ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T M.3387 (03/2024)

SERIES M: Telecommunication management, including TMN and network maintenance

Telecommunications management network

Management requirements for federated machine learning systems

ITU-T M-SERIES RECOMMENDATIONS

Telecommunication management, including TMN and network maintenance

Introduction and general principles of maintenance and maintenance organization	M.10-M.299
International transmission systems	M.300-M.559
International telephone circuits	M.560-M.759
Common channel signalling systems	M.760-M.799
International telegraph systems and phototelegraph transmission	M.800-M.899
International leased group and supergroup links	M.900-M.999
International leased circuits	M.1000-M.1099
Mobile telecommunication systems and services	M.1100-M.1199
International public telephone network	M.1200-M.1299
International data transmission systems	M.1300-M.1399
Designations and information exchange	M.1400-M.1999
International transport network	M.2000-M.2999
Telecommunications management network	**M.3000-M.3599**
Integrated services digital networks	M.3600-M.3999
Common channel signalling systems	M.4000-M.4999

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

Recommendation ITU-T M.3387

Management requirements for federated machine learning systems

Summary

Recommendation ITU-T M.3387 is applicable to the architecture design, research, and development of federated machine learning models (FMLMs). Data privacy and information security pose significant challenges to the big data and artificial intelligence (AI) community as these communities are increasingly under pressure to adhere to regulatory requirements. Many routine operations in big data systems and applications, such as merging user data from various sources to build a machine learning model is considered to be illegal under the current regulatory frameworks.

The purpose of the federated machine learning (FML) is to provide a viable solution that empowers machine learning applications to utilize data in a distributed manner. In an FML framework, the data owners do not exchange raw data directly and do not allow any party to infer the private information of other parties. In order to facilitate the construction and use of FMLMs and improve the quality of the FML service, Recommendation ITU-T M.3387 specifies the management requirements for the federated machine learning systems (FMLSs), including the functional architecture of FMLSs, as well as the requirements of the basic management domain, model management domain, and data management domain.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T M.3387	2024-03-11	2	11.1002/1000/15786

Keywords

Federated machine learning service, federated machine learning system, management requirement.

---

* 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 M.3387

Management requirements for federated machine learning systems

1 Scope

This Recommendation specifies the management requirements for federated machine learning systems (FMLSs). The following aspects are within the scope of this Recommendation:

– Overall functional architecture of FMLSs.

– Requirements of basic management domain, which supervises system property configuration, node permission configuration, service request management, and so on.

– Requirements of model management domain, which supervises initial model deployment, learning algorithm management, aggregation mechanism management, and so on.

– Requirements of data management domain, which supervises the secure storage, retrieval, transmission of data resources, and so on.

– Use case.

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.

[IEEE 3652.1] IEEE standard 3652.1-2020, *IEEE Guide for Architectural Framework and Application of Federated Machine Learning*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 encryption [b-ITU-T X.1367]: The cryptographic transformation of data to produce ciphertext.

3.1.2 intrinsic incentive mechanism [b-ITU-T Y.4205]: A mechanism offering a reward originating from within, as a result of contributing or participating in an activity. e.g., experiencing self-fulfilment, joy or contributing to a greater cause.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 auditor: A node that is responsible for monitoring the performance of the federated machine learning process, ensuring compliance with regulatory requirements.

3.2.2 coordinator: A node that is responsible for building federated machine learning models across various data owners and delivering the models to the federated machine learning clients.

3.2.3 data owner: A node that owns the data set utilized in the federated machine learning and executes local model training while ensuring data privacy.

3.2.4 data quality: A metric used to evaluate the validity and utility of data sets.

3.2.5 data set: A collection of data points or instances that are used for training, testing, or evaluation purposes. Each data point within a data set represents a sample, including the data identifier, data features (consisting of names and values), or the class label (in the case of supervised learning).

3.2.6 federated machine learning (FML): A machine learning framework that facilitates collaborative construction of machine learning models among multiple distributed training nodes without exposing the private data owned by the data owners.

3.2.7 federated machine learning model (FMLM): The result of the training process of a federated machine learning system. The trained model is used for inference tasks on the new data.

3.2.8 federated machine learning management system (FMLMS): A management system that can manage the node resources and model training services of the federated machine learning systems.

3.2.9 federated machine learning service: An artificial intelligence model training service that uses the federated machine learning method and outputs a globally trained model.

3.2.10 federated machine learning service client (FMLSC): An application entity that initiates the federated machine learning service request and receives trained federated machine learning models.

3.2.11 federated machine learning system (FMLS): A system that involves multiple training nodes which collaboratively build and use machine learning models without disclosing the raw and private data owned by the participants.

3.2.12 raw data: A collection of data sets that are acquired, stored and maintained by the data owners. The raw data contains private information of users and data owners.

3.2.13 training: The process of the federated machine learning, including the local training of raw data and aggregation of intermediate updated parameters to optimize the performance of the federated machine learning models.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AI Artificial Intelligence

AUC Area Under the Curve

CAP Computing Access Point

CNN Convolutional Neural Network

CPU Central Processing Unit

FML Federated Machine Learning

FMLM Federated Machine Learning Model

FMLMS Federated Machine Learning Management System

FMLS Federated Machine Learning System

FMLSC Federated Machine Learning Service Client

GPU Graphics Processing Unit

ID Identification

IoV Internet of Vehicles

MEC	Mobile Edge Computing
MSE	Mean Squared Error

5 Conventions

In this Recommendation:

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

– The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement needs not be present to claim conformance.

– The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview

According to [IEEE 3652.1] "*IEEE Guide for Architectural Framework and Application of Federated Machine Learning*", data privacy and information security pose significant challenges to the big data and artificial intelligence (AI) community as these communities are increasingly under pressure to adhere to regulatory requirements. Many routine operations in big data systems and applications, such as merging user data from various sources to build a machine learning model, are considered to be illegal under current regulatory frameworks. The purpose of federated machine learning (FML) is to provide a viable solution that empowers machine learning applications to utilize data in a distributed manner. In an FML framework, the data owners do not exchange raw data directly and do not allow any party to infer the private information of other parties.

The international standard [IEEE 3652.1] defines the architectural framework for FML to promote and facilitate collaborations among multiple parties. However, different business scenarios have different requirements for model training services. Therefore, the federated machine learning system (FMLS) needs to coordinate different FML training nodes to provide secure and stable FML service by managing system properties, model properties, and data properties.

FMLS is a system that provides FML service for federated machine learning service clients (FMLSCs). To provide safe and efficient FML service, system property configuration, training node property configuration, FML service request management, and other management functions should be defined. These management functions are hosted by the federated machine learning management system (FMLMS).

Based on the working principle of FMLS described by [IEEE 3652.1], this Recommendation specifies the management requirements for FMLSs, including the basic management domain, model management domain, and data management domain.

7 Scenario of federated machine learning system management

The scenario of FMLS management is shown in Figure 1. In an FMLS, the FML training nodes are regarded as having different roles according to their functions in the present FML task, including the coordinator, auditor, and data owner.

The coordinator is responsible for coordinating the FML task within FMLS and outputting the learned federated machine learning model (FMLM). The auditor is responsible for monitoring the entire FML process to ensure that the data is trusted and secure. The data owner is responsible for training and updating models locally. More specific functions of these roles are referred to [IEEE 3652.1].

The interfaces related to FMLS management are shown in Figure 1. There are mainly two interfaces involved:

– **Interface I1** is the interface located between FMLMS and FMLSC, which is used to deliver federated machine learning service requirements from FMLSC and return the trained FMLM to FMLSC.

– **Interface I2** is the interface located between the FMLMS and FMLS, which is used to manage node resources and training tasks.

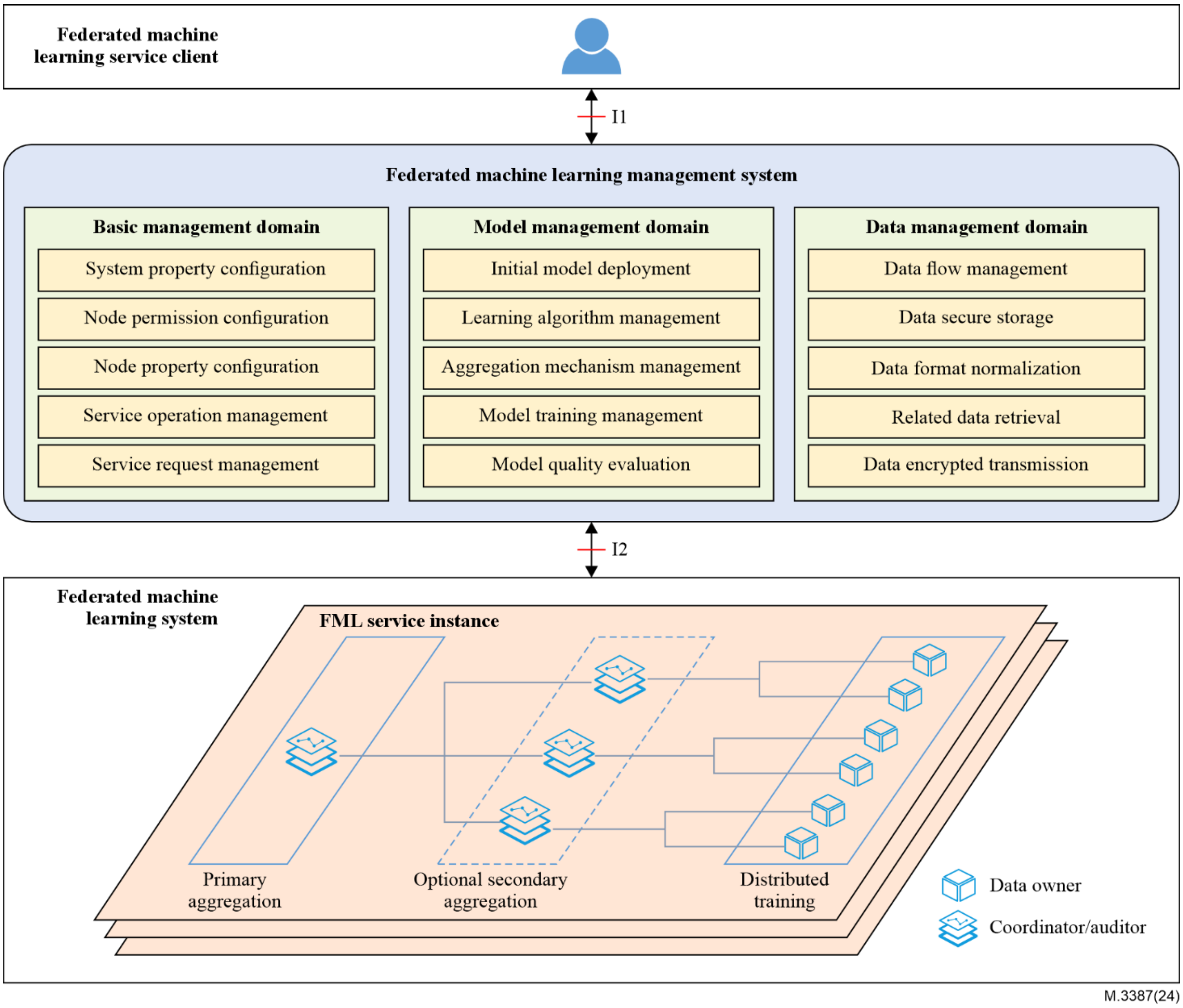

Figure 1 – The scenario of federated machine learning system management

Basic management domain, including system property configuration, node permission configuration, node property configuration, service operation management, and service request management.

– **System property configuration**: initialize and modify the properties of the FMLSs.

– **Node permission configuration**: manage the permissions of the FML training nodes according to the security rules set by FMLMS.

– **Node property configuration**: initialize and modify the properties of the FML training nodes.

– **Service operation management**: manage the FML service topology and evaluate the FML service quality.

– **Service request management**: classify, process, and respond to the FML service requests.

Model management domain, including initial model deployment, learning algorithm management, aggregation mechanism management, model training management, and model quality evaluation.

– **Initial model deployment**: deploy the initial FMLM at the coordinator according to the service requirements.

– **Learning algorithm management**: select proper machine learning algorithms based on the FML service requirements.

– **Aggregation mechanism management**: select or design proper aggregation strategies based on the FML service requirements, resource capacities and data features.

– **Model training management**: control and monitor the model training process, including the transmission and updating of the FMLM.

– **Model quality evaluation**: evaluate the quality of the FMLM based on the evaluation metrics.

Data management domain, including data flow management, data secure storage, data format normalization, related data retrieval, and data encrypted transmission.

– **Data flow management**: control the metadata flow of raw data, and the data flow of the FMLM.

– **Data secure storage**: store the metadata of raw data by using various encryption methods.

– **Data format normalization**: standardize the format of the metadata of raw data, e.g., the table form.

– **Related data retrieval**: retrieve the data related to the FML task as the data sets to undertake FMLM training.

– **Data encrypted transmission**: select the encryption algorithms to encrypt the transmitted data and communication channels.

8 Requirements for basic management domain

8.1 Requirements for system property configuration

The federated machine learning management system (FMLMS) is required to configure the property of the FMLS to support the functional implementation of the FML services, including task properties and resource properties.

8.1.1 Task properties

The FMLMS is required to configure the task properties according to the FML service requests of the FMLSCs.

– Task type: the category of the FML task, e.g., image classification task and text generation task.

– Task priority: the importance of the FML task, e.g., high priority, medium priority and low priority.

8.1.2 Resource properties

The FMLMS is required to configure the resource capacities of an FML task, including computation capacity, communication capacity, and storage capacity.

– Computation capacity: the total computation resource required for the FML tasks, e.g., the number of central processing units (CPUs) and graphics processing unit (GPUs).

– Communication capacity: the total communication resource required for the FML tasks, e.g., transmission power and bandwidth.
– Storage capacity: the total storage resource required for the FML tasks, e.g., free disk and preassigned storage space.

8.2 Requirements for node permission configuration

The FMLMS is required to select proper FML training nodes with sufficient resources according to the present FML task, and then authorize and control the access permission based on the security and reliability of the nodes.

8.3 Requirements for node property configuration

The FMLMS is required to support the property configuration of the FML training nodes, including role properties, computation properties, communication properties, and storage properties.

8.3.1 Role properties

The FMLMS is required to configure the role of the FML training nodes. The role of the FML training nodes includes coordinator, auditor, and data owner. The specific functions of these three roles are referred to [IEEE 3652.1].

8.3.2 Computation properties

The FMLMS is required to support the FML training nodes in configuring their computation-related attributes, e.g., the number of CPUs and GPUs.

8.3.3 Communication properties

The FMLMS is required to support the FML training nodes in configuring their communication-related attributes, e.g., transmission power and bandwidth.

8.3.4 Storage properties

The FMLMS is required to support the FML training nodes in configuring their storage-related attributes, e.g., free disk and preassigned storage space.

8.4 Requirements for service operation management

The FMLMS is required to manage the operation quality of the FML service, including service topology management and service quality evaluation.

8.4.1 Service topology management

The FMLMS is required to manage the topology of the FML service, mainly including service topology generation and service topology reconstruction.

– Service topology generation: generate the FML service topology for the present FML training task, including the roles and connection relationships between the FML training nodes, and send the topology to all the FML training nodes.
– Service topology reconstruction: reconstruct the topology of the FML service in case of a service node failure, resource exhaustion, and so on.

8.4.2 Service quality evaluation

The FMLMS is recommended to evaluate the quality of the FML service, including network operation quality evaluation and service incentive evaluation.

– Network operation quality evaluation: evaluate the performance of the federated machine learning system (FMLS) such as resource consumption and time delay.

– Service incentive evaluation: evaluate FML training nodes' comprehensive contribution to the FML service and set up an intrinsic incentive mechanism according to the contribution to motivate each FML training node to participate in the FML service. The comprehensive contributions include resource consumption, the contribution to model quality improvement, and so on.

8.5 Requirements for service request management

The FMLMS is required to classify and assign service requests when several service requests coexist.

– Service classification: classify service requests according to importance, priority, and delay requirements, and so on.

– Service assignment: response to service requests with scheduling methods, such as priority-based scheduling.

9 Requirements for model management domain

9.1 Requirements for initial model deployment

The FMLMS is required to support FMLM delivery and training initiation according to the FML service requests of FMLSCs.

9.2 Requirements for learning algorithm management

The FMLMS is required to select machine learning algorithms and configure the relevant parameters according to the FML service requirements.

– Algorithm selection: select proper machine learning algorithms, such as neural networks and decision tree.

– Parameter configuration: configure the parameters and hyper-parameters of the machine learning algorithm, such as learning rate, batch size, and regularization coefficient.

9.3 Requirements for aggregation mechanism management

The FMLMS is required to select an aggregation mechanism and configure the relevant parameters according to the FML service requirements, resource capacities, and data features.

– Mechanism selection: select or design a proper aggregation mechanism (e.g., synchronous, asynchronous, semi-synchronous).

– Parameter configuration: configure the parameters of the aggregation mechanism (e.g., number of aggregation rounds, number of clusters, weights in model aggregation).

9.4 Requirements for model training management

The FMLS is required to support the data owners in performing the local training of the FMLM and uploading the learned model to the coordinator.

The FMLS is required to support the coordinator in managing the training process of the FMLM, including broadcasting, aggregating and updating.

The FMLS is required to support the auditor in monitoring the training process of the FMLM based on the regulatory rules, e.g., detecting whether the FML training node is reliable, and measuring the contribution of the FML training nodes.

9.5 Requirements for model quality evaluation

The FMLMS is required to evaluate the quality of the FMLM according to the model performance metrics.

NOTE – Model performance metrics include precision, recall, area under the curve (AUC) for classification models and mean squared error (MSE) for regression models [b-ITU-T Y.3179].

The FMLMS is recommended to adjust the training process through model evaluation to enhance the performance of the model.

10 Requirements for data management domain

10.1 Requirements for data flow management

The FMLS is required to support the generation, storage, transmission and update of the metadata of raw data.

NOTE – The metadata of raw data (e.g., data identification (ID), data characteristic) can optionally be exchanged among data owners during the FML process.

The FMLS is required to support the transmission, aggregation, and updating of the FMLM data.

The FMLS is required to support the security management of the model data to prevent personal privacy from exposure to external and malicious nodes during the FML process.

10.2 Requirements for data secure storage

The FMLMS is required to support secure storage of the metadata of raw data and model data.

10.3 Requirements for data format normalization

The FMLMS is required to collect metadata features of raw data and provide a unified standard database format.

NOTE – Refer to [IEEE 3652.1], the raw data for the FML is typically stored in a standard database format, where each row represents a data sample, and each column represents a feature or label of that sample. A set of feature attributes is usually represented as the eigenvectors (X_1, X_2, ..., X_n). In a supervised learning, the complete training data set consists of features represented by X and labels represented by Y.

10.4 Requirements for related data retrieval

The FMLS is required to support the data owners in retrieving the model-training-related raw data as the data sets. In an FMLS, multiple data sets overlap on sample IDs and feature attributes. According to the overlap degree of sample ID or features, it is divided into the following three cases:

– Horizontal FML: build a model where the data sets have significant overlaps on the feature space but not the ID space. The coordinator is responsible for performing the feature alignment between data owners.

– Vertical FML: build a model where the data sets have significant overlaps on the sample space but not the feature space. The coordinator is responsible for performing the sample alignment between data owners.

– Federated transfer learning: build a model where the data sets have no significant overlap on either the sample space or the feature space. The coordinator is responsible for exploiting the reusable knowledge across the different feature domains.

10.5 Requirements for data encrypted transmission

The FMLS is required to support data privacy protection technologies, such as secure multi-party computing, homomorphic encryption, and differential privacy, ensuring that other FML training nodes cannot infer the raw data information from the model data.

The FMLS is recommended to support channel encryption technologies to maintain a safe environment during the data transmission processes.

Appendix I

A use case example of using FMLMS to manage FMLM training for road anomaly detection services in the Internet of vehicles

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

This appendix presents a typical application and service example for using the federated machine learning management system (FMLMS) to manage the federated machine learning system (FMLS) in the Internet of vehicles (IoV). It also describes the functions of the FMLMS for the FML service, which this Recommendation covers.

I.1 Introduction

The emerging applications based on the intelligent devices such as smart vehicles have stringent requirements for latency and privacy. This renders cloud computing unsuitable for these scenarios and gives rise to FML based on mobile edge computing (MEC). MEC-based FML trains the machine learning models in a distributed manner on mobile devices with limited computing, storage, energy, and bandwidth resources, retaining raw data locally. Model parameters are delivered to closer computing access points (CAPs) for aggregation. In the IoV, sharing data between vehicles for collaborative analysis improves driving experience and service quality. Thus, designing an MEC-assisted FML collaborative computing architecture contributes to the road anomaly detection services while safeguarding data privacy.

I.2 Cloud-edge-terminal collaborative FML architecture

In the IoV, an FMLS utilizes the FML to learn a global FMLM, which is applied to road anomaly detection services. The components of the FMLS include data owners deployed on smart vehicles, coordinators deployed on CAPs, and an FML agent server (represented as AS in Figure I.1) deployed on the cloud server (represented as CS in Figure I.1). The FMLMS is deployed in the cloud and manages the FML training process. MEC technologies are applied to ensure the quality of the FML service by task scheduling and model regional aggregation. The FML training scenario under cloud-edge-terminal architecture is depicted in Figure I.1.

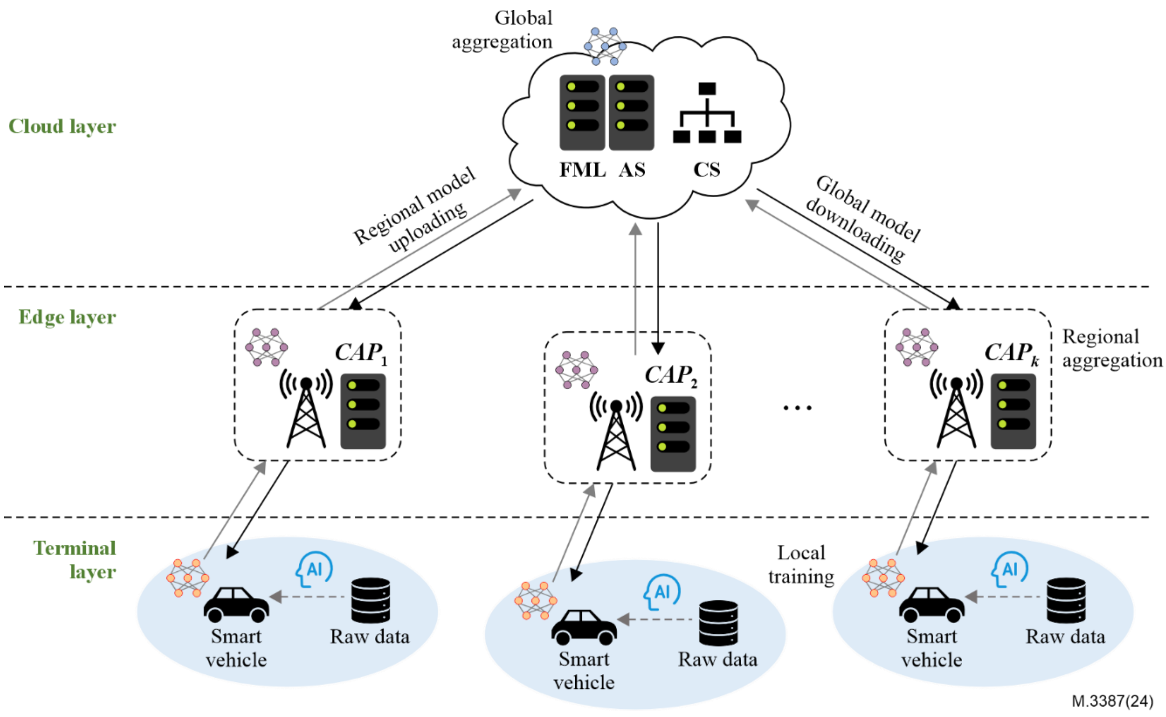

Figure I.1 – Scenario of cloud-edge-terminal collaborative FML in the IoV

As illustrated in Figure I.1, the responsibilities of each layer for the FML training nodes are as follows:

– Terminal layer: Data owners, which are smart vehicles, utilize locally generated data to train a local FMLM and transmit the model parameters to CAPs for regional aggregation (secondary aggregation).

– Edge layer: CAPs, typically the roadside units in vehicular scenarios are individually responsible for collecting local model parameters from data owners within a specific region. They then update regional FMLMs through regional aggregation (secondary aggregation) and send the updated model parameters to the agent server. Additionally, CAPs collect metadata of raw data and device status information, and then send them to the federated machine learning management system (FMLMS).

– Cloud layer: In the cloud, an FMLMS is deployed to manage the FML working process. Simultaneously, the agent server aggregates all the regional model parameters to learn a global FMLM through global aggregation (primary aggregation). Moreover, the FMLMS evaluates the operational quality of the FMLS.

I.3 The management process of FMLS in road anomaly detection model training

In cloud-edge-terminal collaborative FML scenarios, an FMLMS is deployed in the cloud to manage the network resources and the quality of the FML service, ensuring the effectiveness, sustainability, and security of FML service in the IoV. The following example illustrates training a road anomaly detection model for smart vehicles.

Step 1: All potential data owners (i.e., smart vehicles) access the FML network. The federated machine learning service client (FMLSC) requests a road anomaly detection model training service, namely training a road anomaly detection model, from the FMLMS via interface 1.

Step 2: The FMLMS configures the task attributes according to the FML service request, identifying it as an image recognition task and allocating the priority. Based on the network resource situation, the FMLMS selects an incentive strategy to encourage more data owners to join the road anomaly detection model training task.

Using the generated incentive strategy, the FMLMS determines the FML training nodes for the present FML task. Then, the FMLMS allocates the roles of all the FML training nodes. Then, the FMLMS determines the corresponding resource properties for all the FML training nodes, including role, computation, communication and storage properties.

Based on the roles of the FML training nodes, the FMLMS generates an FML service topology, including link relationships between training nodes and the relevant attribute configurations.

Then, the FMLMS determines the learning algorithm and aggregation mechanism for the road anomaly detection task, e.g., convolutional neural network (CNN) and asynchronous aggregation algorithm.

Step 3: FMLMS sends the initial CNN model, system property, node permission, node property, service topology, learning algorithm, and aggregation mechanism to the FMLS via interface 2. Further, FMLMS sends parameters related to privacy algorithms and channel encryption algorithms to the FMLS via interface 2, achieving model data encryption and channel encryption to ensure the privacy and security of the FMLM.

Step 4: FMLS deploys the initial CNN model to all the FML training nodes and requires data owners to preprocess their owned raw data in a standardized format. Then, all the data owners retrieve the relevant image data according to the service request to train the local FMLM.

Step 5: Data owners upload the trained local model to a nearby CAP. Then, CAPs generate regional models based on the collected local model data and then send the regional models to the agent server for global aggregation.

Step 6: FMLMS monitors the operational performance of the FMLS and the quality of the FMLMs. FMLMS can adjust the service topology according to the operational performance and determine whether to terminate the training task based on the quality of the global FMLM. When the model's accuracy meets the service requirements, the FMLMS sends the globally trained FMLM to the FMLSC via interface 1. If the model accuracy does not meet the service requirements, the training task continues.

Bibliography

[b-ITU-T X.1367] Recommendation ITU-T X.1367 (2020), *Standard format for Internet of things error logs for security incident operations*.

[b-ITU-T Y.3179] Recommendation ITU-T Y.3179 (2021), *Architectural framework for machine learning model serving in future networks including IMT-2020*.

[b-ITU-T Y.4205] Recommendation ITU-T Y.4205 (2019), *Requirements and reference model of IoT-related crowdsourced systems*.

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