ITUPublications
Recommandations

Union internationale des télécommunications
Secteur de la normalisation

Recommandation

UIT-T M.3387 (03/2024)

SÉRIE M: Gestion des télécommunications y compris le RGT et maintenance des réseaux

Réseau de gestion des télécommunications

Exigences de gestion applicables aux systèmes d'apprentissage automatique fédéré

RECOMMANDATIONS UIT-T DE LA SÉRIE M

Gestion des télécommunications y compris le RGT et maintenance des réseaux

Introduction et principes généraux de maintenance et organisation de la maintenance	M.10-M.299
Systèmes de transmission internationaux	M.300-M.559
Circuits téléphoniques internationaux	M.560-M.759
Systèmes de signalisation à canal sémaphore	M.760-M.799
Systèmes internationaux de télégraphie et de phototélégraphie	M.800-M.899
Liaisons internationales louées par groupes primaires et secondaires	M.900-M.999
Circuits internationaux loués	M.1000-M.1099
Systèmes et services de télécommunication mobile	M.1100-M.1199
Réseau téléphonique public international	M.1200-M.1299
Systèmes internationaux de transmission de données	M.1300-M.1399
Appellations et échange d'informations	M.1400-M.1999
Réseau de transport international	M.2000-M.2999
Réseau de gestion des télécommunications	**M.3000-M.3599**
Réseaux numériques à intégration de services	M.3600-M.3999
Systèmes de signalisation par canal sémaphore	M.4000-M.4999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T M.3387

Exigences de gestion applicables aux systèmes d'apprentissage automatique fédéré

Résumé

La Recommandation UIT-T M.3387 est applicable à la conception architecturale, à la recherche et à la mise au point des modèles d'apprentissage automatique fédéré (FMLM). La confidentialité des données et la sécurité de l'information posent des défis majeurs aux communautés des mégadonnées et de l'intelligence artificielle (IA), dans la mesure où celles-ci sont soumises à une pression croissante pour se conformer aux exigences réglementaires. De nombreuses opérations courantes dans les systèmes et applications de mégadonnées, comme la fusion de données d'utilisateur issues de plusieurs sources en vue de créer un modèle d'apprentissage automatique, sont considérées comme illégales au regard des cadres réglementaires en vigueur.

L'apprentissage automatique fédéré (FML) vise à proposer une solution viable permettant aux applications d'apprentissage automatique d'utiliser les données de manière répartie. Dans un cadre d'apprentissage FML, les propriétaires de données n'échangent pas de données brutes directement et ne permettent à aucune partie d'obtenir par déduction des informations privées d'autres parties. Afin de faciliter la mise au point et l'utilisation de FMLM et d'améliorer la qualité de service de l'apprentissage FML, la Recommandation UIT-T M.3387 définit les exigences de gestion applicables aux systèmes d'apprentissage automatique fédéré (FMLS), y compris l'architecture fonctionnelle de ces systèmes, ainsi que les exigences relatives aux domaines de la gestion fondamentale, de la gestion des modèles et de la gestion des données.

Historique*

Version	Recommandation	Approbation	Commission d'études	ID unique
1.0	UIT-T M.3387	11-03-2024	2	11.1002/1000/15786

Mots clés

Système d'apprentissage automatique fédéré, exigence de gestion, service d'apprentissage automatique fédéré.

* Pour accéder à la Recommandation, reporter cet URL https://handle.itu.int/ dans votre navigateur web, suivi de l'identifiant unique.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T M.3387

Exigences de gestion applicables aux systèmes d'apprentissage automatique fédéré

1 Domaine d'application

La présente Recommandation définit les exigences de gestion applicables aux systèmes d'apprentissage automatique fédéré (FMLS). Les éléments suivants relèvent du domaine d'application de la présente Recommandation:

– architecture fonctionnelle globale des systèmes FMLS;

– exigences du domaine de la gestion fondamentale, qui encadre notamment la configuration de la propriété des systèmes, la configuration des autorisations des nœuds et la gestion des demandes de services;

– exigences du domaine de la gestion des modèles, qui encadre notamment le déploiement du modèle initial, la gestion de l'algorithme d'apprentissage et la gestion du mécanisme d'agrégation;

– exigences du domaine de la gestion des données, qui encadre notamment la sécurité du stockage, de l'extraction et de la transmission des ressources de données;

– cas d'utilisation.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations ou autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références indiquées ci-après. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[IEEE 3652.1] Norme 3652.1-2020 de l'IEEE, *Guide de l'IEEE pour le cadre architectural et l'application de l'apprentissage automatique fédéré*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 chiffrement [b-UIT-T X.1367]: transformation cryptographique de données produisant un cryptogramme.

3.1.2 mécanisme d'incitation intrinsèque [b-UIT-T Y.4205]: mécanisme offrant une récompense trouvant son origine dans la participation ou la contribution à une activité; par exemple, éprouver un sentiment d'épanouissement ou de joie ou contribuer à une cause plus importante.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 auditeur: utilisateur chargé de contrôler l'exactitude et la qualité de fonctionnement d'un processus d'apprentissage automatique fédéré pour vérifier que le processus est conforme aux exigences réglementaires.

3.2.2 coordonnateur: utilisateur créant des modèles d'apprentissage automatique fédéré à partir de différents propriétaires de données et fournissant des modèles d'apprentissage automatique fédéré aux utilisateurs de modèles.

3.2.3 propriétaire de données: utilisateur revendiquant la propriété d'un ensemble de données utilisé dans l'apprentissage automatique fédéré.

3.2.4 qualité des données: indicateur de l'utilité et de l'efficacité de l'ensemble de données.

3.2.5 ensemble de données: ensemble d'éléments de données composés de caractéristiques de données (elles-mêmes composées de noms et de valeurs de caractéristiques), d'étiquettes de données (pour l'apprentissage (semi-)supervisé) et des identificateurs des éléments de données.

3.2.6 apprentissage automatique fédéré (FML)**: cadre ou système permettant à plusieurs participants de créer et d'utiliser de manière collaborative des modèles d'apprentissage automatique, sans divulguer les données brutes et privées détenues par les participants, tout en assurant un bon niveau de qualité de fonctionnement.

3.2.7 modèle d'apprentissage automatique fédéré (FMLM): aboutissement du processus d'entraînement de modèle d'un système d'apprentissage automatique fédéré.

3.2.8 système de gestion d'apprentissage automatique fédéré (FMLMS): système de gestion pouvant gérer les ressources de nœuds et les services d'entraînement de modèle des systèmes d'apprentissage automatique fédéré.

3.2.9 service d'apprentissage automatique fédéré: service d'entraînement de modèle d'intelligence artificielle utilisant la méthode de l'apprentissage automatique fédéré et produisant un modèle formé au niveau mondial.

3.2.10 client de service d'apprentissage automatique fédéré (FMLSC): entité d'application à l'initiative de la demande de service d'apprentissage automatique fédéré et recevant des modèles d'apprentissage automatique fédéré formés.

3.2.11 système d'apprentissage automatique fédéré (FMLS): système composé de multiples nœuds d'entraînement créant et utilisant de manière collaborative des modèles d'apprentissage automatique sans divulguer les données brutes et privées détenues par les participants.

3.2.12 données brutes: ensembles de données recueillies et gérées par des propriétaires de données. Un ensemble de données contient des informations privées relatives à l'utilisateur et au propriétaire de données et a besoin d'être protégé. Les données brutes sont également désignées comme des données privées pour insister sur la nécessité de protéger la confidentialité.

3.2.13 entraînement: processus d'apprentissage automatique fédéré dans lequel les données brutes restent confidentielles et sont exploitées de façon à optimiser la qualité de fonctionnement d'un modèle d'apprentissage automatique fédéré pour certaines tâches d'apprentissage automatique.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AUC aire sous la courbe (*area under the curve*)

CAP point d'accès informatique (*computing access point*)

CNN réseau neuronal convolutif (*convolutional neural network*)

CPU unité centrale de traitement (*central processing unit*)

FML apprentissage automatique fédéré (*federated machine learning*)

FMLM modèle d'apprentissage automatique fédéré (*federated machine learning model*)

FMLMS système de gestion de l'apprentissage automatique fédéré (*federated machine learning management system*)

FMLS système d'apprentissage automatique fédéré (*federated machine learning system*)

FMLSC client de service d'apprentissage automatique fédéré (*federated machine learning service client*)

GPU unité de traitement graphique (*graphics processing unit*)

IA intelligence artificielle (*artificial intelligence*)

ID identification (*identification*)

IoV Internet des véhicules (*Internet of vehicles*)

MEC informatique en périphérie de réseau mobile (*mobile edge computing*)

MSE erreur quadratique moyenne (*mean squared error*)

5 Conventions

Dans la présente Recommandation:

– L'expression "**il est exigé**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

– L'expression "**il est recommandé**" indique une exigence qui est recommandée, mais qui n'est pas absolument nécessaire. Cette disposition n'est donc pas indispensable pour déclarer la conformité.

– L'expression "**peut, à titre d'option**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité.

6 Vue d'ensemble

Conformément à la norme [IEEE 3652.1], intitulée *Guide de l'IEEE pour le cadre architectural et l'application de l'apprentissage automatique fédéré*, la confidentialité des données et la sécurité de l'information posent des défis majeurs aux communautés des mégadonnées et de l'intelligence artificielle (IA), en ce sens que celles-ci sont soumises à des pressions croissantes pour se conformer aux exigences réglementaires. De nombreuses opérations courantes dans les systèmes et applications des mégadonnées, comme la fusion de données d'utilisateur issues de sources diverses visant à créer un modèle d'apprentissage automatique, sont considérées comme illégales en vertu des cadres réglementaires en vigueur. L'apprentissage automatique fédéré (FML) a pour objet de proposer une solution viable permettant aux applications d'apprentissage automatique d'utiliser les données de manière répartie. Dans un cadre relatif à l'apprentissage FML, les propriétaires de données n'échangent pas de données brutes directement et n'autorisent aucune partie à déduire les informations privées d'autres parties.

La norme internationale [IEEE 3652.1] définit le cadre architectural pour l'apprentissage FML visant à encourager et faciliter la collaboration entre plusieurs parties. Cependant, les exigences applicables aux services d'entraînement de modèles varient entre les différents scénarios d'activité. Par

conséquent, le système d'apprentissage automatique fédéré (FMLS) a besoin de coordonner différents nœuds d'entraînement de l'apprentissage FML pour fournir un service d'apprentissage FML sûr et stable en gérant les propriétés du système, du modèle et des données.

Le système FMLS est un système fournissant un service d'apprentissage FML pour les clients du service d'apprentissage automatique fédéré (FMLSC). Pour fournir un service d'apprentissage FML sûr et efficace, il convient de définir la configuration de la propriété du système, la configuration de la propriété des nœuds d'entraînement, la gestion de la demande de service d'apprentissage FML et d'autres fonctions de gestion. Ces fonctions de gestion sont hébergées par le système de gestion de l'apprentissage automatique fédéré (FMLMS).

La présente Recommandation, fondée sur le principe du système FMLS décrit dans la norme [IEEE 3652.1], définit les exigences de gestion applicables aux systèmes FMLS, y compris aux domaines de la gestion fondamentale, de la gestion des modèles et de la gestion des données.

7 Scénario de gestion du système d'apprentissage automatique fédéré

Le scénario de gestion du système FMLS est présenté dans la Figure 1. Dans un système FMLS, on peut considérer que les nœuds d'entraînement de l'apprentissage FML jouent des rôles différents selon leurs fonctions dans le cadre de la tâche d'apprentissage FML en cours, notamment les rôles de coordonnateur, de vérificateur et de propriétaire de données.

Le coordonnateur est chargé de coordonner la tâche d'apprentissage FML dans le système FMLS et de produire le modèle d'apprentissage automatique fédéré (FMLM) formé. Le vérificateur est chargé d'assurer la surveillance du processus d'apprentissage FML tout entier, afin de veiller à ce que les données soient fiables et sécurisées. Le propriétaire de données est chargé de former et de mettre à jour les modèles localement. On trouvera dans la norme [IEEE 3652.1] des fonctions plus spécifiques de ces rôles.

Les interfaces liées à la gestion du système FMLS sont présentées dans la Figure 1. En général, deux interfaces sont concernées, à savoir:

– L'**interface I1**, située entre le système de gestion FMLMS et le client FMLSC, qui sert à diffuser des exigences relatives au service d'apprentissage automatique fédéré du client FMLSC et à retourner le modèle FMLM formé au client FMLSC.
– L'**interface I2**, située entre le système de gestion FMLMS et le système FMLS, qui sert à gérer les ressources de nœuds et les tâches d'entraînement.

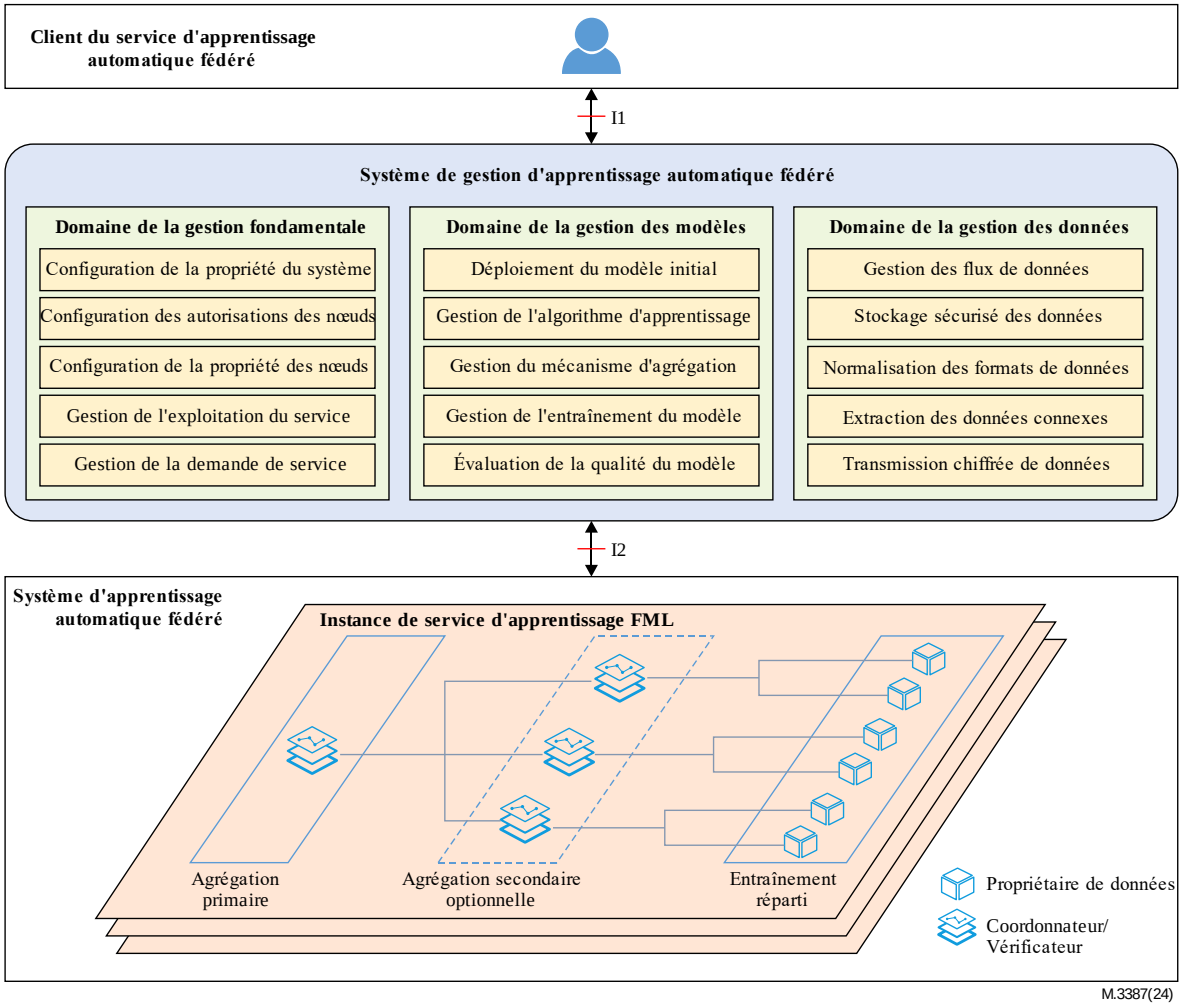

Figure 1 – Scénario de gestion du système d'apprentissage automatique fédéré

Le domaine de la gestion fondamentale comprend la configuration de la propriété du système, la configuration des autorisations des nœuds, la configuration de la propriété des nœuds, la gestion de l'exploitation du service et la gestion de la demande de service.

– **Configuration de la propriété du système**: initialisation et modification des propriétés des systèmes FMLS.

– **Configuration des autorisations des nœuds**: gestion des autorisations des nœuds d'entraînement de l'apprentissage FML conformément aux règles de sécurité définies par le système de gestion FMLMS.

– **Configuration de la propriété des nœuds**: initialisation et modification des propriétés des nœuds d'entraînement de l'apprentissage FML.

– **Gestion de l'exploitation du service**: gestion de la topologie du service d'apprentissage FML et évaluation de la qualité de service d'apprentissage FML.

– **Gestion de la demande de service**: classification et traitement des demandes du service d'apprentissage FML et réponse à ces demandes.

Le domaine de la gestion des modèles comprend le déploiement du modèle initial, la gestion de l'algorithme d'apprentissage, la gestion du mécanisme d'agrégation, la gestion de l'entraînement du modèle et l'évaluation de la qualité du modèle.

– **Déploiement du modèle initial**: déploiement du modèle FMLM au niveau du coordonnateur en fonction des exigences relatives au service.

– **Gestion de l'algorithme d'apprentissage**: sélection des algorithmes d'apprentissage automatique appropriés en fonction des exigences relatives au service d'apprentissage FML.
– **Gestion du mécanisme d'agrégation**: sélection ou conception des stratégies d'agrégation appropriées en fonction des exigences relatives au service d'apprentissage FML, des capacités des ressources et des caractéristiques des données.
– **Gestion du modèle d'entraînement**: contrôle et suivi du processus d'entraînement des modèles, notamment de la transmission et de l'actualisation du modèle FMLM.
– **Évaluation de la qualité du modèle**: évaluation de la qualité du modèle FMLM en fonction des indicateurs d'évaluation.

Le domaine de la gestion des données comprend la gestion des flux de données, le stockage sécurisé des données, la normalisation des formats de données, l'extraction des données connexes et la transmission chiffrée de données.

– **Gestion des flux de données**: contrôle des flux de métadonnées de données brutes et des flux de données du modèle FMLM.
– **Stockage sécurisé des données**: stockage des métadonnées de données brutes moyennant l'application de différentes méthodes de chiffrement.
– **Normalisation des formats de données**: normalisation du format des métadonnées de données brutes, par exemple sous forme de tableau.
– **Extraction de données connexes**: extraction des données liées à la tâche d'apprentissage FML se présentant sous la forme d'ensemble de données en vue de former le modèle FMLM.
– **Transmission chiffrée de données**: sélection des algorithmes de chiffrement pour chiffrer les données transmises et les canaux de communication.

8 Exigences applicables au domaine de la gestion fondamentale

8.1 Exigences applicables à la configuration de la propriété des systèmes

Il est exigé que le système de gestion de l'apprentissage automatique fédéré (FMLMS) configure la propriété du système FMLS pour appuyer la mise en œuvre fonctionnelle des services d'apprentissage FML, y compris les propriétés des tâches et les propriétés des ressources.

8.1.1 Propriétés des tâches

Il est exigé que le système de gestion FMLMS configure les propriétés des tâches en fonction des demandes de service d'apprentissage FML présentées par les clients FMLSC.

– Type de tâche: catégorie de la tâche d'apprentissage FML (exemple: tâche de classification d'images et tâche de génération de texte).
– Priorité de la tâche: importance de la tâche d'apprentissage FML (exemple: priorité élevée, priorité moyenne et priorité faible).

8.1.2 Propriétés des ressources

Il est exigé que le système de gestion FMLMS configure les capacités des ressources d'une tâche d'apprentissage FML, y compris la capacité de calcul, la capacité de communication et la capacité de stockage.

– Capacité de calcul: ressource de calcul totale nécessaire pour les tâches d'apprentissage FML (exemple: nombre d'unités centrales de traitement (CPU) et d'unités de traitement graphique (GPU)).
– Capacité de communication: ressource de communication totale nécessaire pour les tâches d'apprentissage FML (exemple: puissance de transmission et largeur de bande).

– Capacité de stockage: ressource de stockage totale nécessaire pour les tâches d'apprentissage FML (exemple: espace disque libre et espace de stockage préassigné).

8.2 Exigences applicables à la configuration des autorisations des nœuds

Il est exigé que le système de gestion FMLMS sélectionne les nœuds d'entraînement d'apprentissage FML appropriés disposant des ressources suffisantes en fonction de la tâche d'apprentissage FML en cours, puis donne l'autorisation et contrôle l'autorisation d'accès selon la sécurité et la fiabilité des nœuds.

8.3 Exigences applicables à la configuration des propriété des nœuds

Il est exigé que le système FMLMS prenne en charge la configuration des propriétés des nœuds d'entraînement FML, y compris les propriétés des rôles, les propriétés de calcul, les propriétés de communication et les propriétés de stockage.

8.3.1 Propriétés des rôles

Il est exigé que le système FMLMS configure le rôle des nœuds d'entraînement FML. Les nœuds d'entraînement peuvent se voir attribuer le rôle de coordonnateur, vérificateur et propriétaire des données. Les fonctions spécifiques de ces rôles sont décrites dans la norme [IEEE 3652.1].

8.3.2 Propriétés de calcul

Il est exigé que le système FMLMS prenne en charge la configuration des attributs liés au calcul des nœuds d'entraînement FML, par exemple le nombre d'unités CPU et d'unités GPU.

8.3.3 Propriétés de communication

Il est exigé que le système FMLMS prenne en charge la configuration des attributs liés à la communication des nœuds d'entraînement FML, par exemple la puissance d'émission et la largeur de bande.

8.3.4 Propriétés de stockage

Il est exigé que le système FMLMS prenne en charge la configuration des attributs liés au stockage des nœuds d'entraînement FML, par exemple l'espace libre sur le disque et l'espace de stockage préassigné.

8.4 Exigences applicables à la gestion de l'exploitation du service

Il est exigé que le système FMLMS gère la qualité de fonctionnement du service FML, y compris la gestion de la topologie du service et l'évaluation de la qualité du service.

8.4.1 Gestion de la topologie du service

Il est exigé que le système FMLMS gère la topologie du service FML, ce qui comprend principalement la génération de la topologie du service et la reconstruction de la topologie du service.

– Génération de la topologie du service: générer la topologie du service FML pour la tâche d'entraînement FML actuelle, y compris les rôles et les relations de connexion entre les nœuds d'entraînement de l'apprentissage FML, et envoyer la topologie à tous les nœuds d'entraînement FML.
– Reconstruction du service de topologie: reconstruire la topologie du service FML en cas de panne d'un nœud du service, d'épuisement des ressources, etc.

8.4.2 Évaluation de la qualité du service

Il est recommandé que le système FMLMS évalue la qualité du service FML, y compris l'évaluation de la qualité de fonctionnement et l'évaluation incitative du service.

– Qualité de fonctionnement du réseau: évaluer la qualité de fonctionnement des systèmes d'apprentissage automatique fédéré (FMLS), par exemple la consommation de ressources et le temps de transmission.
– Évaluation des incitations du service: évaluer la contribution globale des nœuds d'entraînement FML au service FML et configurer un mécanisme incitatif intrinsèque en fonction de cette contribution, afin d'inciter chaque nœud d'entraînement FML à participer au service FML. Les contributions globales comprennent la consommation de ressources, la contribution à l'amélioration de la qualité du modèle, etc.

8.5 Exigences applicables à la gestion des demandes de service

Il est exigé que le système FMLMS classifie et attribue les demandes de service lorsque plusieurs de ces demandes coexistent.

– Classification des demandes de service: classifier les demandes de service en fonction de l'importance, des priorités et des exigences en matière de délai, etc.
– Attribution des demandes de service: répondre aux demandes de service par le biais de méthodes d'attribution, par exemple l'attribution en fonction des priorités.

9 Exigences applicables au domaine de gestion des modèles

9.1 Exigences applicables au déploiement initial du modèle

Il est exigé que le système FMLMS prenne en charge la fourniture de l'apprentissage FML et le lancement de l'entraînement en fonction des demandes de service FML soumises par les clients FMLSC.

9.2 Exigences applicables à la gestion des algorithmes d'apprentissage

Il est exigé que le système FMLMS sélectionne les algorithmes d'apprentissage automatique et configure les paramètres pertinents en fonction des exigences du service FML.

– Sélection des algorithmes: sélectionner les algorithmes d'apprentissage automatique adaptés, par exemple le réseau neuronal et l'arbre décisionnel.
– Configuration des paramètres: configurer les paramètres et les hyperparamètres de l'algorithme d'apprentissage automatique, comme la vitesse d'apprentissage, la taille des lots et le coefficient de régularisation.

9.3 Exigences applicables à la gestion du mécanisme d'agrégation

Il est exigé que le système FMLMS sélectionne un mécanisme d'agrégation et configure les paramètres appropriés en fonction des besoins de service FML, des capacités de ressources et des caractéristiques des données.

– Sélection du mécanisme: sélectionner ou concevoir un mécanisme d'agrégation approprié (par exemple, synchrone, asynchrone, semi-synchrone).
– Configuration des paramètres: configurer les paramètres du mécanisme d'agrégation (par exemple, nombre de cycles d'agrégation, nombre de groupes, poids dans l'agrégation de modèles).

9.4 Exigences applicables à la gestion de l'entraînement des modèles

Il est exigé que le système FMLS permette aux propriétaires des données de procéder à l'entraînement local du modèle FMLM et de télécharger le modèle appris sur le coordonnateur.

Il est exigé que le système FMLS permette au coordonnateur de gérer le processus d'entraînement du modèle FMLM, y compris la diffusion, l'agrégation et la mise à jour.

Il est exigé que le système FMLS permette au vérificateur de surveiller le processus d'entraînement du modèle FMLM sur la base des règles mises en œuvre, par exemple déterminer la fiabilité du nœud d'entraînement FML et mesurer la contribution des nœuds d'entraînement FML.

9.5 Exigences applicables à l'évaluation de la qualité du modèle

Il est exigé que le système FMLMS évalue la qualité du modèle FMLM en fonction des métriques de performance des modèles.

NOTE – Les métriques de performance des modèles peuvent comprendre la précision, le rappel, l'aire sous la courbe (AUC) pour les modèles de classification et l'erreur quadratique moyenne pour les modèles de régression [b-UIT-T Y.3179].

Il est recommandé que le système de gestion FMLMS ajuste le processus d'entraînement tout au long de l'évaluation du modèle pour améliorer la performance du modèle.

10 Exigences applicables au domaine de gestion des données

10.1 Exigences applicables à la gestion du flux des données

Il est exigé que le système FMLS prenne en charge la génération, le stockage, la transmission et la mise à jour des métadonnées issues de données brutes.

NOTE – Les métadonnées issues de données brutes (par exemple, les identificateurs de données, les caractéristiques des données) peuvent, à titre d'option, être échangées entre propriétaires de données au cours de l'apprentissage FML.

Il est exigé que le système FMLS prenne en charge la transmission, l'agrégation et la mise à jour des données sur le modèle FMLM.

Il est exigé que le système FMLS prenne en charge la gestion de la sécurité des données sur les modèles, afin d'éviter que des données confidentielles soient exposées à des nœuds externes et malveillants au cours de l'apprentissage FML.

10.2 Exigences applicables au stockage sécurisé des données

Il est exigé que le système de gestion FMLMS prenne en charge le stockage sécurisé des métadonnées issues de données brutes et des données sur les modèles.

10.3 Exigences applicables à la normalisation du format des données

Il est exigé que le système de gestion FMLMS collecte les caractéristiques des métadonnées issues de données brutes et fournisse un format de base de données standard et unifié.

NOTE – Consulter la norme [IEEE 3652.1]. Les données brutes utilisées pour l'apprentissage FML sont généralement stockées dans un format de base de données standard, où chaque ligne représente un échantillon de données et chaque colonne représente une caractéristique ou une étiquette de cet échantillon. Un ensemble d'attributs de caractéristiques est habituellement représenté par les vecteurs propres (X_1, X_2, ..., X_n). Dans l'apprentissage supervisé, l'ensemble complet de données d'apprentissage se compose de caractéristiques représentées par X et d'étiquettes représentées par Y.

10.4 Exigences applicables à la récupération des données connexes

Il est exigé que le système FMLS permette aux propriétaires des données de récupérer les données brutes liées à l'entraînement du modèle sous la forme d'ensembles de données. Dans un système FMLS, plusieurs ensembles de données peuvent se chevaucher au niveau des identificateurs d'échantillon et des attributs de caractéristiques. Selon le degré de chevauchement des identificateurs de l'échantillon ou des caractéristiques, trois cas de figure peuvent se présenter:

– Apprentissage FML horizontal: créer un modèle dans lequel les ensembles de données présentent d'importants chevauchements au niveau de l'espace des caractéristiques, mais pas

de l'espace des identificateurs. Le coordonnateur est responsable de l'alignement des caractéristiques entre les propriétaires de données.

– Apprentissage FML vertical: créer un modèle dans lequel les ensembles de données présentent d'importants chevauchements au niveau de l'espace des échantillons, mais pas de l'espace des caractéristiques. Le coordonnateur est responsable de l'alignement des échantillons entre les propriétaires de données.

– Apprentissage transférable fédéré: créer un modèle dans lequel les ensembles de données ne présentent pas de chevauchement important que ce soit au niveau de l'espace des échantillons ou de l'espace des caractéristiques. Le coordonnateur est responsable de l'exploitation de connaissances réutilisables dans différents domaines de caractéristiques.

10.5 Exigences applicables à la transmission chiffrée des données

Il est exigé que le système FMLS prenne en charge les technologies de protection de la confidentialité des données, telles que l'informatique multipartite, le chiffrement homomorphe et la confidentialité différentielle pour empêcher d'autres nœuds d'entraînement de l'apprentissage FML de déduire des informations sur les données brutes à partir des données du modèle.

Il est recommandé que le système FMLS prenne en charge les technologies de chiffrement des canaux pour préserver la sécurité de l'environnement lors des processus de transmission de données.

Appendice I

Exemple de cas d'utilisation du système FMLMS appliqué à la gestion de l'entraînement FMLS pour les services de détection des anomalies routières dans l'Internet des véhicules

(Le présent appendice ne fait pas partie intégrante de la présente Recommandation.)

Le présent appendice fournit un exemple type d'application et de service qui applique le système de gestion de l'apprentissage automatique fédéré (FMLMS) pour gérer le système d'apprentissage automatique fédéré (FMLS) dans l'Internet des véhicules (IoV). Il décrit également les fonctions du système FMLMS pour le service FML, qui font l'objet de la présente Recommandation.

I.1 Introduction

Les nouvelles applications basées sur des dispositifs intelligents, tels que les véhicules intelligents, ont des exigences strictes en termes de latence et de confidentialité. Cela rend l'informatique en nuage inadaptée à ces scénarios et donne naissance à l'apprentissage FML basé sur l'informatique périphérique de réseau mobile (MEC). L'apprentissage FML basé sur l'informatique MEC entraîne les modèles d'apprentissage automatique de manière distribuée sur des appareils mobiles avec des ressources limitées de calcul, de stockage, d'énergie et de largeur de bande, en conservant les données brutes localement. Les paramètres des modèles sont fournis aux points d'accès informatiques (CAP) les plus proches pour agrégation. Dans le cadre de l'IoV, le partage de données entre véhicules à des fins d'analyse collaborative améliore l'expérience de conduite et la qualité du service. Ainsi, la conception d'une architecture informatique collaborative basée sur l'apprentissage FML assistée par l'informatique MEC contribue aux services de détection des anomalies routières tout en protégeant la confidentialité des données.

I.2 Architecture FML collaborative nuage-périphérie-terminal

Dans l'IoV, un système FMLS utilise l'apprentissage FML pour apprendre un modèle FMLM mondial, qui est appliqué aux services de détection des anomalies routières. Les composantes du système FMLS comprennent les propriétaires des données déployés sur les véhicules intelligents, les coordonnateurs déployés sur les points CAP et un serveur d'agent FML (représenté par la mention AS dans la Figure I.1) déployé sur le serveur en nuage (représenté par la mention CS dans la Figure I.1). Le système FMLMS est déployé sur le nuage et gère le processus d'entraînement FML. Les technologies basées sur l'informatique MEC sont appliquées pour garantir la qualité du service FML par le biais de l'attribution des tâches et de l'agrégation régionale des modèles. Le scénario d'entraînement FML dans l'architecture nuage-périphérie-terminal est décrit dans la Figure I.1.

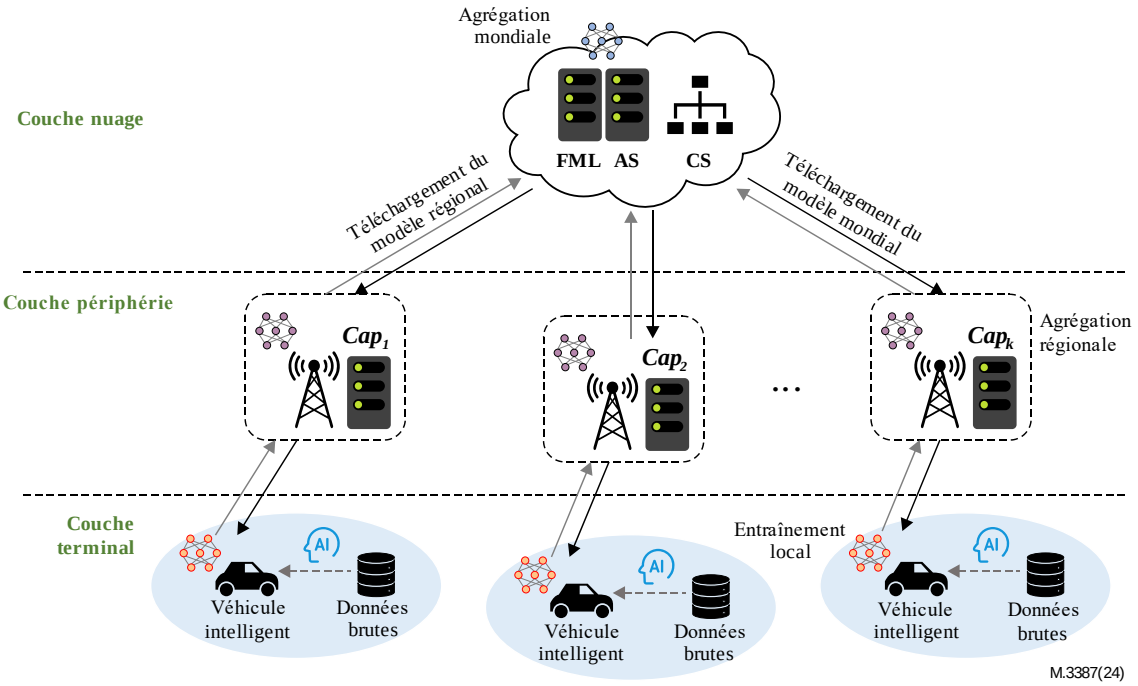

Figure I.1 – Scénario d'infrastructure FML collaborative nuage-périphérie-terminal dans l'IoV

Comme illustré dans la Figure I.1, les responsabilités de chaque couche pour les nœuds d'entraînement FML sont les suivantes:

– Couche terminal: les propriétaires des données, c'est-à-dire les véhicules intelligents, utilisent les données générées localement pour entraîner un modèle FMLM local et transmettre les paramètres du modèles aux points CAP pour agrégation régionale (agrégation secondaire).

– Couche périphérie: les points CAP, généralement les unités de bord de route dans les scénarios faisant intervenir des véhicules, sont individuellement responsables de recueillir les paramètres du modèle local auprès des propriétaires des données dans une région spécifique. Ils mettent ensuite à jour les modèles FMLM régionaux par le bais de l'agrégation régionale (agrégation secondaire), puis envoient les paramètres des modèles mis à jour au serveur d'agent. En outre, les points CAP collectent les métadonnées issues des données brutes et les informations relatives à l'état des dispositifs, puis les envoient au système de gestion de l'apprentissage automatique fédéré (FMLMS).

– Couche nuage: dans le nuage, un système FMLMS est déployé afin de gérer le fonctionnement de l'apprentissage FML. Simultanément, le serveur d'agent agrège tous les paramètres régionaux du modèle pour apprendre un modèle FMLM mondial par agrégation mondiale (agrégation primaire). En outre, le système FMLMS évalue la qualité de fonctionnement du système FMLS.

I.3 Le processus de gestion du système FMLS dans l'entraînement du modèle de détection des anomalies routières

Dans les scénarios de l'infrastructure FML collaborative nuage-périphérie-terminal, un système FMLMS est déployé dans le nuage pour gérer les ressources réseau et la qualité du service FML, garantissant ainsi l'efficacité, la durabilité et la sécurité du service FML dans le cadre de l'IoV. On trouvera ci-après un exemple illustrant l'entraînement d'un modèle de détection des anomalies routières pour les véhicules intelligents.

Étape 1: Tous les propriétaires potentiels de données (c'est-à-dire les véhicules intelligents) accèdent au réseau FML. Le client du service d'apprentissage automatique fédéré (FMLSC) demande au système FMLMS de lui fournir un service d'entraînement du modèle de détection des anomalies routières via l'interface 1.

Étape 2: Le système FMLMS configure les attributs de la tâche en fonction de la demande de service FML, l'identifie comme une tâche de reconnaissance d'image et lui attribue une priorité. Selon la situation des ressources réseau, le système FMLMS sélectionne une stratégie incitative visant à encourager davantage de propriétaires de données à rejoindre la tâche d'entraînement du modèle de détection des anomalies routières.

À l'aide de la stratégie incitative générée, le système FMLMS détermine les nœuds d'entraînement FML pour la tâche FML en cours. Ensuite, le système attribue les rôles à chacun des nœuds d'entraînement FML. Puis, il détermine les propriétés de ressources correspondantes pour tous les nœuds d'entraînement FML, y compris les propriétés liées au rôle, au calcul, à la communication et au stockage.

Sur la base des rôles des nœuds d'entraînement FML, le système FMLMS génère une topologie de service FML, y compris les relations de liaison entre les nœuds d'entraînement et les configurations des attributs pertinents.

Ensuite, le système FMLMS détermine l'algorithme d'entraînement et le mécanisme d'agrégation pour la tâche de détection des anomalies routières, par exemple le réseau neuronal convolutif (CNN) et l'algorithme d'agrégation asynchrone.

Étape 3: Le système FMLMS envoie le modèle CNN initial, la propriété du système, l'autorisation de nœud, la propriété du nœud, la topologie du service, l'algorithme d'apprentissage et le mécanisme d'agrégation au système FMLS via l'interface 2. En outre, le système FMLMS envoie les paramètres associés aux algorithmes de confidentialité et aux algorithmes de chiffrement des canaux au système FMLS et chiffre ainsi les données relatives au modèle et les canaux en vue de garantir la confidentialité et la sécurité du modèle FMLM.

Étape 4: Le système déploie le modèle CNN initial à tous les nœuds d'entraînement FML, et exige que les propriétaires des données procèdent au prétraitement de leurs données brutes exclusives dans un format normalisé. Ensuite, tous les propriétaires de données récupèrent les données pertinentes au sujet de l'image en fonction de la demande de service visant à entraîner le modèle FMLM local.

Étape 5: Les propriétaires des données téléchargent le modèle local entraîné sur un point CAP à proximité. Ensuite, les points CAP génèrent les modèles régionaux à partir des données recueillies sur le modèle local, puis envoient les modèles régionaux au serveur d'agent pour agrégation mondiale.

Étape 6: Le système FMLMS surveille la qualité de fonctionnement du système FMLS et la qualité des modèles FMLM. Le système FMLMS peut ajuster la topologie du service en fonction de la qualité de fonctionnement, et déterminer s'il convient de mettre fin à la tâche d'entraînement en fonction de la qualité du modèle FMLM mondial. Lorsque la précision du modèle répond aux exigences du service, le système FMLMS envoie le modèle FMLM entraîné à l'échelle mondiale au client FMLSC via l'interface 1. Si la précision du modèle ne répond pas aux exigences de service, la tâche d'entraînement continue.

Bibliographie

[b-UIT-T X.1367] Recommandation UIT-T X.1367 (2020), *Format normalisé de journaux d'erreurs pour l'Internet des objets aux fins de la gestion des incidents de sécurité.*

[b-UIT-T Y.3179] Recommandation UIT-T Y.3179 (2021), *Cadre architectural pour le modèle d'apprentissage automatique utilisé dans les réseaux futurs, y compris les réseaux IMT-2020.*

[b-UIT-T Y.4205] Recommandation UIT-T Y.4205 (2019), *Exigences et modèle de référence des systèmes participatifs liés à l'Internet des objets.*

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	**Gestion des télécommunications y compris le RGT et maintenance des réseaux**
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Publié en Suisse
Genève, 2024