One or more FML training coordinator and one, usually more, FML training participant register themselves with a CES.

Step 2. The FML services agent of the CES receives and processes relevant requests, such as conducting permission and other aspects of detection.

Step 3. The TM-FC of the CES detects related request information. If it passes the check, the TM-FC uses the private key of the CES to sign the certificates of the multiple FML training participants and FML training coordinators.

Step 4. If it passes the inspection, the TM-FC of the CES stores relevant data in the DLT system through the DLT agent.

In the process of checking the FML training coordinators and the FML training participants, the CES can obtain the parameter information required for inspection from the DLT platform.

Steps 5 and 6. The CES feeds registration information back to the FML training coordinators and the FML training participants. If the registration is successful, the FML training coordinators and FML training participants can obtain their own certificates signed by the CES, as well as obtaining its certificate and public key. If the registration fails, the FML training coordinators and FML training participants can obtain registration failure information, including its causes.

9.3 FML model-training task registration of FML services

FML model-training tasks are registered by FML training coordinators. Before the registration of the FML training task, the FML training coordinators and the FML training participants (can be multiple) negotiate the FML model training task, including the selection of the FML model, and relevant number and data set information.

When FML model-training task negotiation is completed, whether successful or not, the FML training coordinators and the FML training participants store the relevant information in the DLT system. Related operations can be stored either via a CES or directly in the DLT system.

When the FML model-training task negotiation is successful, FML training coordinators register the negotiated FML training task information in the CES, and obtain the unique identity of FML service.

After successful negotiation and registration of the FML model-training task, FML training coordinators distribute the FML model-training task information, including the identity of the FML model-training task, to FML training participants.

When the FML model-training task is registered successfully, the FML model-training task is executed between the FML training coordinators and the FML training participants. See Figure 9-3.

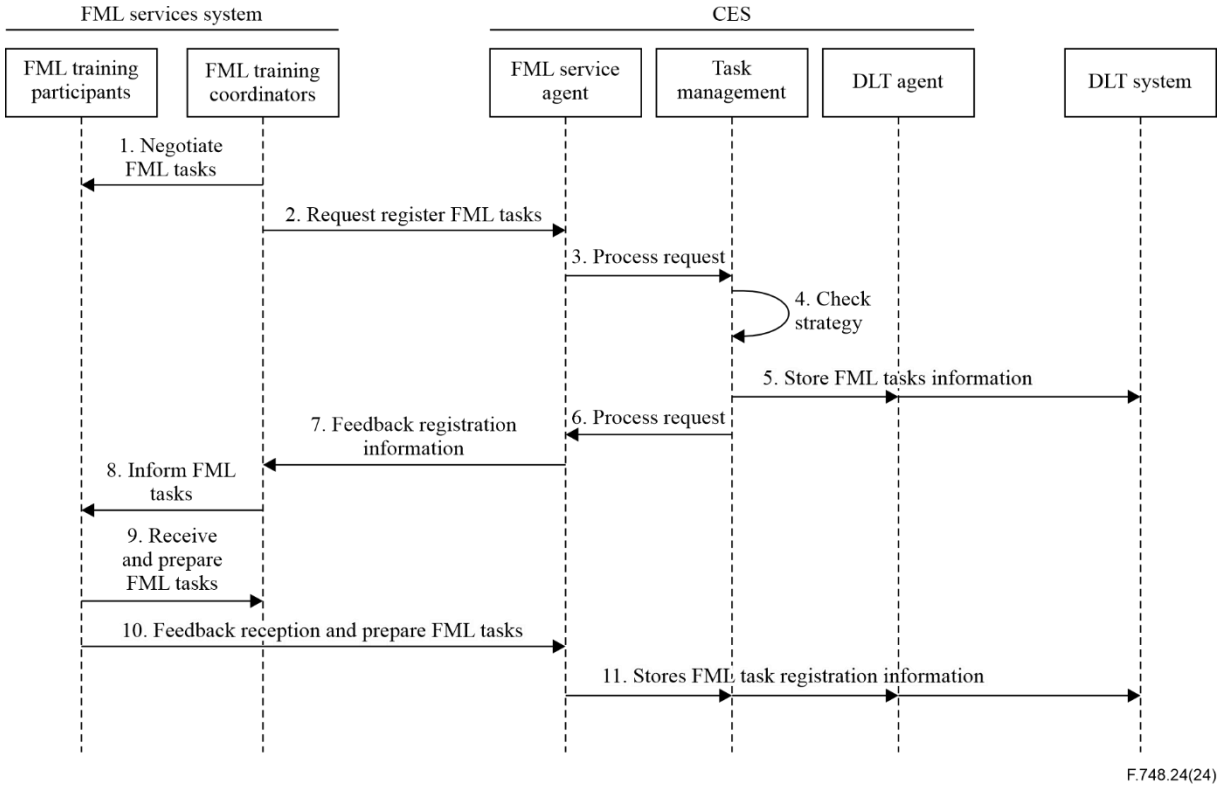

Figure 9-3 – Reference procedures of FML model-training task registration in FML system

In order to protect data privacy, each participant in the FML model-training task encrypts data by using the public key of a CES or the encryption algorithm or key agreed in advance when storing data. Thus, only the private key owner of the CES or the owner of the previously agreed decryption algorithm or key can decrypt and use the relevant data. At the same time, the CES stores information about each participant in the FML model-training task, so that when calculating contributions to the FML model-training task, only participants are allowed to query and calculate the contribution degree through task identity.

In the registration of an FML model-training task, if the registration is successful, the CES generates its unique identity, and stores the relevant identity and the information about the FML model-training task itself or in the DLT system. At the same time, participants in the FML model-training task and the CES negotiate the encryption methods and parameters of the subsequent data. For relevant encryption methods, data can be encrypted directly using the public key of the CES or other pre-set encryption or decryption methods and random encryption or decryption keys can be used.

The relevant steps mainly include the following.

Step 1. The FML training coordinators and the FML training participants negotiate the FML model-training task.

Step 2. If the negotiation is successful, FML training coordinators send the negotiated FML model-training task description information to the CES to register the FML model-training task information.

Steps 3, 4. The TM-FC of the CES checks the service policy that is expected to be specified, for e.g., whether the FML training coordinators and the FML training participants are registered, and whether the FML model-training task description information is complete.

Steps 5, 6, 7. The CES stores processing results; in addition, relevant processing results can be stored in the DLT system. At the same time, registration processing results are fed back to FML training coordinators.

Step 8. FML training coordinators sends feedback to each relevant FML training participant.

Steps 9, 10, 11. Each relevant FML training participant sends information to FML training coordinators about whether it accepts and intends to participate in the FML model-training task, and may also send it to the CES to store the relevant information.

9.4 FML model-training task execution (one-time computation)

After successful negotiation and registration of the FML model-training task, FML training coordinators notify each relevant FML training participant to perform the FML training task. Relevant process and result data can be recorded in the DLT system through the CES. The stored data can be encrypted using either the public key of the CES or a pre-agreed encryption algorithm and key before being written to the DLT system.

FML training participants count information such as the amount of computation spent to execute the FML model-training task and the amount of data accessed to its own data, and upload it to the DLT system through the CES. See Figure 9-4.

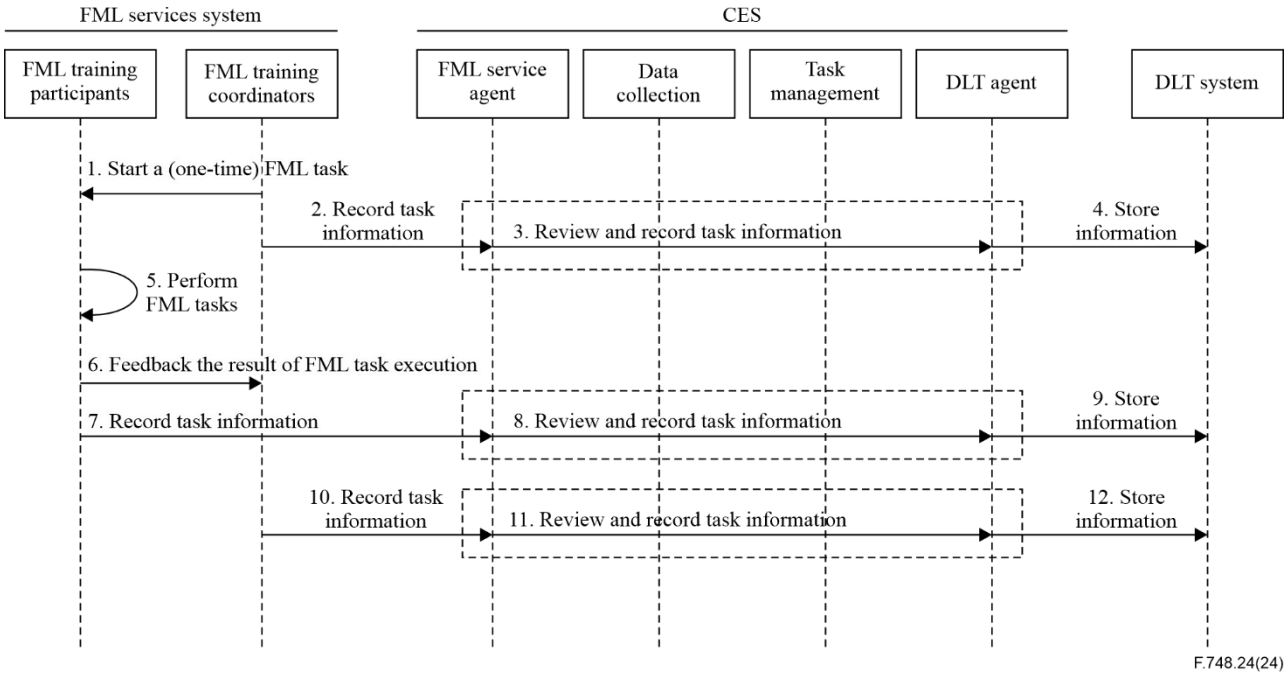

Figure 9-4 – Reference procedures of FML model-training task execution (one-time computation)

The relevant steps mainly include the following.

Step 1. FML training coordinators notify each FML training participant to perform the one-time FML model-training task after negotiation and registration. The notification contains the identity, model-training modules and parameters of the FML model-training task.

The notification content may contain the method and key of encryption for the returned data, which is used by FML training participants to return the data after calculation.

The notification content may include information about other FML training participants, such as task identity and description.

On its dispatch, FML training coordinators can encrypt notification content by using the public key of FML training participants or other encryption and decryption mechanisms negotiated in advance. When FML training participants receive the information, they can decrypt the notification content by using their private key (or encryption and decryption mechanism negotiated in advance).

Other mechanisms can also be used to protect communication security and privacy between coordinators of and participants in FML training.

Steps 2, 3, and 4. FML training coordinators store status information about FML model-training task execution and initiate execution in the DLT system through the CES.

When a FML training coordinator stores information, it can use its private key pair to store information signatures. The signature method can be generation of a digest of key information (or all information) stored in the information, and then encryption of the generated digest using its own private key. Signature information is stored together with the stored information in the DLT system via the CES.

FML training coordinators can simultaneously encrypt their own stored information and its signature information using the public key of the CES. In this way, only the private key of the CES can be owned to view the relevant information, to ensure data security and privacy of FML training coordinators. This encryption process can be handled by FML training coordinators themselves or via the CES. FML training coordinators may also encrypt relevant data using other previously agreed encryption algorithms and keys.

Step 5. Relevant FML training participants receive and analyse the FML model-training task from the FML training coordinators, and then executes the FML model-training task.

The FML model-training task requires prior negotiation.

If the FML model-training task information is encrypted, FML training participants decrypt the FML model-training task information according to the agreed rules.

The relevant FML training participants inspect and certify the FML model-training task. If certified, the FML model-training task is performed.

During the inspection, certification and implementation process, the relevant parties calculate the relevant information recorded by the participants for uploading to storage and contribution evaluation.

Step 6. The relevant FML training participants feed the processing results back to the multiple FML training coordinators. If accepted and executed, feedback FML results; if the command is not accepted or the command fails to be executed, the command sends related instructions.

Steps 7, 8, 9. Relevant FML training participants upload the information related to the inspection, authentication, implementation and feedback operations to the DLT system via the CES.

Similarly to coordinators, relevant FML training participants calculate a digest of the uploaded data information and sign it. At the same time, the uploaded relevant information can be encrypted using the CES public key (or other previously agreed algorithms or keys).

After the completion of the FML in steps 10, 11 and 12, the FML training coordinator writes the execution of the FML service into the DLT system through the CES. These steps are similar to 2, 3 and 4.

9.5 FML model-training task execution (multiple repetitive computation)

The FML model-training task with multiple repetitive calculations refers to the need for FML training participants to perform repetitive calculations, and need to cooperate with other participants in the

calculation process (such as exchange of intermediate parameters, etc.). FML training participants can communicate and cooperate with each other through FML training coordinators.

In the process of multiple repetitive FML model-training tasks, FML training participants perform the calculation multiple times, and during the calculation process, FML training coordinators exchange parameters with other participants, such as intermediate calculation results. At the same time, to successfully execute the FML model-training task, FML training coordinators can also actively send a task evaluation notification to the FML training participants to check and judge the execution effect.

The termination of multiple repeatable FML model-training tasks may be based on pre-set computation termination conditions or the decision of whether and when to terminate can be made by FML training coordinators. In multiple repeatable FML model-training tasks, each FML training participant performs calculations independently, based on its data, as well as parameters transmitted by the FML training coordinators, and each FML training participant cannot directly transfer data to other participants.

In the process of repeated FML model-training tasks, the FML training coordinators and the FML training participants continue to write information that can be used for contribution evaluation to the DLT system via the CES as required. Related write procedures and processing mechanisms are similar to FML model-training task execution (one-time computation task) (see clause 9.4). The difference between the two is that in multiple repetitive FML model-training tasks, the FML training coordinators and the FML training participants need to attach the FML model training task identity clearly when writing information to facilitate the subsequent contribution evaluation calculation. See Figure 9-5.

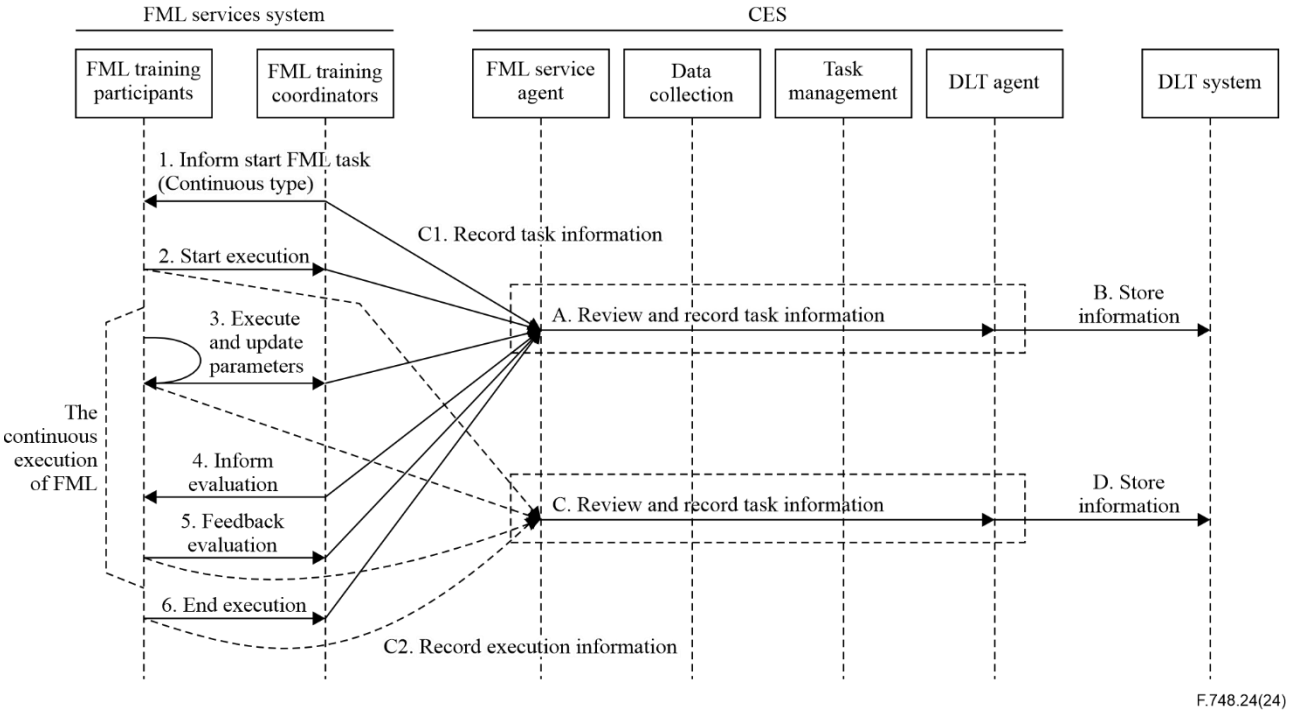

Figure 9-5 – Reference procedures of FML model-training task execution (multiple repetitive computations)

The relevant steps mainly include the following.

Step 1. FML training coordinators notify relevant FML training participants to perform the FML model-training task. This step is similar to step 1 in Figure 9-4.

Step 2. Each FML training participant checks and judges whether to accept the FML model-training task, and informs FML training coordinators whether to accept and execute the FML model-training task.

Steps 3, 4 and 5. If FML training participants accept the FML model-training task, it shall be continuously executed, and during the execution process, the parameters of the execution intermediate process shall be continuously updated to FML training coordinators; meanwhile, the evaluation task sent by FML training coordinators shall be accepted, processed and fed back.

An evaluation task is sent by the FML training collaborative to evaluate the intermediate result performed by FML training participants to facilitate their performance of the computing processes assigned to them.

Step 6. After processing the FML model-training task, FML training participants notify FML training coordinators of the completion and final result of their execution.

Steps A and B. FML training coordinators store execution information of the FML task via the CES. These steps are similar to steps 3 and 4, and steps 11 and 12 in Figure 9-4.

Steps C and D. FML training participants store execution information of the FML model-training task via the CES. These steps are similar to steps 8 and 9 in Figure 9-4.

In the process of repetitive FML model-training task execution, coordinators of and participants in FML training continuously store their own status via the CES, so as to facilitate subsequent contribution evaluation.

9.6 Evaluation of FML model-training task contribution

Any party to the FML model-training task may apply for and seek the contribution of the parties (or agreed parties) to the FML model-training task.

The contribution calculation module refers to the parties involved in the FML model-training task that are used to calculate the contribution of each party in the FML model-training task. Contribution computing modules are usually stored in an executable program (e.g., smart contracts). The contribution calculation modules can be stored in the CES or DLT system.

The contribution calculation is based on relevant data stored in the DLT system. The DLT system ensures: the security and consistency of the data stored by participants in the FML training task; and the privacy protection of the relevant data via the CES. At the same time, the reliability of the FML model-training task contribution is checked by correlation of the calculated values and those in the actual data set.

The FML training coordinators and the FML training participants can negotiate the contribution calculation approach (steps 1 and 2), and store the negotiated contribution calculation approach in the DLT system via the CES (steps 2.1 and 2.2). The parties involved in the FML service system may choose the contribution calculation approach determined in advance and stored in the DLT system. See Figure 9-6.

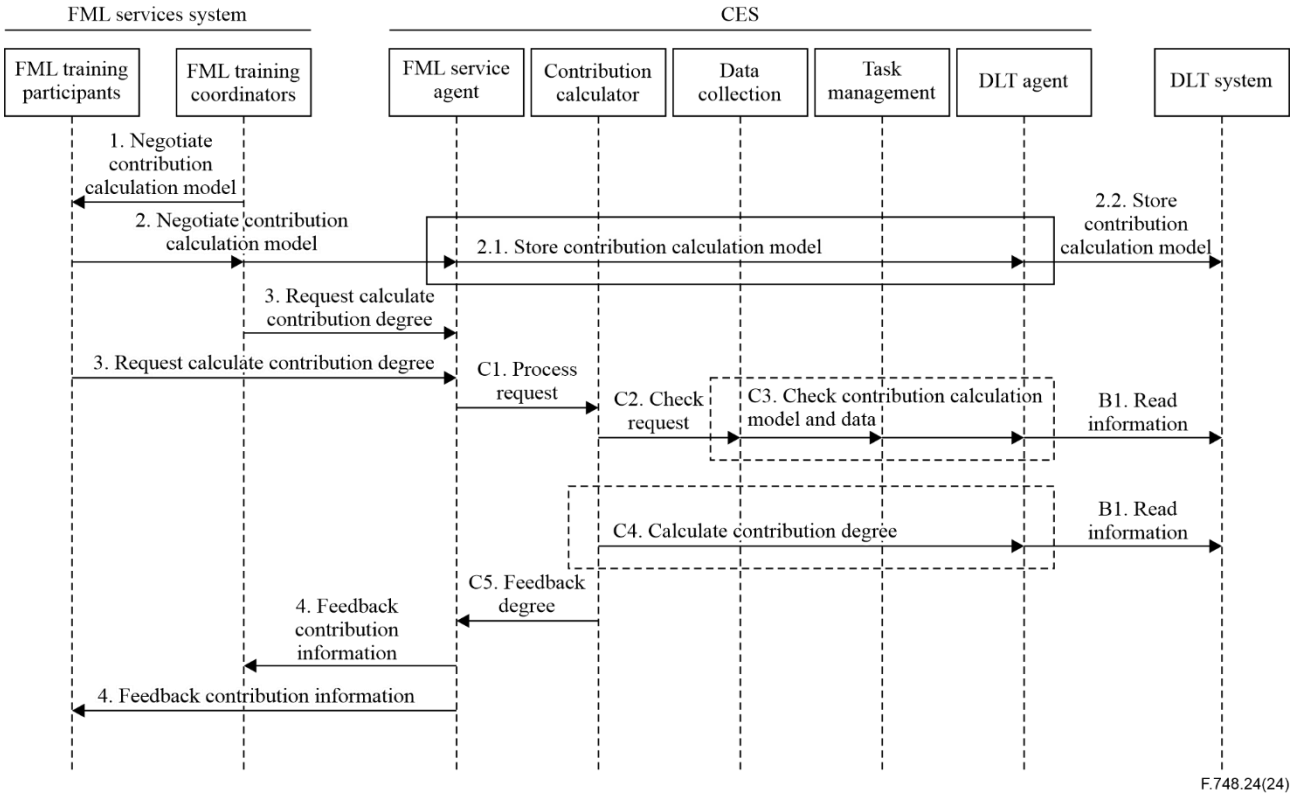

Figure 9-6 – Reference procedures of FML model-training task contribution evaluation

Contribution can be calculated in a variety of ways, e.g., through the effective contribution ratio, including total computation, actual computation, effective computation and data validity.

Data validity is determined by comparing the correlation between the actual calculated data and the data set for the FML model-training task. When the FML model-training task is executed, the data set on which it depends can be agreed. The relevant judgement approach is involved in the previous description.

The following is a simple calculation approach for contribution degree evaluation as an example.

Contribution = Effective contribution/Total effective contribution

Total effective contribution = the sum of the effective contribution of all relevant parties

Effective contribution = volume of calculated data × number of calculations + number of updated and accepted parameters

When calculating contribution, the CES needs to check the relevant identity information of the FML training participants, the FML training coordinators, the task information of the FML training task and the relevant log information. Relevant logs and other information can usually be stored in the DLT system and stored encrypted using the aforementioned encryption method.

10 General functional components of coordinators of and participants in FML training

10.1 FML training coordinator

The main FCs of FML training coordinators include device registration, model management, contribution management, data management, task coordination, log update, task management, participants device synchronization and log synchronization.

– The device registration FC of FML training coordinators is used to deal with the registration operation and related information management of FML training coordinators. The FML

collaborative device registers itself with CES using the device registration FC, and can search and verify the registration information related to the registered FML training participants.

– The model management FC of the FML training coordinators is used to manage the models of FML model-training tasks.

– The contribution management FC of the FML training coordinators is used to negotiate the contribution calculation modules of the FML model-training task and request the contribution calculation of the FML model-training task.

– The data management FC of the FML training coordinators is used to manage the index information of the target computing data set of the FML model-training task. Relevant index information, excluding the original data, contains at least the identifier of the data, a description and classification of the data information, and digest information. The relevant index information needs to be sufficient for the FML training coordinators to measure the FML model-training task and to identify a data item. At the same time, during the execution of FML service, the FML model-training task execution module will use the same algorithm to generate and compare summaries to make statistics and evaluate whether the pre-set data set is used. For a FML training task that is computed once, there is no need to count and evaluate whether to use a pre-set data set when executing a FML model-training task.

– The task coordination FC of the FML training coordinators is mainly used to cooperate with the FML training participants according to the selected FML training task model and related parameters. For FML training tasks with repetitive computation, the task coordinators FC provides continuous services and provides coordinated transmission of relevant intermediate result parameters and related information between FML training participants.

– The log update FC of the FML training coordinators is mainly used to generate log information during the execution of the FML model-training task, including data access, information synchronization, etc., according to the execution of the task cooperation FC.

– The TM-FC of FML training coordinators is mainly used to manage FML model-training tasks and related information.

– The log synchronization FC of the FML training coordinators is mainly used to write the process log of the FML service to CES.

The synchronization of the participants of the FML training coordinators is mainly used to cooperate with each FML training coordinators, including the negotiation of FML training tasks, synchronization of FML model-training results or parameters of the intermediate process.

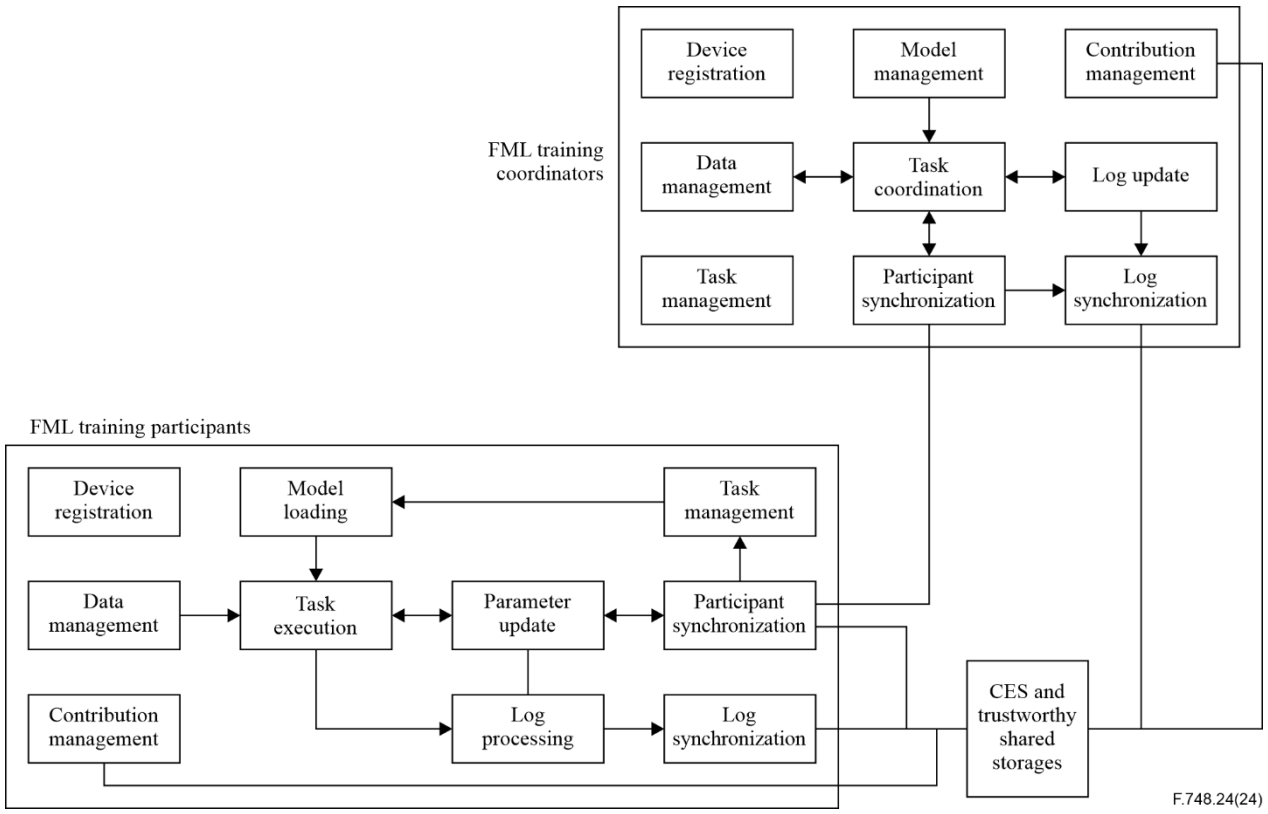

Figure 10-1 – Main functional components of FML training coordinators and FML training participants

10.2 FML training participant

The main FCs of FML training participant mainly include device registration, model loading, task management, data management, task execution, parameter update, participant device synchronization, contribution management, log processing and log synchronization, etc.

– The device registration FC of FML training participants is used to register itself and find the registration information of other participants in and coordinators of FML training.

– The model-loading FC is used to obtain the FML calculation model. The FML training model is a set of executable modules, which can come from FML training participants themselves or from FML training coordinators, etc. FML training participants can perform the FML model-training task by executing computational modules.

– The TM-FC of the FML training participants is used to negotiate and obtain the FML model-training task and the associated computing model code.

– The data management FC of FML training participants is used to provide computational data to the task execution FC when performing the FML task. If the data set for the FML model-training task is agreed upon in advance, the data management FC is responsible for checking and providing the data set.

– The task execution FC of FML training participants is used to execute applicable modules of the loaded FML training model, and relies on the data set provided by the data management FC. The final or intermediate result is synchronized with FML training coordinators through the parameter update FC and the coordinators synchronization FC. At the same time, the logs of intermediate process and data usage used in the processing process are sent to the CES through the log-processing module and log synchronization FC. The task execution FC can review the calculated data set to check whether the previously agreed data set is used, and at the same time generate logs of the relevant results to send to the CES.

– The contribution management FC of FML training participants is used to negotiate the contribution evaluation model with FML training coordinators and to cooperate with CES to calculate the contribution evaluation information of the FML training task.
– The log processing FC and log synchronization FC of FML training participants are used to send the log information to the CES.

The FCs of the CES can be deployed in coordinators of and participants in FML training and perform the functionalities of the CES.

11 Security consideration

FML model-training tasks can be based on the agreed raw data sets of the parties. The raw data sets themselves do not need to be shared, just the index information of the raw data sets (such as data identifier and digest). At the same time, parts of the FML model-training tasks are executed according to the same executable program, so as to ensure the certainty of the calculation. The execution module to train ML models of the FML model-training task can be executed in the secure container of the coordinators of and participants in FML training, and the execution modules can check the raw data set during the execution process, so as to further ensure the reliability of the calculation.

The FCs for task coordination and contribution management of the FML training participants, the FCs for task execution and contribution management of the FML training participants, and the DC-FC and CC-FC of the CES may all run in a secure execution environment. The secure execution environment may be provided by software (e.g., a secure container or secure virtual machine) or a hardware environment (e.g., a secure chip).

The data set information, task executable FC, and log information of FML model-training tasks can be safely stored in the DLT system, which can not only provide security for data and modules, but also protect the privacy of the data, and make multi-party secure computation more traceable and trusted.

FML training participants and coordinators may come from different companies, countries and regions, and the CES should provide mutual authorization and authentication mechanisms to ensure communication security. An FML service involves multiple parties and should provide a security mechanism to ensure data security and reliability for data communication and computation.

Appendix I

Use cases of a contribution evaluation service for FML services

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

In the construction of smart cities, various government departments and enterprises have various kinds of massive data. At the time of publication, some socially important development projects, such as systems for credit information and transportation planning need to be completed jointly with the data of government and enterprises. Considering the confidentiality of governmental and commercial data, the project can only be completed by using FML services to jointly learn between government and enterprises.

For example, in order to build a safe public traffic system, public security departments, traffic management departments and automobile enterprises gather data to train image recognition and traffic prediction models by FML services. Public security departments, traffic management departments and automobile enterprises act as FML training participants, and regulatory departments act as FML training coordinators. A CES manages FML training tasks and acts as a bridge between coordinators of and participants in FML training to exchange training data. In addition, a CES stores the exchanged training data in a DLT system. A CES also manages itself and stores data in DLT systems. DLT systems guarantee the reliability, integrity, consistency, availability and immutability of data. As a result, a CES, supported by DLT system(s), provides a trusted contribution degree evaluation service for each participant. See Figure I.1.

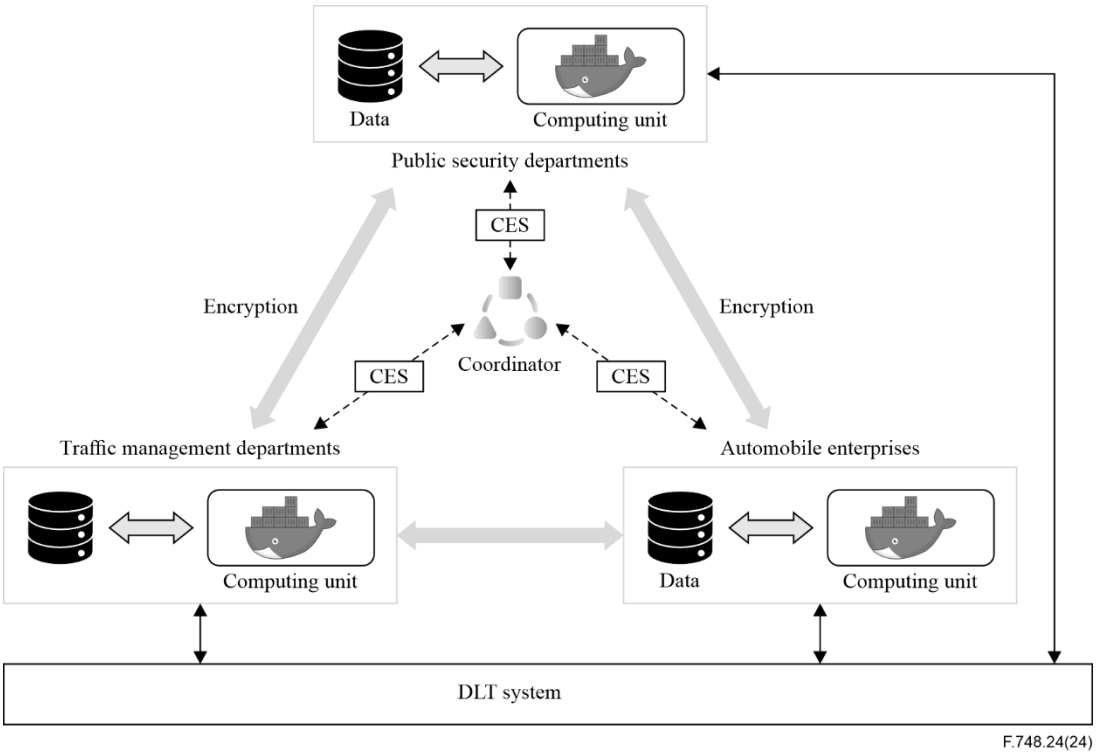

Figure I.1 – Using a CES to build a safe public traffic system

Bibliography

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.

[b-ITU-T Y.3052] Recommendation ITU-T Y.3052 (2017), *Overview of trust provisioning for information and communication technology infrastructures and services.*

[b-IEEE 3652.1] IEEE 3652.1-2020, *IEEE Guide for architectural framework and application of federated machine learning.*

[b-ISO/TR 15801] Technical Report 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