IEEE SA
STANDARDS ASSOCIATION

IEEE Guide for Architectural Framework and Application of Federated Machine Learning

IEEE Computer Society

Developed by the
Learning Technology Standards Committee

IEEE Std 3652.1™-2020

IEEE

IEEE Guide for Architectural Framework and Application of Federated Machine Learning

Developed by the

Learning Technology Standards Committee
of the
IEEE Computer Society

Approved 24 September 2020

IEEE SA Standards Board

Abstract: Federated machine learning defines a machine learning framework that allows a collective model to be constructed from data that is distributed across repositories owned by different organizations or devices. A blueprint for data usage and model building across organizations and devices while meeting applicable privacy, security and regulatory requirements is provided in this guide. It defines the architectural framework and application guidelines for federated machine learning, including description and definition of federated machine learning; the categories federated machine learning and the application scenarios to which each category applies; performance evaluation of federated machine learning; and associated regulatory requirements.

Keywords: computation efficiency, economic viability, federated machine learning (FML), IEEE 3652.1™, incentive mechanism, machine learning, model performance, privacy, privacy regulations, security

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-1-5044-7053-7 STD24407
Print: ISBN 978-1-5044-7054-4 STDPD24407

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the IEEE SA myProject system. An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; https://www.copyright.com/. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website. Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the IEEE SA Patent Policy.

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants (entities)

At the time this draft standard was completed, the Shared Machine Learning Working Group had the following membership:

Qian Yang, *Chair*
Ji Feng, *Vice Chair*

Organization Represented	*Name of Representative*
4Paradigm	Wei-Wei Tu
4Paradigm	Xiawei Guo
AI Singapore	Jianshu Weng
AI Singapore	Seng Meng Koo
Alipay	Kepeng Li
Beijing Baidu Netcom Science Technology Co., Ltd	Jue Hong
Beijing Baidu Netcom Science Technology Co., Ltd	Xiaoru Li
BGI	Meng Yang
CETC Big Data Research Institute Co., Ltd.	Yanhong Pu
CETC Big Data Research Institute Co., Ltd.	Xu Cheng
China Telecom	Biying Pan
Chinese Academy of Sciences (ICT)	Yiqiang Chen
Chinese Academy of Sciences (ICT)	Xinlong Jiang
Clustar Technology Co., Ltd	Kai Chen
Clustar Technology Co., Ltd	Xinchen Wan
Eduworks	Robby Robson
Ennew IOT Co., Ltd	Xiaoxu Ma
Ennew IOT Co., Ltd	Zengxiang Li
Hangzhou Qulian Technology Co., Ltd.	Xiaofeng Chen
Huawei	Gaokun Pang
Huawei	Xiaoqi Cao
JD iCity	Junbo Zhang
JD iCity	Yu Zheng
JD iCity	Yang Liu
LogiOcean	Mingshu Cong
LogiOcean	Xiang Li
Qingdao Hisense Electronic Industry Holdings Co., Ltd	Xuesong Gao
Qingdao Hisense Electronic Industry Holdings Co., Ltd	Yuyi Zhang
SensesGlobal	Yu Yuan
Sinovation Ventures AI Institute	Ji Feng
Sinovation Ventures AI Institute	Qi-Zhi Cai
Sinovation Ventures AI Institute	Yonggang Wang

Squirrel AI ..... Richard Tong
Squirrel AI ..... Wei Cui
Tencent ..... Yongxia Wang
Tencent ..... Shuqui Qin
WeBank ..... Qiang Yang
WeBank ..... Lixin Fan
WeBank ..... Tianyu Zhang
Xiaomi ..... Yanhua Li
Xiaomi ..... Wei Li
YITU ..... Chunhao Zhao

When the IEEE Learning Technology Standards Committee sponsored and oversaw the Shared Machine Learning Working Group it had the following leadership team:

Richard Tong, *Chair*
Jim Goodell, *Vice Chair*
Avron Barr, *Past Chair*
Shelly Blake-Plock, *Treasurer*
Brandt Redd, *Secretary*
Robby Robson, *Past Chair and Liaison to ISO SC36*

The Working Group gratefully acknowledges the contributions of the following participants. Without their assistance and dedication, this standard would not have been completed.

Xiaoqi Cao
Xu Cheng
Yuantong Ding
Lixin Fan
Xiawei Guo
Jue Hong
Kepeng Li
Xiang Li
Yang Liu
Shuqi Qin
Yonggang Wang
Chunhao Zhao
Yu Zheng

The following members of the entity Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

0xSenses Corporation
4Paradigm Inc.
AI Singapore
Beckhoff Automation
Beijing Clustar Technology Co., Ltd.
Beijing Genomics Institute at Shenzhen
Beijng Baidu Netcom Science Technology Co., Ltd.
CETC Big Data Research Institute Co., Ltd.
China Telecommunications Corporation
Eduworks Corporation
Ericsson AB
Hangzhou Qulian Technology Co., Ltd.
Huakong TsingJiao Information Science (Beijing) Limited
Huawei Technologies Co., Ltd
JD.com, Inc.
LogiOcean Financial Technologies Ltd
Shanghai Fudata Technology Co., Ltd.
Sinovation Ventures AI Institute
Tencent
WeBank Co., Ltd.
Xiaomi Communications Co., Ltd.
YITU Technology
Yixue Education, Inc.

When the IEEE SA Standards Board approved this standard on 24 September 2020, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse
Doug Edwards
J. Travis Griffith
Grace Gu
Guido R. Hiertz
Joseph L. Koepfinger*
David J. Law
Howard Li
Dong Liu
Kevin Lu
Paul Nikolich
Damir Novosel
Dorothy Stanley
Mehmet Ulema
Lei Wang
Sha Wei
Philip B. Winston
Daidi Zhong
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 3652.1-2020, 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, such as the European Union's General Data Protection Regulation. Many routine operations in big data applications, such as merging user data from various sources in order to build a machine learning model, are considered to be illegal under current regulatory frameworks. The purpose of federated machine learning is to provide a feasible solution that enables machine learning applications to utilize the data in a distributed manner that does not exchange raw data directly and does not allow any party to infer private information of other parties. Federated machine learning is expected to promote and facilitate collaborations among multiple parties, some of which are data source owners, such that user privacy and information security are protected. This guide will promote the use of distributed data sources without violating regulations or ethical considerations.

Contents

IEEE Guide for Architectural Framework and Application of Federated Machine Learning

1. Overview

Companies and organizations are collecting increasingly more detailed information about users. On the one hand, this information is exploited by machine learning techniques to improve products, services, and welfare. It is a consensus that valuable information can be extracted, preferably, through raw data that belong to different organizations. On the other hand, due to the potential misuse and adversarial attacks, there can be severe challenges to the protection of data privacy and security in a distributed machine learning paradigm as such. Federated machine learning (FML) is a technology that aims to build and use machine-learning models by collectively exploiting the data at each data owner's location without compromising user privacy and information security. Practitioners can benefit from a standard for federated machine learning that facilitates both the protection of user data privacy and security, at the same time, supports efficient, flexible, and scalable processing of raw data with advanced machine learning techniques.

1.1 Scope

Federated machine learning is a technological framework that allows a machine learning model to be collectively constructed and used through data that is distributed across repositories owned by different organizations or devices. While facilitating the building of federated machine learning models, this framework also aims to preserve privacy, improve security, and meet regulatory requirements concerning data usage. This standard defines the architectural framework and application guidelines for federated machine learning, including the following:

— Description and definition of federated machine learning

— The categories of federated machine learning technologies and the application scenarios to which each category applies

— A set of measures concerning the performance evaluation criteria for federated machine learning

— Associated features of federated machine learning that fulfill different regulatory requirements

1.2 Purpose

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 such as the European Union's General Data Protection Regulation. Many routine operations in big data applications,

such as merging user data from various sources in order to build a machine learning model, are considered to be illegal under current regulatory frameworks. The purpose of federated machine learning is to provide a feasible solution that enables machine learning applications to utilize the data in a distributed manner that does not exchange raw data directly and does not allow any party to infer private information of other parties. Federated machine learning is expected to promote and facilitate collaborations among multiple parties, some of which are data source owners, such that user privacy and information security are protected. This guide will promote the use of distributed data sources without violating regulations or ethical considerations.

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).[1,2]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

There are no normative references in this guide.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause. [3]

accuracy: The fraction of results that are correct, i.e., the fraction of results that are either true positives or true negatives.

auditor: A user who is responsible for checking the correctness and the performance of an FML process to verify that the process complies with regulatory requirements.

coordinator: A user who builds FML models from different data owners and provides FML models to model users.

[1]The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.
[2]The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.
[3]*IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

data owner: A user who has ownership claim to a data set used in federated machine learning.

data quality: A metric that indicates the usefulness and effectiveness of the data set.

data set: A collection of data items that consist of data *features* (consisting of feature names and values), data *labels* (for (semi-) supervised learning), and data item identifier (ID).

encryption: an algorithm to convert plaintexts to ciphertexts to provide confidentiality with a cryptographic key as a parameter.

feature: A subset of measurable properties of data items.

federated machine learning: 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. See 4.1 for details.

federated machine learning model: The result of the model-training process of a federated machine learning system. The learned model can be used in order to make certain machine-learning inference tasks on new data, e.g., classification, recognition, prediction, and recommendation.

label: A common property associated with a subset of data features for (semi-) supervised learning.

model user: The user who uses an FML model in various tasks.

outcome: The result of an FML system's inference process based on new data.

outcome profile: A list of outcomes of all agents based on a certain testing data.

payment scheme: A payment scheme is a function, which decides the transfer payments to data owners and model user

precision: The fraction of the true positive among the true positive plus the false positive data.

raw data: Raw data is a collection of data sets that is obtained and maintained by data owners. This data set contains user and data owner's private information and needs protection. Raw data are also referred to as **private data** to emphasize the need of privacy protection.

recall: The fraction of the true positive among the true positive and the false negative.

testing data set: A data set that is used to evaluate the performance of a trained FML model.

training: A federated machine learning process, in which the raw data are kept private and are exploited to optimize the performance of an FML model for some given machine-learning tasks.

training data set: A data set that is used to train the FML model.

transfer payment: The monetary payments that a coordinator pays or charges the data owners and model users.

user: An individual, entity, party/participant, or institution involved in FML. A user may play the role of a coordinator, a data owner, a model user or an auditor. It should be noted that a user may, simultaneously, play multiple roles.

3.2 Acronyms and abbreviations

FML	federated machine learning
MSE	mean square error
RMSE	root mean square error
MAPE	mean absolute percentage error
IRI	individual rationality index
BSM	budget surplus margin
EI	efficiency Index
DOR	data offering rate
FI	fairness index

3.3 Symbols

IR_i	individual rationality of data owner *i*
p_i	payment of data owner *i*
c_i	cost of providing data of data owner *i*
w_i	user-defined weight for the relative importance of data owner *i*
d_i	effective data owned by data owner *i*
D	total effective data owned by all data owners
B	budget surplus margin
P	total payments paid to data owners
R	total revenue received from model users
Num_{train}	number of training samples
Num_{test}	number of test samples

4. FML reference architecture

Federated machine learning is a distributed machine-learning framework that enables multiple participants to collaboratively train and use a machine learning model for a given task, e.g., classification, prediction, and recommendation. Within this framework, all raw data owned by different participants are protected by secure and privacy-preserving techniques, which prevent the data from being tampered and disclosed by other participants or reverse-engineered by other participants.

An FML framework consists of data, users, and systems that are illustrated in Figure 1. In the framework, data are distributed across different repositories and are used to build FML sub-models that are, subsequently, integrated to result in a federated model in a secure and privacy-preserving manner.

An FML user can be a natural person, a corporation, or other organizations with the legal capacity to participate in the FML framework. In addition, FML users may play four roles, which are the data owners, the model users, the coordinators, and the auditors (see details in Clause 6). The FML system consists of multiple functional modules that provide FML services to users (see more detail in Clause 7).

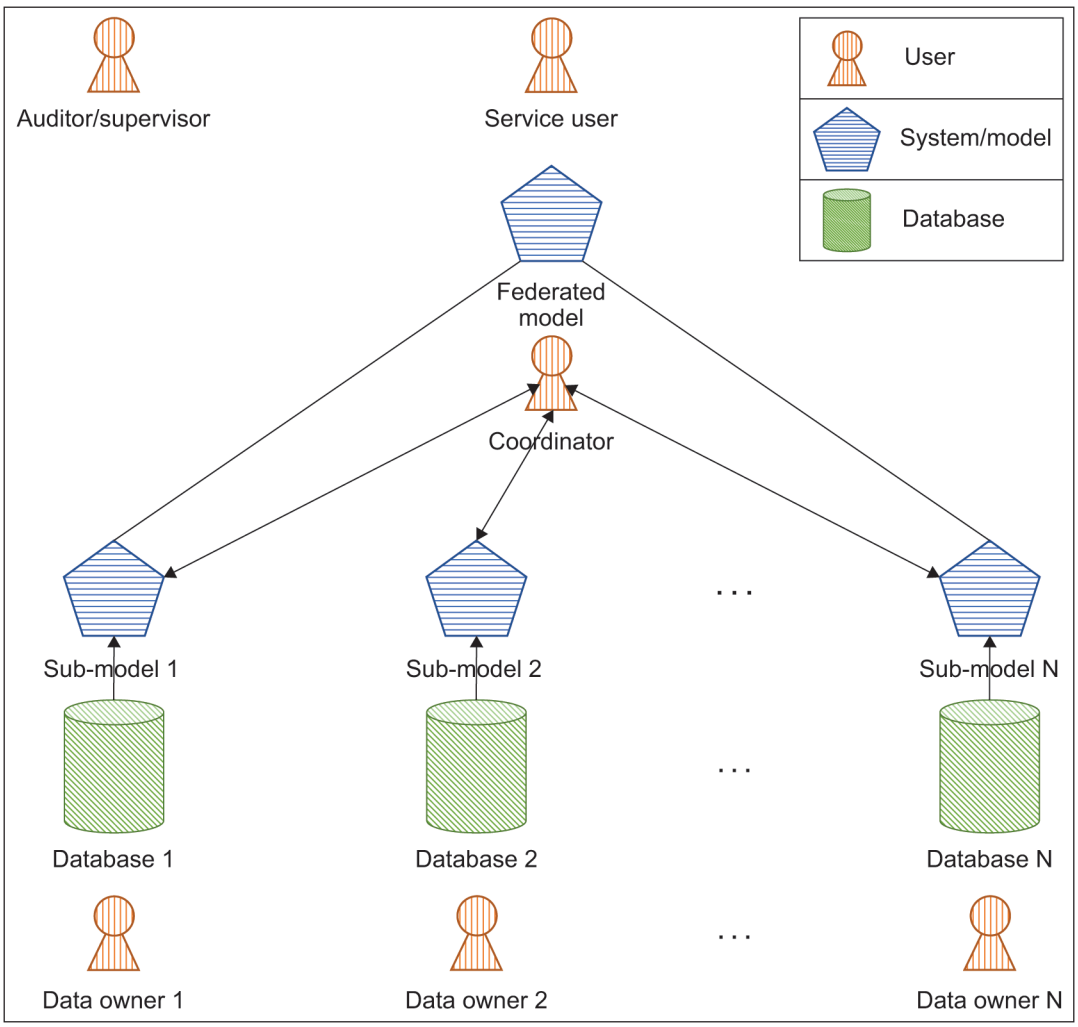

Figure 1—A schematic diagram of FML framework, consisting of data, user and system

5. FML data view

5.1 Overview

FML data is often stored in a standard database format, i.e., tables, whereby each row represents a data sample and each column represents a feature or label of the sample. In supervised learning, a complete training data set consists of both features, denoted by X, and labels, denoted by Y. A set of feature attributes are usually represented as a feature vector (X1, X2, …, Xn). Moreover, a unique sample ID is associated with each data sample. In an FML system, data from multiple data sets may have overlaps in sample IDs and/or feature attributes. Depending on the extent of overlapping along either sample IDs or features, the following three cases are of interest for a federated machine learning framework:

— The overlap of feature attributes (X1, X2, …) is *substantially larger* than the overlap of sample IDs (U1, U2, …)

— The overlap of sample IDs (U1, U2, …) is *substantially larger* than the overlap of feature attributes (X1, X2, …)

— The overlap of sample IDs (U1, U2, …) and the overlap of features (X1, X2, …) are both *small*

In the list above, "substantially larger" (and "significant overlap") is judged by whether the overlapping data can be used to build a high-quality machine learning model, where the measure of quality is determined by applications.

Depending on the application scenarios, FML is categorized as Horizontal FML, Vertical FML, and Federated Transfer Learning (as shown in Table 1). Also, depending on whether the data sets used have the same format or different format, FML is categorized into homogeneous FML or heterogeneous FML.

Table 1—FML data view categorization

Data distribution		Overlap of features	
		Large	Small
Overlap of sample IDs	Large	FML not needed	Vertical FML
	Small	Horizontal FML	Federated transfer learning

5.2 Horizontal FML

Horizontal FML refers to building a model in the scenario where data sets have significant overlaps on the feature spaces (X1, X2, …) but not on the ID spaces. In this case, an FML model can be built as if the data is split and join *horizontally*. Horizontal FML may apply to scenarios where the number of sample IDs from data owners is too small to build a high-quality model. An FML model should perform better than the sub-models built by one single data set, and the performance of the FML model is very close to that of the model built when all data were put together in one location.

See Figure 2.

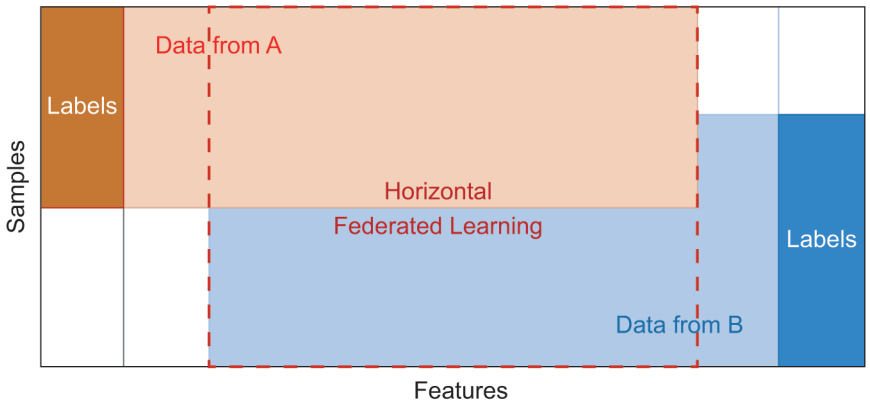

Figure 2—Horizontal FML

5.3 Vertical FML

Vertical FML refers to building a model in the scenario where data sets have significant overlaps on the sample space D, but not on the feature spaces (X1, X2, …). In this case, an FML model can be built as if the data is split and joined vertically. Vertical FML may apply to scenarios where there are insufficient features or labels to build a high-quality model. An FML model should perform better than the sub-models built by one single data set, and the performance of the FML model is very close to that of the model built when all data were put together in one location.

See Figure 3.

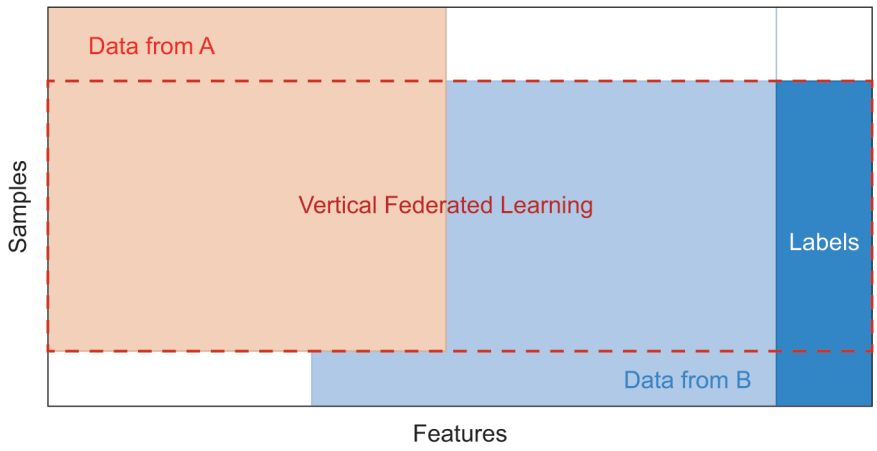

Figure 3—Vertical FML

5.4 Federated transfer learning

Federated Transfer Learning (FTL) refers to the federated machine learning technique designed for application scenarios where data sets have no significant overlap on neither the sample space nor the feature space. FTL takes advantage of transfer learning techniques to exploit reusable knowledge across different feature domains, and consequently, results in high-quality FTL models despite small data and weak supervision difficulties.

See Figure 4.

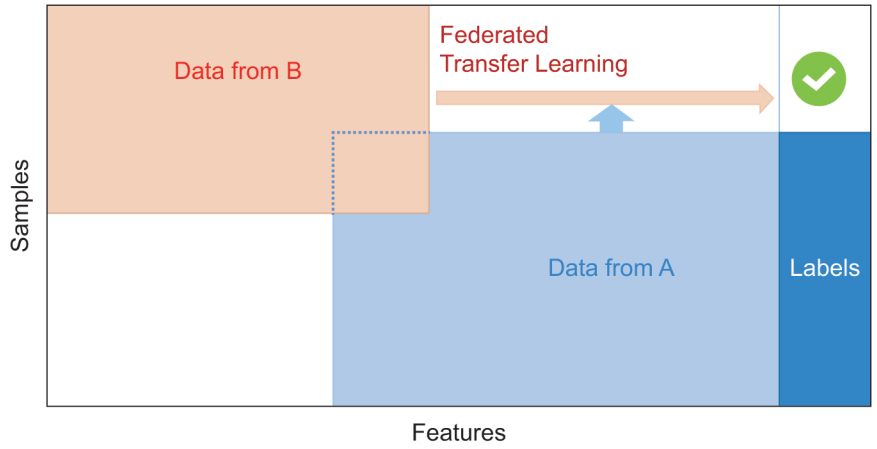

Figure 4—Federated transfer learning

6. FML user view

6.1 Overview

In a federated machine learning framework, users may play any of four roles, namely, the data owners, the model users, the coordinators, and the auditors. The roles are as shown in Figure 5. Note that a user may simultaneously play more than one role.

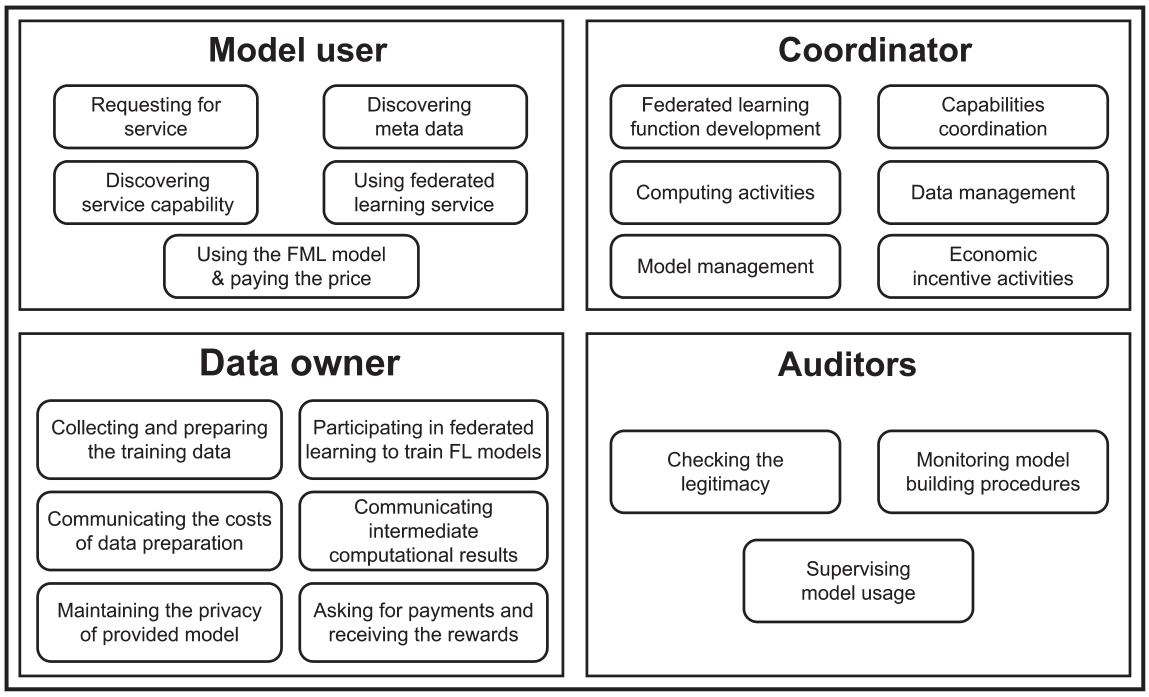

Figure 5—Federated machine learning user roles

6.2 Roles of FML users

6.2.1 Model user

Federated machine learning model users can establish business relations with federated machine learning coordinators. The activities of the model user are as shown in Figure 6, including the following actions:

— Requesting for service
— Discovering metadata of services
— Discovering service capabilities
— Using federated machine learning services
— Using the FML model in inferences and engaging in payment transactions

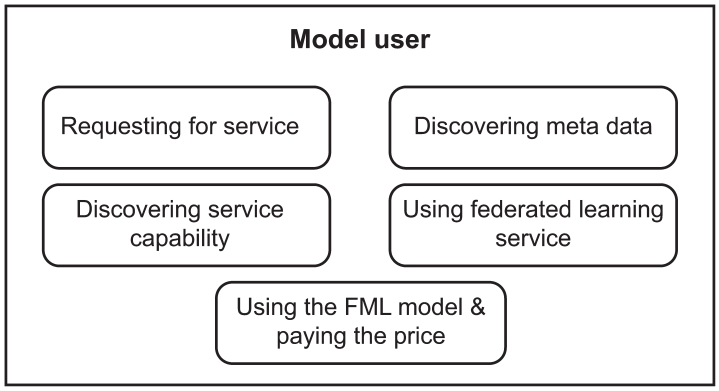

Figure 6—Activities related to learning model users

6.2.2 Data owner

Federated machine learning data owners contribute their data sources for building an FML system. They provide model parts to FML coordinators or to each other in a privacy-preserving manner and receive rewards as a result of these contributions. Activities related to the data owners, as shown in Figure 7, include:

- Collecting and preparing the training data locally
- Communicating the costs of data preparation with other parties
- Maintaining the privacy of the provided model via encryption, homomorphic encryption, differential privacy, secure multi-part computation, etc.
- Participating in federated machine learning to train FML models
- Communicating intermediate computational results with other parties during the fml inference phase
- Asking for payments and receiving the rewards

In FML, the data owners do not transfer the raw data to other parties.

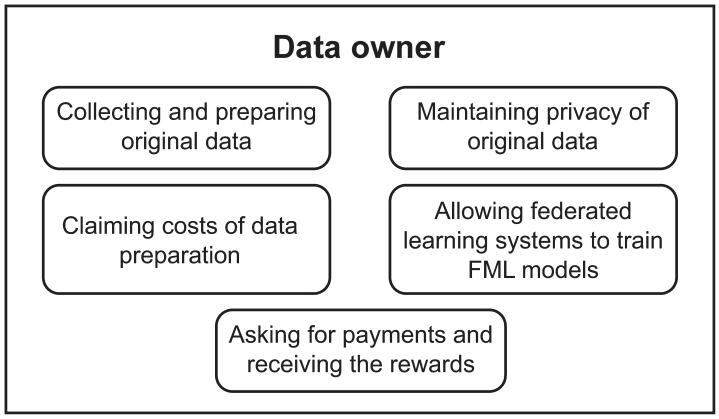

Figure 7—Activities related to the data owner

6.2.3 Coordinator

Federated machine learning coordinators initiate, maintain, and provide FML services for both data owners and model users. The activities related to coordinators, as shown in Figure 8, includes:

- Federated machine learning function development consisting of algorithm development, infrastructure development, service development, etc.
- Computing activities, including model training and testing, secure and privacy-preserving computing management (security protocol determination, key generation, data decryption), and other necessary operations
- Model management consisting of model training and testing, model meta-information management, model key management, etc.
- Model management also consisting of model inferencing when one or more model users initiate requests for applying federated models to their own data, which require sub-models owned by other parties being involved in the computation of FML model outcomes
- Administration activities including service access, service capability announcement, and update, service meta-information management, participant meta-information management, etc.
- Data management consisting of metadata information management, release, discovery, etc.
- Economic incentive activities consisting of calculating the payments to data owners and model users

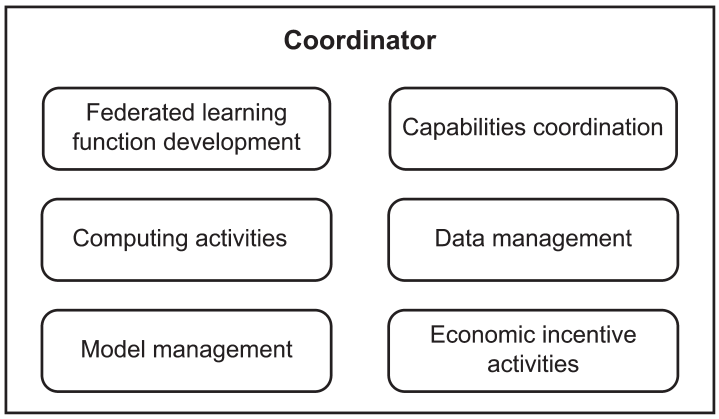

Figure 8—Activities related to coordinators

6.2.4 Auditors

Federated machine learning auditors are responsible for checking the correctness of the FML process and verifying that the process complies with the system constraints in terms of performance and security requirements, as well as regulatory requirements. The activities related to auditors, as shown in Figure 9, may include:

- Verifying the legitimacy of the data sources involved in the FML process
- Monitoring and bookkeeping the model-building processes
- Requesting the coordinators to explain data management, model management, and economic incentive strategies

— Supervising model usage and requesting users to validate model usage requests

— Verifying the existence and adherence to security and privacy procedures and regulations

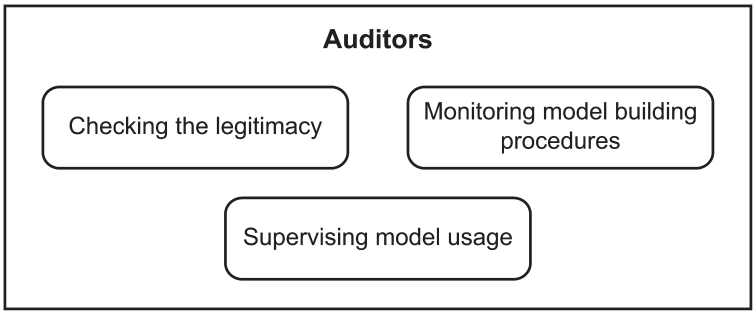

Figure 9—Activities related to Auditors

7. FML system view

7.1 Overview

Figure 10 illustrates a reference hierarchical framework of federated machine learning, in which functional modules define elementary federated machine learning activities. Modules are grouped into layers according to the relevance of their activities, while modules in different layers can interact with each other through cross-layer functions. Note that depending on varying requirements in different use cases, functional modules may be included in or omitted from a specific federated machine learning framework. Note that any FML systems may include one or more modules encapsulated in each layer of the reference framework.

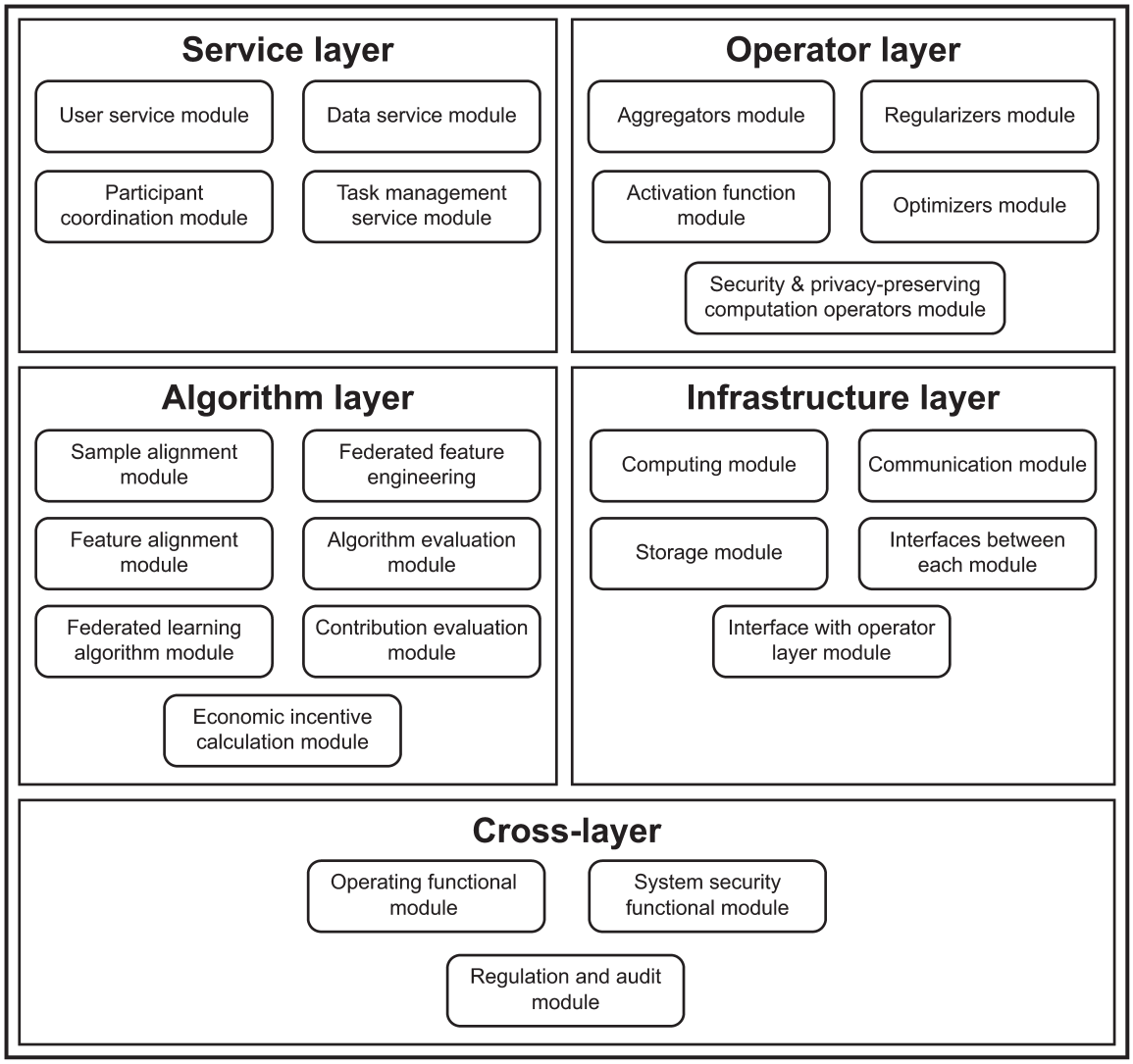

Figure 10—A hierarchical framework of FML

7.2 Service layer

The service layer implements business logic based on service requirements and provides service to federated machine learning users. A service layer includes a user service module, participant coordination module, data service module, and task management service module described in 7.2.1 through 7.2.4.

7.2.1 User service module

A user service module supports federated machine learning users to access and use FML services by providing the following components:

— A user interface, such as command line page, GUI, API, which allow federated machine learning users to interact with available FML services

— A task submission function that allows users to submit requirements of federated machine learning services such as modeling and inferencing

7.2.2 Participant coordination module

A participant coordination module supports the activities of service managers and provides services for federated machine learning users. It should include, but not limited to, following functions:

- A member management function, which provides identity management, authority management, data privacy, and other auditable services
- A monitoring function that monitors the real-time status of federated machine learning systems
- An issue management function, which tracks and reports issues raised in the federated machine learning framework
- A security management function, which improves the security of information of federated machine learning service
- An event management function that provides services for predefined or customized events

7.2.3 Data service module

A data service module provides functions for managing local data repository. It should include, but not limited to, the following functions:

- A set of import/export tools that enable importing/exporting of data or models
- A data release function that facilitates data owners to contribute their data to the learning tasks initiated by other parties
- A metadata management scheme that manages and maintains metadata of raw data
- A data contribution evaluation scheme that evaluates the contribution of raw data
- An optional economic module that evaluates the cost of data owners and the benefit of model users

7.2.4 Task management service module

A task management service module is responsible for the management of FML tasks such as modeling and inferencing. It should include, but not limited to, the following functions:

- A task submitting function that allows any user to create and submit federated machine learning tasks
- A query function that queries federated machine learning task status and logs
- A termination function that handles the ending of federated machine learning tasks
- An error handling function that handles the abnormal termination of federated machine learning tasks, or the time-out task that is not responding within a preset time duration
- A recovery function that enables the recovering of the failed or time-out tasks

7.3 Algorithm layer

The algorithm layer implements federated machine learning algorithmic logics and provides support for the service layer. Activities associated with the algorithm layer are described in 7.3.1 through 7.3.7.

7.3.1 Sample alignment module

A sample alignment module is mainly used for vertical federated machine learning. The module identifies the overlapped samples of different data sources and does not disclose sample feature information.

The module has the following interface:

— INPUT: A list of all sample identifiers in different data sources

— OUTPUT: A list of all overlapped sample identifiers

7.3.2 Feature alignment module

A feature alignment module is mainly used for horizontal federated machine learning. The module identifies the overlapped features of different data sources and does not disclose non-overlapping features and sample IDs.

The module has the following interface:

— INPUT: A list of all feature names in different data sources

— OUTPUT: A list of overlapped feature names in different data sources

7.3.3 Federated feature engineering module

A federated feature engineering module can be used for horizontal and vertical federated machine learning, as well as federated transfer learning. The module identifies overlapped input features and determines a set of new features that are relevant to the learning task.

The module has the following interface:

— INPUT: The data set that is used for feature engineering

  — A list of all overlapped features in data sources

  — A list of identifiers of all overlapped samples in data sources

— OUTPUT: A updated set of features of data sources

Notice that the outcome of feature engineering is dependent on the learning task. Since different applications of federated machine learning algorithms have different requirements for features, this module should be customized according to specific requirements e.g., for time-domain features, space domain features, and frequency domain features, etc.

7.3.4 Federated machine learning algorithm module

A federated machine learning algorithm module covers all kinds of basic algorithms needed by federated machine learning for different application scenarios or tasks. It should include, but not be limited to, the following algorithms:

— A set of federated machine learning algorithms that can be used in supervised learning, semi-supervised learning, and unsupervised learning scenarios, e.g., tree-based algorithms, deep learning algorithms [B22], linear learning algorithms of federated machine learning.

The module has the following interface:

— INPUT: the data sets that are used for federated machine learning

  — A list of all overlapped features in the data sets, a list of all overlapped samples in the data sets, a set of hyper-parameters controlling the learning algorithm

— OUTPUT: (part of) the learned FML model

Notice that there is a diversity of FML models, such as trees and neural networks, that should be supported by the federated machine learning algorithm module.

7.3.5 Algorithm evaluation module

An algorithm evaluation module should evaluate federated machine learning models according to various evaluation measures. Refer to Clause 9 for details. The module should include, but not be limited to, the following measures:

— Performance evaluation
— Efficiency evaluation
— Privacy-preserving evaluation
— Security evaluation

The module has the following interface:

— INPUT: The learned FML model
  — The testing data set that is used to evaluate the FML model
  — A list of all overlapped features in the testing data set
— OUTPUT: A list of evaluation results (performance, efficiency, security and privacy, etc.)

7.3.6 Contribution evaluation module

A contribution evaluation module should evaluate the contribution to the overall performance of the FML model provided by each owner's raw data.

The module has the following interface:

— INPUT: The training data sets from all data owners
  — The testing data set that is used to evaluate the contributions
  — A list of all overlapped features in the data sets
  — A list of all overlapped samples in the training data sets
  — The hyper-parameters controlling the learning algorithm
  — The used federated machine learning algorithm
— Output: A list of scores indicating the contributions of all data owners

Notice that the outcome of this module should assist in interpreting the decision-making logic of the FML model and indicate the contributions made by each owner's raw data. The outcome should also facilitate the investigation of the root causes of underlying problems.

7.3.7 Economic incentive calculation module

An economic incentive calculation module should calculate the payments to participants. If included, then this module should have the following outputs:

a) The payoff to each data owner

b) The payoff to each model user

The inputs should include the effective data provided by each data owner. Moreover, the metrics of assessing the inputs and output are referred to 9.5.

7.4 Operator layer

The operator layer provides elementary operations that are needed by federated machine learning algorithms, despite the large variety of learning algorithms. The layer should enable algorithm developers to implement a federated machine learning algorithm rapidly based on these operators. Operators include, but are not limited to the following:

— Secure and privacy-preserving computation operators, which provide one or more implementations of secure and privacy-preserving computations

— Aggregators that aggregate sub-models of respective data owners

— Activation operators that provide the common implementation of activation functions

— Regularizer operators that provide the common implementation of regularizers

— Optimization module that provides the common implementation of optimization methods

7.4.1 Aggregators module

Aggregators should support the well-established aggregation methods, e.g., [B7], but should also be customized according to the aggregation strategy and encryption mode. It is expected that aggregators adhere to the secure and privacy-preserving principle, which prevents leakage of private information.

7.4.2 Activation module

Activation functions should include, but not be limited to, the following:

— Activation functions adopted in traditional machine learning, such as sigmoid, SoftMax, tanh, softsign

— Federated activation functions, such as Taylor expansion sigmoid, based on semi-homomorphic encryption and ReLU based on secret sharing [B12]

7.4.3 Regularization module

Regularizers should include, but not limited to, the following:

— Regularizers of traditional machine learning, such as L1, L2, etc.

— Federated regularizers of federated machine learning, such as Taylor L1 sigmoid based on semi-homomorphic encryption, and Taylor L2 sigmoid based on semi-homomorphic encryption [B12]

7.4.4 Optimization module

An optimization module provides the common implementation of the optimization methods for increasing the performance of an FML model. The optimization methods contain loss functions, optimizers, and gradient processors.

Loss function should include, but not limited to, the following:

- Loss functions of traditional machine learning, such as Cross Entropy, Mean Squared Error, and Mean Absolute Error
- Federated loss functions of federated machine learning, such as Cross Entropy of dichotomies based on semi homomorphic encryption

Optimizers should include, but not limited to, the following:

- Optimizers of traditional machine learning, such as SGD, RMSProp, AdaGrad, Adam
- Federated optimizers of federated machine learning

Gradient processors should include, but not limited to, the following:

- Gradient processors of traditional machine learning
- Federated gradient processors of federated machine learning

7.4.5 Computation operator

The basic principle of secure and privacy-preserving computation operator should include, but not limited to, the following:

- The encryption or desensitization modules of the participant process data using algorithm supported by other participants and coordinators, and remove information related to the original data
- The coordinators take responsibility for encryption, decipherment, and key management, as well as transferring results to relevant parties
- The coordinators take responsibility for preventing the inference of the private data from the information exchanged during computation

The implementation methods of secure and privacy-preserving computation operator should include, but not limited to, one of or the combination of the following methods:

- Homomorphic encryption
- Secret sharing
- Oblivious transfer
- Garbled circuit
- RSA encryption algorithm with short or long-byte data
- Consensus algorithms with obfuscation
- Differential privacy

General secure and privacy-preserving computation operators include the following:

— Arithmetic operator
— Size comparing operator
— Logical and/or/ not operator
— Vector calculation operator

7.5 Infrastructure layer

The infrastructure layer provides capabilities of computing, storage, and communication of long-byte encrypted data units (e.g., 1024 bits) for the operator layer of federated machine learning frameworks. The infrastructure layer supports all the functions needed by traditional machine learning. In addition, it includes the following components and interfaces to support special functions needed by federated machine learning:

— A computing component that provides capabilities of long-byte data unit computing operations
— A storage component, which provides capabilities of long-byte data unit storing operations to store the encrypted output model and intermediate data, and encrypted data import and export operations, etc.
— A communication component that provides capabilities of long-byte data unit communication operations. It supports a large magnitude of data communication workload (e.g., 1 or 2 magnitudes higher than traditional distributed ML), and both iterative inter-datacenter and intra-datacenter communication
— Interfaces between each component, which provide capabilities of long-byte encrypted data unit transmission and short-byte plain data unit (e.g., 8 bits) transmission
— An interface with the operator layer, which provides capabilities of long-byte encrypted data unit transmission

7.5.1 Computing component

Computing components include functions of the following:

— Providing services of long-byte data unit computing operations in federated machine learning.
— Providing a clear FML task meta-information management scheme to monitor the normal running of federated machine learning activities. The FML-task meta-information management scheme includes FML-service meta computing information management, FML-participant meta computing information management and FML-model meta computing information management, etc.
— Providing APIs for developing federated machine learning algorithms in computing aspects, such as providing handles of computing resources for federated machine learning applications to reference and to operate on.

7.5.2 Storage component

Storage components include functions of the following:

— Providing services of long-byte data unit storage operations in federated machine learning, such as long-byte data import and export from other storage systems to storage components.
— Having a clear FML-task meta-information management scheme to monitor the normal running of federated machine learning activities. The FML-task meta-information management scheme includes

FML service meta storage information management, FML participant meta storage information management and FML -model meta storage information management, etc.

— Providing APIs with abilities of storage components access.

7.5.3 Communication component

Communication components include functions of the following:

— Providing services of long-byte data unit communication operations in federated machine learning, such as iterative inter-datacenter and intra-datacenter communication operations, etc.

— Providing services to support the large magnitude of data communication workload (e.g., 1 or 2 magnitudes higher than traditional distributed machine learning).

— Having a clear FML task meta-information management scheme to monitor the normal running of federated machine learning activities. The FML task meta-information management scheme includes FML-service meta-communication information management, FML-participant meta-communication information management, and FML model meta-communication information management, etc.

— Providing APIs with abilities of federated machine learning algorithm development.

7.5.4 Interfaces between each component

The interfaces between each component transmit the following:

— Short-byte plain data (e.g., 8 bits) from/to other hosts in common federated machine learning participants

— Long-byte encrypted data from/to other federated machine learning participants or coordinators, and short-byte plain data (e.g., 8 bits) from/to other hosts in common federated machine learning participants

7.5.5 Interfaces with operator layer

The interfaces with operator layer transmit the following:

— Metadata and parameters of federated machine learning tasks, and requests from operators and feedbacks from each component for federated machine learning tasks. The feedbacks from each component may be in either long-byte encrypted data form or short-byte plain data form (e.g., 8 bits).

7.6 Cross-layer module

Cross-layer function interacts with modules of the service layer, algorithm layer, operator layer, and infrastructure layer to offer supporting capabilities, including but not limited to, operational function, system security function, monitoring, and evaluation function.

7.6.1 Operating functional module

Operating functional modules include, but are not limited to, the following:

— A service catalog that provides lists of all the services of the federated machine learning system

— A strategy management function, which provides definitions, update and accessing strategy of federated machine learning service, and management of strategies

— An exception and problem management function that provides abilities to capture incidents and problem reports

— A service delivery management function that provides management functions of service delivery such as functional interfaces of delivery

7.6.2 System security functional module

System security functional modules mainly provide guarantees of security attributes such as confidentiality, integrity, availability, and privacy protection for each functional layer, layer interactions, and each participant including, but not limited to, the following:

— An account management function that verifies that all relevant parties have their own accounts

— An authentication management function that verifies relevant parties be authenticated and act in their own capacity

— An authorization and security policy management function, which verifies that the relevant party can only operate on the authorized content

— A data integrity management function, which prevents data integrity damage caused by misoperation and malicious damage by integrity testing and various specification requirements

— A data destruction function that is responsible for completely deleting the data to avoid information leakage

— A privacy divulgence protection function that protects sensitive information from leakage or illegal access so that information can only be accessed with full authorization.

7.6.3 Regulation and audit module

Regulation and audit modules make services regulable and auditable to avoid privacy exposure based on the governance requirements of the federated machine learning participants. They work as the authority to determine whether the training prediction process, the final model, and other indicators meet the following requirements:

— Having a sound and perfect regulatory governance system

— Implementing the real-time supervision of regulators as federated members

— Setting clear regulatory governance rules

— Storing audit information related to service, resource and performance

8. Common concerns

8.1 Overview

There are concerns about privacy and security, model performance efficiency, and economic viability that federated machine learning users should take into account. These common concerns of federated machine learning are shown in Figure 11 and elaborated in this clause.

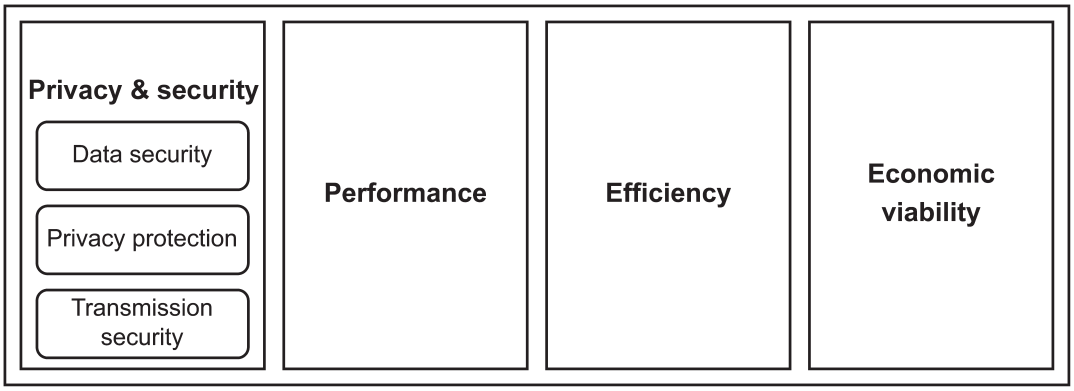

Figure 11—FML common concern

8.2 Privacy and security

Adhering to the privacy and security principles posed by both the ethical and regulatory requirements, this standard aims to provide a guide for the design, development, and implementation of federated machine learning frameworks. It should also be used as a baseline in the monitoring and measurement of performance, benchmarking, and auditing aspects of privacy and security management programs of a federated machine learning system.

8.2.1 Data privacy

Adhering to the privacy principle means:

— A federated machine learning system should avoid information leakage. The information received from the sub-models does not leak the source data information, and attackers cannot infer the participants' information by eavesdropping gradient during the training or inference stages.

Secure computation methods including, but not limited to, homomorphic encryption and partial-homomorphic encryption should be considered for preserving data privacy.

8.2.2 Security

Adhering to the security principle means the following:

— A federated machine learning model should be sufficiently robust to defend malicious attacks, such as testing time adversarial examples and training time data poisoning.

— A federated machine learning model should be robust to other threats such as backdoor attacks, which aim to induce the model overfitting to backdoor patterns that trigger misjudgment or misbehaviors of federated machine learning models.

8.2.3 Transmission security

Adhering to the transmission security means the following:

— No private information about raw data and model parameters are tampered or disclosed under transferring procedure. Attackers cannot infer private information even if they captured the transferred data.

Any other type of encryption methods (includes SSL, TLS, OPE) that can prevent transmission threats should be considered.

8.3 Efficiency

Adhering to the computational and communicational efficiency means:

- An FML algorithm should be analyzed to determine its resource usage so that the user of the algorithm can have an early estimate of the possible overhead and be aware of appropriate resources.
- The design of the algorithm concerning the amount of data transferred and the computational logic utilized should be optimized according to the use case requirements.
- An FML algorithm is deemed efficient if its resource consumption, or computational cost, is at or below some acceptable level.

Benchmarks can be used to assist with gauging an algorithm's relative performance. Refer to 9.3. for the elaboration of efficiency evaluation.

8.4 Economic viability

8.4.1 Economic objectives

Beyond data security and privacy preserving consideration, FML may need to economically incentivize users to join and stay in the federation. The economic incentive calculation module, as defined in 7.3.7, determines how to reward contributions made by federated machine learning users, e.g., data owners. The objectives of this module include keeping all participants in the federation (individual rationality), leading to a nonnegative profit for the coordinator (weak budget balance), maximization of the total utilities of all data owners (Pareto efficiency), incentivizing data owners to provide all their data (incentive compatibility), and equal unit price of effective data (fairness).

Note that it is hard to attain all these objectives simultaneously. Depending on different use cases, FML coordinators should choose one or more objectives to optimize. The attainment of these objectives should be quantified by measures in 9.5.

8.4.2 Economic settings

In order to attain economic viability, the FML system should adopt an appropriate economic incentive scheme which should include the following functions:

- Assessing the quantity of increased performance of the model by a new data set
- Rewarding data owners with its contribution to the performance of the model
- Charging model users according to their usage of the federated model
- Evaluating the cost of each data owner for collecting a data set

Furthermore, the FML coordinator, who is in charge of designing appropriate incentive schemes, should take into consideration a set of economic settings that may have influences on the attainment of economic objectives.

Information asymmetry: The FML coordinator cannot verify whether or not the data owners contribute all their data to federated machine learning; neither can it verify the true cost incurred by data owners. The FML coordinator should consider such information asymmetry.

Incomplete information: In some use cases, the FML coordinator may be uncertain about the future revenue of the federated model. Data owners may be uncertain about their own costs for collecting data. Model users may be uncertain about the potential usefulness of the federated model. Such incomplete information should be taken into consideration.

Dynamic system evolution: In some use cases, the FML coordinator allows users to join or leave the federation dynamically. For these use cases, the incentive scheme should also be dynamic.

Information updates: FML users are rational individuals who game with the FML coordinator. As time goes on, FML users may obtain new information that may cause them to change their evaluations of economic incentives. Such information updates may change the behaviors of the users.

9. Performance evaluation

9.1 Overview

A performance evaluation scheme is introduced to confirm the conformance of the performance of Federated machine learning ecosystems and algorithms. The performance evaluation scheme allows an FML system to be evaluated by using specific metrics, which are widely adopted by academic and industrial researches, concerning efficiency, security as well as the performance of FML systems (see [B13], [B10], [B19]). Notice that measures specified in this clause are not exclusive and more testing specifications can be made for different settings of influential factors described in 9.4.5.

9.2 Privacy and security

An FML system is considered privacy-preserving if it can effectively defense leakage attacks which aim to uncover or inference private FML data. The severity of leakage attacks should be evaluated according to the following measures, namely:

— The extent of leakage: The amount of data being disclosed, e.g., measured by byte, with respect to the amount of information of original private data. This ratio ranges from 0.0 to 1.0. Optionally, the differences between the disclosed data and the original data, measured by Mean Squared Error (MSE) may be used to quantify the extent of leakage, e.g., as in [B22].

— The influence of leakage: The probability of private information, such as personal identity, being inferred from the disclosed data.

For the sake of privacy-preserving, it is required both the extent of leakage and the probability of privacy disclosing be lower than certain acceptable levels. The specification of acceptable levels is application dependent; refer to A.2 for examples.

An FML system is considered arrack-proof if it can effectively defend attacks that aim to tamper the behaviors of FML models, by either generating adversarial samples (both training or testing) or implanting backdoors into the system.

The severity of FML attacks should be evaluated according to the following measures, namely:

— The extent of alternation: The amount of data or models being altered, e.g., measured by byte, with respect to the amount of information of unaltered data or models. This ratio ranges from 0.0 to 1.0.

— The influence of alternation: The change of model performances, with respect to the model performances with unaltered data or models. This ratio ranges between 0.0 to 1.0, and optionally, may be weighted or normalized by the significance of consequences.

The level of FML system security, in the face of data or model poisoning attacks, should be evaluated by the above measures, with 0.0 indicating an absolute secure FML system and 1.0 indicating an endangered one. An absolute secure FML system is often required in many application scenarios; refer to A.2 for a summary.

Implementations of FML systems in different use cases may require varying acceptable levels of security and privacy-preserving. Implementers should document how these acceptable levels are determined in different cases. Refer to [B22] and [B4] for examples of acceptable levels.

9.3 Model performance

Adhering to the quality principle means verifying that federated machine learning systems are well-behaved, up-to-date, adequate, and relevant for the purpose of use. It is, therefore, mandatory to establish evaluation mechanisms and periodically check the performance and quality of FML models through appropriate means.

FML models are expected to achieve an equivalent or more competitive performance to that of a data-centralized model, which is a model trained on the data collected from all parties. The difference, denoted as FML model performance discrepancy, between FML model performance with respect to that of the data-centralized model, should be evaluated as described in 9.3.1.

9.3.1 FML model performance discrepancy

The process for evaluating model performance discrepancy is dependent on the selection of appropriate methods and metrics according to tasks. Model performances in varying applications may be measured in terms of accuracy, precision, recall, image quality, or any other measures relevant to application tasks. Regardless of the underlying performance measures used, nevertheless, the model performance discrepancy is a key factor that is widely applicable to quantify the differences between two models of interests.

For example, in the context of classification, the FML model performance discrepancy, i.e., Acc_{disc} illustrated in Figure 12, is measured by the distance between an FML model accuracy and that of a data-centralized model, i.e., $Acc_{disc} = Acc_{cent} - Acc_{fed}$. Whereas in other applications, the discrepancy of model performances may be quantified by different measures, e.g., the distance between ROC curves, or divergences between probability distributions associated with FML and data-centralized models.

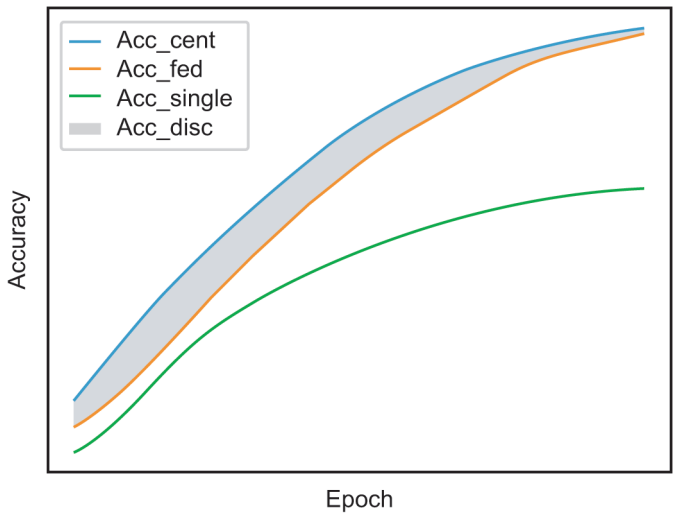

Figure 12—FML model accuracy distance (i.e., the gray area between learning curves of Acc_{cent} and Acc_{fed})

9.4 Computation efficiency

An FML algorithm is considered efficient if it takes a reasonable amount of time or consumes an acceptable amount of memory space on hardware. After an FML algorithm is initiated, FML efficiency should be evaluated according to commonly used measures as follows:

— Training time
— Testing time
— Intrinsic memory usage
— Auxiliary memory usage

9.4.1 Training time

Training time (T_{train}) illustrated in Figure 13 describes the efficiency of an FML system to complete the training process. T_{train} is measured by the duration between the starting and ending of a training session, i.e., $T_{train} = t_{end} - t_{start}$. The training time increases, proportionally, as the size of the data set increases. Normalized training time should discount the influence of data set size, by dividing the training time by the number of training samples, i.e., $T_{train\_norm} = \frac{T_{train}}{\#Num_{train}}$.

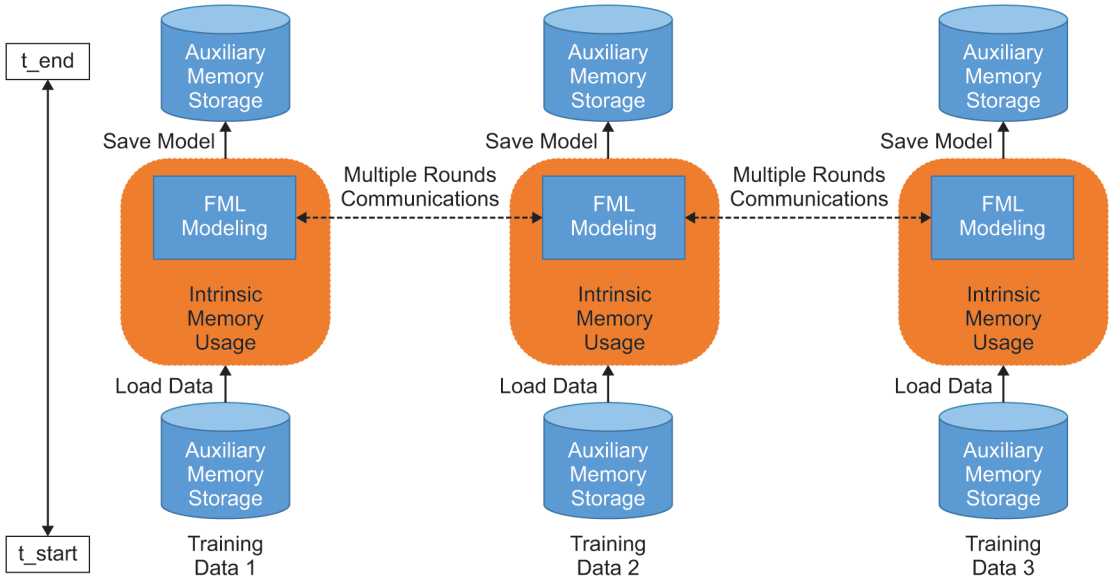

Figure 13—Training time

9.4.2 Testing time

Testing time (T_{test}) illustrated in Figure 14 describes the efficiency of an FML system to complete the testing process. T_{test} is measured by the duration between the starting and ending of a testing session, i.e., $T_{test} = t_{end} - t_{start}$. The testing time increases, proportionally, as the size of the data set increases. Normalized testing time should discount the influence of data set size, by dividing the testing time by the number of testing samples, i.e., $T_{test\_norm} = \frac{T_{test}}{\#Num_{test}}$.

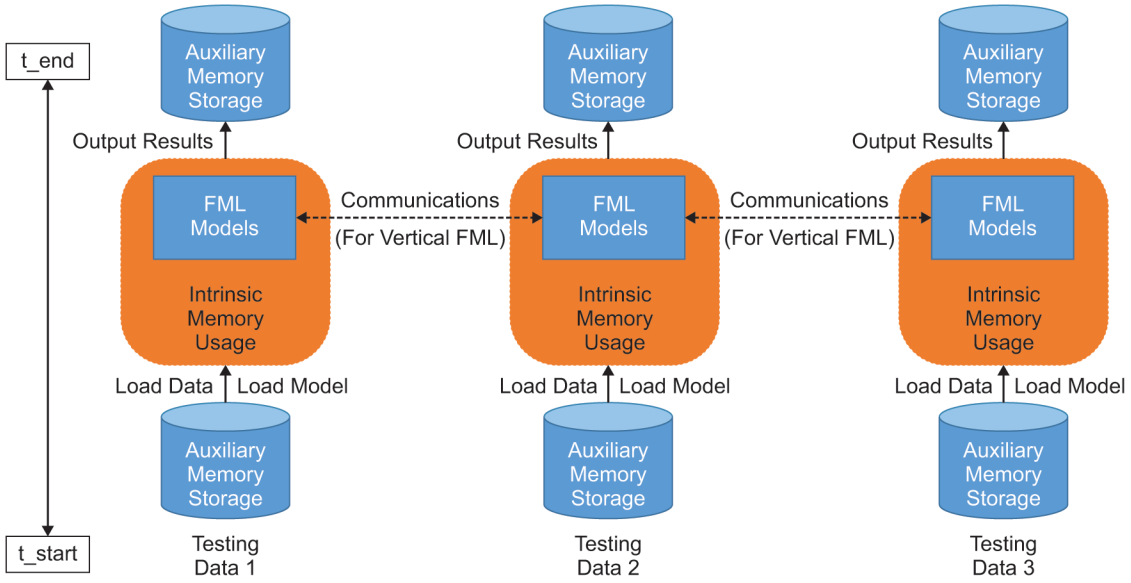

Figure 14—Testing time

9.4.3 Intrinsic memory usage

The intrinsic memory usage (M_{intr}) quantifies the amount of memory needed for the data on which the code operates as shown in Figure 14.

9.4.4 Auxiliary memory usage

The auxiliary memory usage (M_{aux}) quantifies the amount of memory needed by the code, as shown in Figure 14.

9.4.5 Factors concerning efficiency

The evaluation of FML algorithm efficiency should take into consideration of the following aspects:

a) Roles and structure:
   1) When evaluating the FML algorithm, the entire framework structure should be explained.
   2) The evaluation of an algorithm should be organized by roles or tasks, as described in 6.2.

b) Data set:
   1) For each participant, the data set it owns should be described.
   2) For horizontal FML models, the sample size of the data set, or the batch sizes, should be recorded.
   3) For vertical models, the number of features and the feature data types in each platform should be specified.

c) Hardware:
   1) The hardware information, including the number of servers, CPUs, GPUs, memory, and storage, should be elaborated.
   2) For edge devices including phones, home terminal devices, remote cameras, etc., the cost of battery energy and network resources should be specified as well.

d) Implementation:

1) The choice of programming language, the choice of a compiler, the compilation options, and the operating system used should be specified.

2) Other factors that may affect training/testing time and memory consumption include data alignment, data granularity, cache locality, cache coherency, garbage collection, instruction-level parallelism, multithreading, simultaneous multitasking, and subroutine calls.

e) Encryption and decryption:

1) Encryption and decryption, significantly, increase computational complexity and the required memory space. The choice of encryption/decryption algorithms, as well as the parameter settings should be specified, when reporting the training/testing time and required memory.

f) Communication efficiency:

1) The communication efficiency depends on both the hardware and network capability. Specifically, data size, bandwidth, network topology, firewall, switch, and network types should be specified when evaluating the communication efficiency in FML.

g) Deployment:

1) Deployment techniques like virtual machines and containers, etc., are commonly used in the data center. There are some factors about the deployment techniques which should be considered for FML.

i) Make sure that the host machine of a virtual machine/container using FML data is physically attack-proof; FML data could be transferred to another host machine which should be physically attack-proof and adhere to the regulatory requirements;

ii) Special hardware might be used for computation acceleration, encryption/decryption, compression, etc. in the FML framework. When these workloads with special hardware are deployed on virtual machine/container, hardware efficiency, compatibility, robustness, and shareability should be considered.

9.5 Economic viability

Federated machine learning is an economic process, whereas the federated models are utilized to provide various services to model users. Once an FML task is accomplished, in order to maintain the economic sustainability of the federation, the coordinator should transfer monetary payments from model users to data owners. Depending on the application scenarios, economic viability should be evaluated according to one or more measures as outlined in 9.5.1 through 9.5.5.

9.5.1 Individual rationality index (IRI)

Individual rationality requires that the payments to each data owner can cover their respective individual cost of providing data. Rational data owners are not expected to stay in the federation if their costs cannot be covered by payments.

The individual rationality indicator IR_i for data owner *i* is defined as follows:

IR_i=1 if it is beneficial for data owner *i* to stay in the federation and 0 elsewise.

For business entities, it is beneficial to stay in the federation when $p_i - c_i \geq 0$. For non-profit entities, the criteria may be different.

The ideal case is that the payment scheme satisfies individual rationality for all participants. For general cases, we measure the average of individual rationality indicators. For example:

Individual rationality index $IRI = \left(\sum^{N} w_i\right) \times IR_i$, where w_i is a user-defined weight for the relative importance of data owner *I*, e.g., $w_i = \frac{d_i}{D}$, where d_i and D denote the effective data owned by data owner *i* and $D = \sum_{i}^{N} d_i$.

The individual rationality index varies from 0.0 to 1.0, with 1.0 indicating individual rationality constraints satisfied for all participants.

9.5.2 Budget surplus margin (BSM)

The budget surplus is the difference between the total revenue received from model users and the total payments paid to data owners. In practice, the budget surplus can be the profit made by the coordinator. Budget surplus margin is the ratio of the budget surplus to total revenue of the federation. For example:

$$Budget\ surplus\ margin\ = \frac{\left(total\ revenue\ received\ from\ model\ users - total\ payments\ paid\ to\ data\ owners\right)}{total\ revenue\ received\ from\ model\ users}$$

The budget surplus margin varies from -infinity to 1.0, with 0.0 indicating a break-even point, and positive/negative values indicating net profits/loss, respectively.

9.5.3 Efficiency Index (EI)

In federated machine learning, Pareto efficiency is achieved if it is impossible to reallocate economic resources to make any data owner better off without making at least one data owner worse off. Pareto efficiency is achieved when the social surplus, defined as the total federation revenue minus the total costs of data owners, is maximized over all possible behaviors of data owners. For example:

$$Social\ surplus\ = federation\ revenue - the\ total\ cost\ of\ data\ owners$$

The efficiency index is the ratio of realized social surplus to the maximum possible social surplus when all data owners selflessly cooperate.

$$Efficiency\ Index\ = realized\ social\ surplus / maximum\ social\ surplus$$

The efficiency index varies from -infinity to 10, with 1.0 indicating the Pareto efficiency.

9.5.4 Data offering rate (DOR)

In FML, it is desired that data owners offer all their data to the federation, although the federation may reject some of the offered data. The data offering rate is defined as the total data offered by all data owners to the total data owned by all data owners.

$$Data\ offering\ rate\ = \frac{total\ effective\ data\ offered\ by\ all\ data\ owners}{total\ effective\ data\ owned\ by\ all\ data\ owners}$$

A payment scheme is called incentive-compatible if it incentivizes all data owners to offer all their data to the federation. When a payment scheme is incentive-compatible, the data offering rate is 1.0.

The data offering rate varies from 0.0 to 1.0, with 1.0 indicating all data being offered.

9.5.5 Fairness Index (FI)

In FML, it is desired that the payment of a unit of effective data to be the same for all data owners. The normalized unit price of effective data for data owner *i* is as follows:

$$normalized\ unit\ price_i = \frac{payment\ to\ data\ owner\ i\ /\ effective\ data\ provided\ by\ data\ owner\ i}{total\ payment\ to\ all\ data\ owners\ /\ total\ effective\ data\ provided\ by\ all\ data\ owners}$$

Such a normalized unit price is invariant with the change of measure.

The fairness index is the variance of the normalized unit price across all data owners, rescaled to [0.0, 1.0].

$$Fairness\ index\ = \frac{1}{1+\ Var\ \left(normalized\ unit\ price_i\right)}$$

The fairness index varies from 0.0 to 1.0, with 1.0 indicating the absolute fairness.

9.6 Data sets

When evaluating the FML algorithm, the quality and the format of data sets should be examined.

9.6.1 Data quality

Data quality can be examined in terms of the following measures:

— Sparsity: If a data set is distributed too sparsely at different locations, for example, each location only contains several samples while the total number of locations is large, then this data set should be considered not suitable for FML, due to the overheads of communications.

— Skewness: For horizontal FML, a data set should be considered in bad quality if the number of samples on each device is highly skewed, as data skewness will lead to imbalanced training time on different devices. For vertical FML, similar to horizontal FML, a data set should be considered in bad quality if the number of features on each device is highly skewed. This may cause imbalanced training time as well.

— Distribution: It is recommended that data from different sources should be independent and identical distributed. Non-I.I.D. of data sets should also be used to simulate real-world use cases, in which non-I.I.D. data sets are often presented.

— Data number: The data set should be reasonably large enough to produce statistically significant meaning and satisfy the purpose of the FML modeling.

9.6.2 Other related issues

Apart from data quality, issues related to data sets include the following:

— Structured data: Structured data refers to a data set that each sample can be represented by an identical group of features. To use structured data for training in FML, apart from feature columns and the label column, a column of unique sample IDs that can globally determine and match samples should be included in each data file, no matter in horizontal or vertical FML. Furthermore, the first row of submitted data files should always be table headers.

— Image data: To use image data for training in FML, a column of image addresses, either in local or file systems, and a column of the label should be provided in data files.

— Text data: When using text data to train the FML model, the data files from all partitions should include three columns such as ID, text data, and label.

Annex A

(informative)

Use cases and requirements

A.1 Introduction

Application domains showcased in this annex are both diverse and representative, providing an overview of the wide applicability of a federated machine learning framework. Refer to Table A.1 for a summary of application use cases.

A.2 General

The application and commercialization of federated machine learning in the industry include different use cases, which have different features of the federated machine learning function. Federated machine learning application areas are broadly categorized as three types, according to requirements from different marketing sectors, i.e., business-to-consumer (B2C), business-to-business (B2B), and business-to-government (B2G). Requirements for each application type are summarized in Table A.1, in terms of use cases, efficiency, security, accuracy, and efficiency requirements in FML applications. Notice that, for each use case in Table A.1, the specified requirements are made under assumptions of specific settings, which may be adapted for a range of influential factors described in 9.4.5.

Table A.1—Requirements for applications

Use case type	Use cases	Efficiency requirements				Security requirements	Privacy requirements	Model performance requirements	Economic viability requirements
		Training time	Testing time	Intrinsic memory usage	Auxiliary memory usage				
B2B	Finance	0	3	2	2	4	2	3	IRI: Y BSM: Y EI: Y DOR: Y FI: Y
	Health	0	0, 1 *	2	2	4	2	2	IRI: Y BSM: Y EI: Y DOR: Y FI: Y
	Marketing	1	1	2	2	4	2	2	IRI: Y BSM: Y EI: Y DOR: Y FI: Y

Table continues

Table A.1—Requirements for applications *(continued)*

Use case type	Use cases	Efficiency requirements				Security requirements	Privacy requirements	Model performance requirements	Economic viability requirements
		Training time	Testing time	Intrinsic memory usage	Auxiliary memory usage				
B2G	Government governance	0	2	2	2	4	2	2	IRI: N(G), Y(B) BSM: Y EI: Y DOR: Y FI: Y
	Government Services	0	3	2	2	4	2	3	IRI: Y BSM: Y EI: Y DOR: Y FI: Y
	Urban Computing	0	2	2	2	4	2	3	IRI: Y BSM: Y EI: Y DOR: Y FI: Y
B2C	Telecom.	2	3	3	3	4	2	3	IRI: Y BSM: Y EI: Y DOR: Y FI: Y
	Education	3	3	2	2	3	3	4	IRI: Y BSM: Y EI: Y DOR: Y FI: Y
	Internet of Thing (IOT)	0	1	2	2	3	2	2	IRI: Y BSM: Y EI: Y DOR: Y FI: Y

*0 for testing of clinical applications, and 1 for other applications. (G): Government, (B): Business

Table A.2—Security requirements level

Security requirement level	Requirements
0	No corresponding plans for potential attacks
1	Successfully defending read-write attack for a model on a central server
2	Successfully defending data recovery for channel monitoring
3	Successfully defending data recovery for read-write attacks database and channel monitoring
4	Successfully defending model controlling based on 1–3 attacks.

Table A.3—Privacy requirements level

Privacy requirement level	Requirements
0	No defending ability
1	Successfully defending leakage during transferring
2	Successfully defending database and aggregator leakage

Table A.4—Model performance requirement level

Model accuracy requirement level	Requirements
0	Achieving an equivalent or more competitive performance to that of a single-data-node model
1	Achieving a performance with noticeable deterioration compared to that of a data-centralized model
2	Achieving a performance with insignificant deterioration compared to that of a data-centralized model
3	Achieving an equivalent or more competitive performance to that of a data-centralized model

Table A.5—Time efficiency requirements level

Time efficiency requirement level	Requirements
0	Supporting completion in the order of weeks
1	Supporting completion in the order of days
2	Supporting completion in the order of hours
3	Supporting completion in minutes or seconds

Table A.6—Memory efficiency requirements level

Memory efficiency requirement level	Requirements
0	Supporting computations on super-computing clusters
1	Supporting computations on high-performance single-node machines
2	Supporting computations on ordinary computing power servers
3	Supporting computations on edge devices

A.3 Finance

Finance or financial services is an important area that can be greatly improved with the use of AI and big data. Traditionally financial companies or banks make business decisions based on their own data, such as information of bank account, credit card use, and loan history, which might be insufficient to evaluate customers' financial risks because these data only present a small part of user behavior needed for risk modeling. In contrast, customers' yearly income, real estate situation, and shopping history may provide more valuable information, but these are the private information of users that need to be protected. In financial application scenarios, regulatory requirements and privacy concerns prevent banks and financial companies from sharing their own data.

Using federated machine learning techniques, banks and financial services can build secure and privacy-preserving machine-learning models in tandem with companies and organizations such as e-commerce service providers that have broader data such as the customers' shopping history data. These data can assist banks to better assess the financial risks of potential customers.

In the finance sector, FML can be conducted with two partnering businesses. FML applications in finance are typically business-to-business (B2B) use cases.

A.3.1 Role design

The role design in this case may include the following:

— Data owner: The participants of model development with data about finance, social network, consumption, credit, etc.

— Model user: The financial service providers (business companies, banks, and etc.) who make use of federated machine learning models

— Coordinator: The FML service provider that builds FML models from different data owners and provides FML models to model users

— Auditor: The government regulators and the compliance department of the coordinator, data owner, or model user

It might be possible that the roles of coordinator, data owner, and the model user are played by the same organization.

A.3.2 Main activities of each role

The main activities of data owners are as follows:

— Collecting and preparing original finance-related data

— Claiming costs of data preparation

— Maintaining the privacy of the raw data

— Allowing federated machine learning systems to train finance-related FML models

— Asking for payments and receiving the rewards

— Communicating intermediate computational results with other parties during the FML inference phase

The main activities of module users are as follows:

— Requesting for service

— Discovering service capability

— Using federated machine learning service for the finance-related purpose

— Discovering meta-data

— Using the FML model for finance-related purpose and paying the price

The main activities of coordinator are as follows:

— Federated machine learning function development includes financial algorithm development, infrastructure development, service development, etc.

— FML computing activities include starting modeling, encrypted computing management (security protocol determination, key generation, data encryption, and decryption), etc.

— Computing activities include starting modeling, participating in modeling, matching the same clients, building, transferring and receiving secure encryption computing protocol, data encryption and decryption, etc.

— FML model management includes financial model discovering, sub-model meta-information management, sub-model composition, and model key management.

— Capabilities coordination includes service access, service ability release, service meta-information management, participant meta-information management, etc.

— Data management includes meta-data information management, release, and discovery.

— Economic incentive activities include calculating the payments to data owners and model users.

The main activities of auditor are as follows:

— Auditors have the responsibility to check the legitimacy of the data sets used to make sure that they are obtained legally.

— Monitoring the model building procedures; auditors can request the coordinator to explain details on model building, data management, model management, and economic incentive strategies.

— Supervising model usage; the auditors have the responsibility to request that users explain their purposes of using the model in their legitimate activities.

A.3.3 Function

Data owners may not use or disclose protected financial information, except either as the individual who is the subject of the information (or the individual's representative) authorizes in writing.

Data owners are permitted, but not required, to use and disclose protected financial information, without an individual's authorization, for the following purposes or situations:

— To evaluate the validity of the individual users unless required for access or accounting of disclosures

— To execute loan, payment, marketing, and other financial operations

— To develop the model or sub-models of data owners

Model users may use the protected financial information for its own loan, payment, and other necessary activities. Data owners also may disclose protected financial information for the financial activities of their own business.

A.3.4 Security and privacy requirements

In the financial sector, FML should implement the highest levels of security and privacy protection. As the sensitive financial data involves the interests of countries, institutions, and individuals, the profits from illegal acts in this field are often so high that there is a huge risk of underground industries and third-party attackers. At the same time, the financial industry is a typical industry with strong regulatory requirements with an

emphasis on legal compliance. The most stringent privacy protection policies often apply in the financial sector.

A.3.5 Performance

The main risks faced by financial institutions are overdue loans and fraudulent loans caused by user credit risk and fraud. Traditional financial institutions may only know users' borrowing history and behavior locally, but they know little about users' interests, consumption tendencies, behavior, and other private information. In order to conduct modeling without involving privacy leakage and improve the assessment of risks of loans, the traditional practice is to provide each institution with a separate model and then integrate all models results to get the evaluation result. However, this modeling method often has low performance and the obtained result may not be accurate enough. Federated machine learning can solve this problem by joint modeling the users' overall behavior across many sectors and financial institutions and can obtain lossless models. By way of FML, each data holder can exchange encryption parameters to jointly train a model, and obtain more reliable evaluation results when the data is retained locally. It can help financial institutions avoid risks more effectively.

Multi-party fraud detection involving multiple loan applications is the main method for financial institutions to use. Multi-party lending happens when a fraudulent customer borrows money from one financial institution and pays back a loan to another, which in many places is an illegal practice that can bring down the entire financial system. To find such users, the traditional practice is that financial institutions go to a central database to query user information, while each institution should upload all its users. However, this procedure will expose the privacy and data security of all important users of financial institutions, which violates many regulations such as the GDPR. In addition, the user label information of various financial institutions can be inferred by the statistical models to obtain a risk score for a user, so as to evaluate the credit ranking of the user. Due to the different judgment standards of each agency on the user label, a bad-loan rate can be defined by each agency and can be used as the weight to balance the standards of each agency. One way to define a bad loan is a delay in payment by 30 d. However, this method has the problem of exposing users' privacy. Under FML, there is no need to create a central database, and anyone involved in the study of financial institutions can query new users to the other part of the federal agency. FML can answer queries of local loan status and provide information about overdue and collection rates without leaking a user's private information.

A.3.6 Performance incentive

In the financial scenario, the incentives for each participant are as follows:

— For regulators in the financial industry, FML is an effective and innovative solution, that can solve many obstacles and accelerate the development of the industry.

— For the financial sector, the primary thing is to convince regulators to accept FML, as this industry, regardless of the country or region, is highly regulated and attaches great importance to legal compliance.

— Model users benefit from the scale of data across multiple institutions, leading to a superior product from which all customers can benefit.

— Data owners have introduced the risk of exposing competitive information (e.g., where their expertise is, and the scale of operations). Therefore, for data providers, it is appropriate to provide generous compensation or the corresponding field status.

In some cases, especially when large volumes of data are involved, legally sharing data can become prohibitively expensive. FML allows for much more concise insights to be shared instead. Participants in FML may value the reduced costs and budgets for data transfer.

A.4 Telecommunications

Mobile devices equipped with neural network processing units exploit their strong computational power to train neural network (NN) models using data captured by a wide range of on-device sensors. With such on-device computational power and data, mobile applications have significantly improved their usability and bring convenience to people's lives. However, serious ethical and regulatory concerns about data privacy remain, since mobile devices have collected enormous amounts of personal data such as biometric data, photos, and other personal information, and sent them to remote servers. Taking personalized recommendation service as an example, it is used to manage users' flight, meeting, and hotel booking information and provide recommendations based on users' personal information such as contacts, message, calendar, location, sports/sleep data, app usage etc. In this case, horizontal FML techniques provide a secure and trustworthy solution to prevent leakage of sensitive personal data.

A.4.1 Role design

The role designs within telecommunications may be defined as follows:

— Data owner: The user or owner of the mobile device

— Model user: The user or owner of the mobile device and/or the application service providers

For more information, see Clause 6.

A.4.2 Main activities of data owners

The main activities of data owner within telecommunications may be defined as follows:

— Data service includes releasing meta-data information, discovering network data, managing original data (including, but not limited to, storage mode, usage mode, encryption mode), using data, etc.

For more information, see Clause 6.

A.4.3 Main activities of model users

The main activities of data users within telecommunications may be defined as follows:

— Computing activities include starting modeling, modeling inferencing, starting prediction, receiving secure encryption computing protocol, data encryption, etc.

For more information, see Clause 6.

A.4.4 Security and privacy requirement

The raw data should not be leaked during the entire process of federated machine learning, the parameters and intermediate results in model calculations should not be intercepted. More requirements can be found in 9.2. (Security requirement level: 3–4; Privacy requirement level: 2)

A.5 Health

There are diverse health-related data such as trans-omics data including genome, epigenome, transcriptome, metabolome, proteome and metagenome, imaging data, and phenotype data collected from wearable devices

or other channels, along with the environmental, socioeconomic, and behavior data. However, health-related data, especially patients' data is highly sensitive and distributed in nature, thus collection and sharing of such data may bring critical legal and ethical privacy concerns. For example, if insurers learn a patient's health data and find out he/she has severe or high medical cost diseases, they may refuse to provide insurance service. FML can overcome those obstacles by providing a federated machine learning model across organizations while keeping sensitive health data within the local environment. FML applications in the healthcare field may have different scenarios, including business-to-government (B2G), business-to-business (B2B), business-to-customer (B2C), or mixed models.

For common FML scenarios in healthcare there is a need for the collaborative building of FML models among different hospitals, companies, research institutions, etc. Direct-moving data between hospitals may raise concerns about security, privacy, and availability of medical data. FML can address these concerns, and the horizontal FML model should achieve better performance than models trained with single institutional data. As an example, applying horizontal FML in genetic studies allows for the comprehensive analysis of genes, and helps to discover the hidden patterns between genotype and phenotype; it also benefits diagnostic and treatment development of diseases, such as cancer. Currently, samples collected from a single institution are insufficient to cover all the mutations in breast cancer type 1 and breast cancer type 2 (BRCA1/2) genes, while FML provides a feasible and secured way of training an FML model predicting the risk of breast and ovarian cancer.

In contrast, a vertical FML model exploits the vertically-partitioned health data from different institutions, where the two data sets share the same patient set but differ in feature space (i.e., pathological data, multi-omics data). This is usually the case in collaboration between hospitals and other medical companies with different data types. A typical example is to build a medication guidance system between hospitals and DNA/RNA sequencing companies when the hospitals have patients' clinical data, and sequencing companies have patients' genetic data. By building a vertical FML model, hospitals and companies can combine their features without revealing patients' privacy. Researchers or clinicians should be able to build better diagnostic or predictive models with FML than with single institutional data. Vertical FML can also include both B2B and B2C as a mixed scenario.

For all scenarios mentioned above, government departments can be added as other parties in the FML for acting supervisors or management roles. Both vertical and horizontal FML have board applications in healthcare research and industry. A traditional collaboration involving healthcare data usually requires an extensive amount of effort to comply with regulations and laws, while FML can provide a secure and trustworthy privacy protection mechanism during the training process along with decent model accuracy. Furthermore, FML fertilizes the joint study of different health-related data, deepening our understanding of biological systems and advancing the development of precision medicine.

A.5.1 Role design

A.5.1.1 Main activities of coordinators

In this standard, coordinator is defined as a healthcare supervising department of government (B2G) or hospitals, research institutes, pharmaceutical companies, etc. (B2B).

The main activities of coordinators include the following:

- FML function development activities include health-related algorithm development, infrastructure development, service development etc.
- FML computing activities include starting health-related modeling, secure and privacy-preserving computing management (security protocol determination, key generation, data decryption), etc.
- FML model management includes health-related model discovering, model meta-information management, model key management, etc.

— Capabilities coordination includes service access, service ability release, service meta-information management, participant meta-information management etc.

— Data management includes meta-data information management, release, discovery, etc.

A.5.1.2 Main activities of data owners

Data owners include healthcare service providers (hospitals, clinics, sequencing companies, etc.) who, with patients' consent, provide data to facilitate healthcare services.

The main activities of data owners include the following:

— Data service includes releasing meta-data information, discovering network data, managing original data (including, but not limited to, storage mode, usage mode, encryption mode), using data, etc.

— Computing activities include starting modeling, participating in modeling, starting prediction, receiving secure encryption computing protocol, data encryption, etc.

A.5.2 Main activities of model users

Model users include researchers and research institutions, healthcare service providers, insurance companies, pharmaceutical companies, etc.

The main activities of model users include the following:

— Computing activities include starting modeling, participating in health-related modeling, starting prediction, receiving secure encryption computing protocol, data encryption, etc.

— Model management includes health-related model data management, model meta-information management (version, participant, modeling time, valid time, etc.), model release model usage, etc.

— Service management includes the ability of modeling and predicting, list of services provided to users, service access, service planning, etc.

A.5.3 Main activities of auditors

Auditors are defined as governments or other supervising authorities.

The main activities of auditors include monitoring data usage and regulatory compliance.

A.5.4 Security and privacy requirement

The federated machine learning system should avoid raw data leakage during all processes, including data storage, data access, data transferring, and model training. The system should prevent data inferring and privacy exposure of individuals from both outsiders and malicious participants. (Security requirement level: 3–4; Privacy requirement level: 2.)

A.6 Education

Uses of machine learning in education and training range from standard data mining for the purpose of sales and marketing, to techniques such as Bayesian Knowledge Tracing that use hidden Markov models to determine the likelihood that a learner transitions from non-mastery to mastery by engaging in a particular activity. More generally, the field of educational data mining (EDM) uses a variety of traditional machine learning

techniques, including clustering algorithms and pattern recognition algorithms, and an increasing number of adaptive instructional systems (AIS) are using forms of machine learning to classify students, classify learning activities, determine optimal learning pathways, and make personalized recommendations. Very recently the research community has also started to consider reinforcement learning as a means to enable AIS to learn pedagogical strategies. Finally, many instructional systems interact with and assess learners using natural language. For example, they might automatically grade an essay response, or engage in dialogs via an avatar. Underlying these natural language processing (NLP) abilities are machine learned models of semantic spaces, domain ontologies, dialects, and other data. The application of AI in education can simply be understood as creating an adaptive learning technology to customize learning programs for students, therefore, it is B2C.

There are at least three fundamental problems posed by these applications of machine learning to education and training:

a) The protection of personally identifiable data, which is regulated in general, but even more highly regulated in the educational arena, especially when children are involved.

b) The interoperable exchange and sharing of the models generated by AIS, many of which are expressed in terms of knowledge, skills, abilities, attitudes, and other characteristics and include learner models, domain models, pedagogical models, and potentially reward functions.

c) The ethical practice of AI, which includes verifying that the models generated are not applied in unwarranted or unwanted ways, and are either not biased or transparent about their biases.

FML can help address at least a) and b), and possibly c). To this end, the following use cases have been identified:

— Construction of learner models with data from multiple learning systems: In this use case multiple learning systems produce data about learners, some of whom use more than one system, but the systems are prohibited from sharing data and the identity of learners. Each system applies its own machine learning to estimate mastery, or to make predictions such as time-to-mastery based, or to estimate the effect of a particular activity as a function of the current (and possibly past) learner states. These estimates are shared and a larger model is constructed using federated machine learning, and shared with each learning system, to improve the accuracy of each system and, if appropriate, the recommendations it makes. For this to work, it is necessary to have federated identities.

— Sharing domain models as knowledge graphs: A domain model is often represented as a knowledge graph. Often, this graph is considered static and is input into an instructional system, but it is also possible for a system to analyze source materials, data created by instructional systems designers, and learner interactions (especially speech and text input) to derive or modify domain models.

— Learning pedagogical strategies: Pedagogical strategies are represented in AIS in many ways. A common way is as a set for rules, which may be an event-condition-action table, a sequence of speech or dialog acts, rules based on instructional design theories, or branching and remediation rules based on estimates of the learner's current state. In existing AIS, these rules are almost universally hard-coded, but the input to the rules is often machine learned. For example, the rules might dictate different instructional behaviors based on the categorization of learners, and the categorizations might be learned from data. Or, the rules might require estimates of the effectiveness of learner activity, or classification of learning activity in educational taxonomies (e.g., Blooms). To the extent that learners or activities are shared by multiple systems, FML can be used to improve accuracy without compromising the privacy of data. In addition, it is possible that the rules themselves are machine learned. In that case, using methods like reinforcement learning, it is important to have large data sets that can only be generated by aggregating data from multiple sources across multiple students, which is also facilitated by FML.

A.6.1 Role design

A personalized education platform should teach students with their aptitude. It should keep a good balance between large scale and high-quality personalized education with most-advanced AI technologies in the world.

Role design activities include the following:

— Differentiation among subjects: The systems should build different learning models for different segments and disciplines, and recommend the most suitable learning methods, exercises, and tests for students.

— Customization for students: The systems should conduct an assessment for individual students, develop fundamental maps on what they have mastered and what needs more practice. Then, it recommends individuals focus more on the latter and avoid repeating the former, in which way each student can learn at his/her own pace.

— Empowerment for teachers: Intelligent adaptive education uses AI to simulate the experience of excellent teachers. This is especially important to regions that lack educational resources. At the same time, teachers can track the development of individual students, thus providing more efficient programs for them.

A.6.2 Main activities of each role

Activities of AI education platform are as follows:

— Develops learning programs and courses that work best under the guidance of AI technology, and at the same time cater to the needs of students

— Continues to improve the platform based on the feedback and data collected, in order to make it smarter and more user-friendly

— Customize the services for students from different age groups, different areas, and with different purposes

Activities of students are as follows:

— Finish a first-step test at the very beginning of using the platform, so that the AI teacher can better know what students are and are not good at

— Focus on the knowledge gap and avoid repeating what they have already had a good command of, with the help of AI technology

— Make the learning process more efficient after using the AI education platform

Activities of teachers/coachers are as follows:

— Make their teaching methods cater more to the needs of the students with the assistance of the platform.

— Save time previously spent on revising students' homework (can be completed by AI platform); utilize the time instead of interacting with students and renovating the courses

A.6.3 Function

AI in education generally focuses on identifying what a student does and does not know through diagnostic testing, and then developing personalized curricula based on each student's specific needs. The functions of AI education in detail are as follows:

a) Not allowed to use and disclose:

   1) The operator should not use or authorize other agencies to use the protected student data without authorization, unless consent from students and parents are obtained.

   2) The operator should not use or disclose the protected personal privacy data unless authorized in writing by the information subject or its guardians or clients.

b) Permitted use and disclosure:

   1) Publicly available course and book data, which could be used for all users.

   2) Data authorized by students and parents in order to improve the services of the operator.

A.6.4 Security and privacy requirement

The federated machine learning system should get consent from users before collecting their data, and avoid raw data leakage during all processes including data storage, data access, data transferring, and model training. The system should prevent data inferring and privacy exposure of individuals from both outsiders and malicious participants. All students' data should only be used to create their personalized learning programs.

A.6.5 Performance

In the process of contractual opening of education data, each participant (i.e., AIS, subject) initiate its own needs, the platform operator then coordinates all participants to follow the agreed standard rule to complete each party's calculation tasks and upload the required parameters to the platform. The platform operator will combine all the uploaded data to complete the final model and send back the model to all the participants. All the participants will use the final model leveraging a much bigger and richer data pool to do the desired investigation without sharing their original data. In this process, education data will not leave flow out of the data original station. All parties will only get the result of model training in the end. Therefore, the federated machine learning of education not only reduces release the education data but also greatly preserves all the participants' security and privacy and benefits all.

A.6.6 Performance incentive

In the framework of federal learning on education, the incentives for each participant are as follows:

— The platform operators establish and manage all the final model processes for each participant involved in contractual opening, used to record data contractual open participation. The platform collects all the submodels for training the final model without hurting each participant's security and privacy. All the participants will pay to use the final model. The platform will congregate more and more submodels based on each participant (i.e., AIS or subject or subjects group, such as STEM) to strengthen its mode then sell it to both the participants and external model users.

— Internal participants: In education federated machine learning, each paralleled participant, such as AIS, serves as data owner and model user. Each AIS contributes to a lower level model for the final model training. It is necessary to collect data following the model data structure requirements, to follow and operate the training steps that the platform requests, and use the final model in order to gain better

performance on student/teacher engagement, student learning performance predictions, and student learning path recommendations or learning group recommendations.

— External participants: External participants could be the current final model users or future model contributors. When they need to use the joint model, the model operator invites the data owner to participate in the joint modeling, and the external participants pay the operator a certain fee based on the data usage. Thus they can use the model to benefit their business as well as contribute the current model.

A.7 Urban computing

Urban computing is a process of acquiring, integrating and analyzing heterogeneous big data generated by a diversity of sources including sensors, devices, vehicles, buildings, and humans in urban space. Applications of urban computing aim to tackle major city challenges, such as air pollution, increased energy consumption, and traffic congestion. In many urban computing scenarios, there are regulatory requirements and privacy concerns, with regards to the sharing of smartphone GPS data. Commercial entities like ride-hailing or bike-sharing companies may also be unwilling to share their data. Furthermore, due to the slow and unreliable network connections, there are practical challenges in consolidating all the data acquired by edge devices, such as vehicle GPS units. Therefore, urban computing belongs to the business-to-government (B2G) category.

FML can overcome these challenges by building a federated machine learning model across organizations, while the individual data of each organization stay in their local environment. Horizontal FML can be used in cases where two data sets share the same feature space, but have dramatically different samples. Data sets from different taxi companies constitute such an example. On the other hand, vertical FML models exploit vertically-partitioned data, for instance, with a user's smartphone GPS data and his or her credit history.

Federated transfer learning solves the problem where the two data sets differ in both samples and feature space. Smart ride-hailing is one example of the use case. Ride-hailing companies have a strong incentive to find optimal solutions to the vehicle routing problem. GPS data from these vehicles provide information on the number of vehicles and their speed along with different road segments, facilitating the predictions about future traffic conditions. While ride-hailing companies may be unwilling to share valuable data with each other, FML solves the problem by allowing different companies to build and train a federated machine learning model, with model parameters—but not the private data—securely exchanged under the federated system's encryption mechanism.

Environmental protection is another example of the use case. Air quality prediction can help residents take precautionary measures and allow city governments to implement corresponding countermeasures. However, this can be challenging since the air quality of a region depends on many factors, including industrial emissions, vehicle exhaust, and meteorological conditions. Factories may not be willing to share data about their real-time emissions, from which sensitive operational and financial information may be gleaned. Regulatory and privacy concerns may also prevent environmental regulators from collecting data about individual vehicles' location, model, and speed, from which vehicle exhaust information could be deduced. Current prediction models therefore generally rely on AQI readings from sparsely distributed air quality monitoring stations and meteorological conditions and are unable to make use of more fine resolution industrial emissions and vehicle exhaust data. FML solves this problem, allowing the training of a federated machine learning model on heterogeneous big data, increasing the accuracy of air quality prediction.

A.7.1 Role design

Role designs in urban computing are as follows:

— Coordinator: The government departments or urban-computing related corporations

— Data owner: Individuals, corporations, or government departments contributing data in urban sensing and data acquisition

— Model user: The government departments, corporations with government authorizations, researchers and research intuitions with government authorizations, individuals

— Auditor: The government regulator that is responsible for urban-computing applications

A.7.2 Main activities of each role

The main activities of each role within urban computing are as follows:

a) Activities of coordinator

1) FML function development activities include urban-computing related algorithm development, infrastructure development, service development, cross-departments negotiation, etc.

2) FML computing activities include starting urban-computing related modeling, secure multi-party computing management (security protocol determination, key generation, data decryption, modeling supervision, record-keeping), etc.

3) FML model management includes urban-computing related model discovering, model meta-information management, model key management, etc.

4) Capabilities coordination includes service access, service ability release, service meta-information management, participant meta-information management, etc.

5) Data management includes meta-data information management, release, discovery, etc.

6) Economic incentive activities include calculating the payments to data owners and model users

7) Distribution of urban-computing applications

b) Activities of data owner:

1) Collecting and preparing original urban data

2) Claiming costs of data preparation

3) Maintaining privacy and security of original urban data

4) Allowing federated machine learning systems to train FML models

5) Asking for payments and receiving the rewards

6) Responsible for providing compliant data and verifying the legality of the data source

7) To cooperate with reasonable data modeling tasks or urban-computing services with proper data

c) Activities of model user:

1) Requesting for urban-computing services

2) Discovering service capability

3) Using federated machine learning service

4) Discovering meta-data

5) Using the FML model and paying the price

d) Activities of auditor

1) In charge of making regulations and requirements for urban-computing federated machine learning

2) Checking the legitimacy of the data set, that the auditors have the responsibility to check the legitimacy of the data set

3) Monitoring model building procedures, that the auditors have the responsibility to claim the coordinator to explain the model building details, data management, model management, and economic incentive strategies

4) Supervising model usage, that the auditors have the responsibility to claim the user to explain their purpose of the model using

A.7.3 Function

The function of modules in detail are as follows:

a) Not allowed to use and disclose

1) The participants should not use the data of other participants without authorization unless the written permission of the related data provider is obtained.

2) The operator should not use or disclose the protected privacy data unless authorized in writing by the information subject or its guardians or clients. The person is regarded as an information subject or the person's representative.

b) Permitted use and disclosure

1) Publicly available government data, which could be used by all participants.

2) Data authorized by participants for useful urban computing research or application.

A.7.4 Security and privacy requirement

Privacy data, such as driving trajectory and GPS data, is used in urban computing, which brings great privacy risks. The highest privacy requirements should be used for urban computing. At the same time, urban computing also involves the confidentiality of some companies or institutions, such as business models, unpublished research results, etc., which also require close attention at the security level.

A.7.5 Performance

The performance of urban computing applications depends on both the quality of the data and the ability to analyze data. In order to improve the performance of urban computing, first, it is crucial to encourage high-quality data owners to join the ecosystem. Second, one has to improve data analysis capabilities and find exciting conclusions from limited data.

A.7.6 Performance incentive

In urban computing, the incentives for participants are as follows:

— From all the roles in urban computing, the data owner is the most important. Without strong incentives to meet the varying expectations of different participants, the problem of poor motivation and unwillingness of individuals or organizations to participate in the urban computing process abounds.

— A key challenge that should be adequately addressed for urban computing is the design of an appropriate incentive scheme which motivates individuals to participate in large-scale sensing campaigns. The real money or any valuable virtual cash, redeemable credit, etc. Are given as monetary incentives.

— For data platforms without a sufficient number of contributing parties, platform-centric or user-centric monetary incentives can be used to encourage contributions to the federation.

— Non-monetary incentives can also be given to data owners, who are rewarded for their contributions.

For service developers and providers, their gains are the obvious economic benefits, such as more exhibition opportunities, greater user traffic, and more cooperation possibilities in the future. However, for service providers, when the user ecosystem is becoming more and more mature, it also puts forward requirements for their capabilities, prompting them to develop new programs, improve technology, and provide more comprehensive services.

A.8 Government services

Government services can be greatly improved by using big data that is collected across multiple sources. Applications of such services include accurate traffic flow predictions and early identification of public vigilance threats etc. Moreover, government services are government-sponsored, and jointly provided by government agencies and private businesses. Thus, government services are business-to-government (B2G).

While government agencies possess a large volume of data, this data may exist in the form of data solo with administrative procedures and privacy concerns preventing data being exploited by different agencies. FML can overcome these challenges by building a federated machine learning model across government agencies and businesses, while the individual data of each organization remain intact in their local environment. Horizontal FML can be used in cases where data sets share overlapped feature space e.g., in data from different taxi companies. Vertical FML allows the exploitation of vertically-partitioned data, where data sets have significant overlaps in sample IDs but differ in the feature space. A citizen's employment records and medical history belong to vertical FML use cases. Federated transfer learning solves the problem where data sets differ significantly in both samples and feature space. Such an example is showcased by spatiotemporal public vigilance data, collected by different police stations in neighboring cities.

Although the integration of data across different administrative regions is prohibited by administrative and regulatory barriers, an FML model can consider holistic information about each person, as well as a larger training set that encompasses citizens across different administrative regions. The data of each agency remains private and only model parameters are exchanged during the training of the FML model.

A.8.1 Role design

Role designs within government service are defined as follows:

— Coordinator: Government departments, such as department of transportation, department of public vigilance, department of finance, department of social security, etc.

— Data owner: The government departments with various types of urban data, a business focusing on urban related industries, research institutes.

— Model user: Government departments, private companies with government authorizations, universities, and research intuitions with government authorizations, non-profit institutions with government authorizations

— Auditor: Governments or other supervising authorities

A.8.2 Main activities of each role

The main activities of each role are defined as follows:

a) Activities of coordinators
   1) FML function development activities include government service related algorithm development, infrastructure development, service development, cross-departments negotiation, etc.
   2) FML computing activities include starting government service related modeling, secure multi-party computing management (security protocol determination, key generation, data decryption, modeling supervision, record keeping), etc.
   3) FML model management includes government service related model discovering, model meta-information management, model key management, etc.
   4) Capabilities coordination includes service access, service ability release, service meta-information management, participant meta-information management, etc.
   5) Data management includes meta-data information management, release, discovery, etc.

b) Activities of data owners
   1) Collecting and preparing original government data
   2) Claiming costs of data preparation (optional)
   3) Maintaining privacy and security of original data
   4) Allowing federated machine learning systems to train FML models
   5) Asking for payments and receiving the rewards (optional)
   6) Communicating intermediate computational results with other parties during FML inference phase

c) Activities of model users
   1) Requesting for government services
   2) Discovering service capability
   3) Using a federated machine learning service
   4) Discovering meta-data

d) Activities of auditors
   1) Verifying the legitimacy of the government data sources
   2) Monitoring and book keep for the model building processes
   3) Requesting the coordinators to explain data management, model management, and economic incentive strategies
   4) Supervising model usage and requesting users to validate model usage requests

A.8.3 Function

The functions of modules in detail are as follows:

a) Not allowed to use and disclose

1) The participants in government services should never use or authorize other agencies to use the protected data of other participants in the contract without authorization unless the written permission of the related data provider is obtained.

2) The participants should never use or disclose the protected privacy data unless authorized in writing by the information subject or its guardians or clients. The person, or the person's representative, is regarded as an information subject.

b) Permitted use and disclosure

1) Data authorized by data providers in the government regulated and protected contracts, including those provided by government agencies.

2) Data authorized by government departments for value-added services.

A.8.4 Security and privacy requirement

Data owners should not disclose any protected government data, except the data is categorized as not sensitive and can be open for public use, such as weather history. Data owners should not disclose any citizen's information to the public, unless it is considered legal by laws or regulations. Model users should develop and apply the FML models in a secure system and the data access should be assigned with a life cycle and limited to a minimum; any raw data should be destroyed once the task is finished. The auditors should regularly review the past federated modeling and inference histories, and any other related issues. During the overall federated modeling procedure, any raw data leakage should not occur including data storage, data access, data transferring, and model training. The system should prevent data inferring and privacy exposure of individuals from both outsiders and malicious participants.

A.8.5 Performance

The performance of government, and the services that it finances, are a major contributor to societal wellbeing. The government is set on using data more effectively to help deliver better public services. Better use of data can improve the design, efficiency, and outcomes of services. For example, services that help to share health insurance information by region hospitals can enable better and faster medical payment channels. Building on these models can help spread best practice and improve government service standards across the country.

A.8.6 Performance incentive

In the government service scenario, the incentives are as follows:

— Creating a new data service infrastructure that allows organizations to overcome barriers to data sharing and build on government promises of improving service capabilities requires clear leadership and a collaborative approach. Opportunities are arising to redirect leadership through new structures, such as new regulatory agencies, and new positions in the government.

— Local government can also play an important role in promoting FML-based services across the public sector. Local cooperation agreements can provide an infrastructural and standards template for larger-scale cooperation agreements. By giving local areas space to try and test FML arrangements, it will help to demonstrate which projects are successful and could be scaled-up regionally and nationally.

— Government departments should identify and support initiatives in all policy areas, supporting organizations if they need to properly engage citizens and understand how they want their data to be used across public services.

— Moving forward, it should be mandatory for any system procured within the public sector to adopt open standards, encouraging competition and improving interoperability by avoiding vendor lock-in situations.

A.9 Government governance

Government governance can be simply understood as the self-optimization and the governance of social affairs carried out by the government as the dominant. Specifically, the development of e-government toward open government and smart government aims, ultimately, to provide efficient, smart and personalized administrative services to people. This reform calls for the connecting and sharing of enormous data, which are distributed across a hierarchy of regional government departments. The difficulty of opening and sharing government data from distributed data sets lies in requiring the protection of highly sensitive and private information contained in government data. It is of essential importance to explore the new mode of sharing government data, which can enhance the usability of open data without compromising data security. It is also expected to encourage the data providing department and improve administrative efficiency. Federated machine learning provides an effective solution that improves government data security and privacy security under the condition that data not being disclosed to unauthorized participants.

A.9.1 Role design

The opening of government data is an important work in the government governance domain. For example, the government data contractual opening platform as a federated machine learning system may involve regulators of data open, regulators of benefits, independent third parties, operators, and developers of the platform.

— Data owner: The government regulator who is responsible for government data contractual opening.

— Regulator for benefits: The government department of finance, which is responsible for supervising, managing, and allocating the benefits earning by the government in the process of data contractual opening.

— Independent third party: It is performed by the authorities and authorized by the government.

— Operator: The state-owned enterprise is given credit by the government, providing the government data value-added services.

— Participant: The organizations joined in the contractual opening, which includes government departments, public sectors, non-profit organizations, enterprises, research institutes, etc.

— Coordinator: The company authorized by the operator to be responsible for developing the function of the contractual opening platform.

A.9.2 Main activities of each role

Activities of regulators for data open include the following:

— In charge of making regulations and requirements for government data contractual opening

— Authorize, indicate, and supervise the operators to process the government data contractual opening

— In charge of coordinating the government departments, join in the contractual data opening, and evaluating the performance of departments involved

Activities of regulators for benefits include the following:

— Responsible for making unified management and allocation of the government department income involved in the contractual opening

— Responsible for supervising the benefit distribution of the operator

Activities of independent third party include the following:

— In charge of evaluating the performance of regulator for data open, participant, which specifically refers to the government department or public sector, and operator

Activities of operators include the following:

— In charge of implementing the related requirements of government data contractual open provided by data open supervise guideline

— Contacting government departments, establishing contractual open data catalog and database

— Responsible for operating the government data contractual open platform, exploring and satisfying the requirement from participants

— Fulfilling the requirements from participants, authorizing the platform developer to make functional development, and upgrading

— Responsible for distributing benefits to each participant in the contractual opening

Activities of participants include the following:

— Creating the computing activities, including initializing model, involved in the modeling, staring prediction, involving prediction, accepting secure encryption computation, data encryption, etc.

— Responsible for making model management, including model data management, model meta-information management, model release, mode usage, etc.

— Service management, including modeling, predicting ability, service list provided to users, service accessing, service planning, etc.

— Providing data service, including releasing data meta information, exploring internet data, managing original data, using data, etc.

Activities of platform developers include the following:

— Fulfilling the requirements from operators, in charge of the contractual opening platform function development or upgrading, including algorithms development, infrastructure development, service development, etc.

A.9.3 Function

One of the key points to build strong governance capacity is promoting data exchange while exploring potential value. The design and function points for the system of government data contractual open service should be met as follows:

a) Not allowed to use and disclose:

   1) The operator should not use or authorize other agencies to use the protected government sensitive data without authorization, unless the written permission of the government department is obtained.

   2) The operator should not use or disclose the protected personal privacy data unless authorized in writing by the information subject or its guardians or clients—the individual regarded as an information subject or the personal representative.

b) Permitted use and disclosure:

1) Publicly available government data, which could be used by for all participants.

2) Data authorized by government departments for value-added services.

3) The protected sensitive data, used or disclosed by data owners for the following purposes:

i) Used by government departments to carry out social governance work

ii) Used by government departments to provide public services

iii) Partial or limited data set up for scientific research

iv) Other permitted use

A.9.4 Performance

In the process of contractual opening of government data, each participant may initiate requests of FML models as needed The platform operator then coordinates all participants to join an FML training session, during which government data owned by each participant do not leave their localhost and all participants can only get the result of model training in the end. Due to the encryption of exchanged FML model parameters, both the privacy and security of government data are not compromised.

A.9.5 Performance incentive

In the government data contractual opening scenario, the incentives for each participant are designed as follows:

— The operators establish, record, and manage distributions of virtual currency to governments or public departments involved in contractual opening, according to the contributions of each department.

— Each department is paid by the operators to participate in the contractual opening.

— Government departments may pay other departments to contribute FML modeling through the management of operators.

— Government departments or public departments may pay the operators for the FML services provided.

A.10 Marketing

The development of a smart marketing strategy is usually achieved by mathematically modeling over big data sets. Conventionally, the data sets used for modeling are the collected fundamental profiles and historical behaviors of the advertiser's existing clients. The features of these data sets, however, mostly fall in the category of the subarea that the advertiser serves in, and thus may have limited descriptive capability to produce an accurate and descent statistical model. This eventually restricts the practical performance of a marketing strategy. Therefore, it is essential for an advertiser to aggregate data sets from massive areas to form a comprehensive database, based on which the learned model can exhibit both theoretically and practically satisfactory performance. However, as the increasingly strict data privacy regulations take effect, including the GDPR, and the public awareness of data confidentiality keeps rising, the data flow among various subareas is generally prohibited subject to data privacy concerns, which in turn impedes the development of high-performance models for traditional marketing platforms.

The introduction of FML, especially vertical FML, makes virtual data aggregation without a privacy breach possible for making high-quality marketing decisions. A wide range of features and samples achieved by FML enrich the potentially useful patterns that can be extracted by training a machine learning model and thereby significantly improve the marketing model performance. Cooperating with client's social behavior data

collected from social media companies via FML, for example, credit companies have the capability to identify clients of potentially high default rates who scarcely leave any dishonest marks in the whole credit system in the past. Similarly, FML also enables a video game company to attract a group of players of high-consumption capability by training a marketing model over the financial data provided by a bank. With FML, data now manage to flow among politically isolated databases and produce economic values for various business and industries.

A.10.1 Role design

Client: Companies who pursue satisfactory business results by implementing marketing models, including customer product companies, video game companies, credit companies, etc.

The role design of clients includes the following:

— Conduct data annotation and prepare sample labels related to its target business

— Prepare the infrastructure for computation, storage, and communication usage

— Conduct computing activities subject to FML protocols, including local computation, data encryption and encrypted communication with feature providers to complete FML model training and prediction

Feature provider: Companies that collect a wide range of up-to-date data sets from their own business areas.

The role design of feature providers includes the following:

— Prepare structured data collected from its own customers

— Prepare the infrastructure for computation, storage, and communication usage

— Conduct computing activities subject to FML protocols, including local computation, data encryption and communication with clients to complete FML model training and prediction

Algorithm provider: Coordinator who is in charge of the deployment, operation, and maintenance of FML service.

The role design of algorithm providers includes the following:

— Provide FML service deployment guidance for clients and feature providers

— Conduct regular operation and maintenance of FML service in progress

— Improve existing FML protocols in terms of algorithm privacy, accuracy, and complexity and develop new FML protocols based on traditional machine learning and data mining algorithms

A.10.2 Security and privacy requirement

Security requirement: Since data is one of the most valuable assets to a company, the highest attention (level 4) should be paid to the data flow security under FML service implemented in a marketing platform, including data collection, storage, computation, and communication.

Privacy requirement: Not only sample features and labels should be kept private throughout the execution of FML model training, but the sample IDs should be also given sufficient concerns in FML model prediction and marketing advertisement injection. In online prediction, for example, clients may request for the confidentiality of the potential target population related to their business inferred by a trained FML model. Another example

is that an algorithm provider in offline prediction may request the inferred target population be shared with the designated clients but kept unaware to the other participants.

A.11 IoT/edge computing

With the development of 5G and Internet of Things (IoT) technology, edge devices and local data will be exponentially growing. One of the main trends in 5G and edge computing is to power the edge with intelligence instead of leaving the intelligence in a server cloud. That is to say, more mobile phones or IoT devices require the ability to make decisions and take action automatically. How to process data and build machine learning models locally to enable the privacy-preserving as well as personalize user experience is an important area across the academic and industrial domains. Traditional AI performs the cloud-based or centralized modeling process, which needs data transferred to the cloud servers and conducting the training, evaluation, deployment, and serving.

Federated Machine Learning is a machine learning framework where independent clients (e.g., mobile devices or organizations) collaboratively train a model under the coordination of a central server (e.g., service provider) while keeping the local training data decentralized. The FML is different from traditional distributed machine learnings in three ways. First, users have more control over the devices and data to prevent the privacy leakage issue. Second, clients are unstable and heterogeneous. Last but not least, it brings the benefit of fewer communication costs. FML emphasizes the principles of data localization, low latency, and less power consumption, and can reduce many of the systemic privacy risks and costs resulting from traditional and centralized machine learning algorithms.

With the introduction of horizontal, vertical, and transfer federated learning, collaborative training can be widely used on mobile phones or IoT devices to enable the data and model enhancement. Many AI scenarios on edge devices are regularly improved. These improvements include personalized image processing for cameras, short video content generation, better automatic speech recognition (ASR), and natural language understanding (NLU) for personal virtual assistants, improved recommendation system, online advertising, smart air-conditioner and intelligent glasses with AR/VR, etc. Most of the existing pipelines of aggregating local data into a logically or physically centralized server for processing can be developed with FML.

A.11.1 Role design

The development of IoT/edge computing using a federated machine learning system may involve the following:

- Clients: Mobile phones or IoT devices with local data. These data contain the user interaction log and other contents.
- Servers: The central serves to communicate with the clients, coordinate the collaborative model training process and transfer the parameters or gradients, etc.
- Users: Owners of mobile phones or IoT devices. They interact with the edge devices which produce related data and stored them locally.
- Companies: The producers or providers of mobile phones or IoT devices, and also are responsible for deploying the federated machine learning model to these clients.

A.11.2 Main activities of each role

The main activities of each role are as follows:

a) Main activities of clients:

   1) FML client performs model training, deployment, and serving.

   2) FML client communicates with the servers transferring model parameters or parameter gradients (data encryption and decryption) etc.

   3) FML client data management includes local data management and processing, transferring intermediate data while computing as well as modeling etc.

b) Main activities of servers:

   1) FML server is responsible for coordinating the overall, collaborative model training process.

   2) FML server is responsible for communicating with the clients including broadcasting the model parameters.

   3) FML server performs computing, which involves aggregating the model parameters or parameter gradients, performing the model updating and sending it back to the clients.

c) Main activities of companies:

   1) Responsible for producing mobile phones or other IoTdevices.

   2) Integrating mobile or embedding OS (Operating System) like iOS, Android or MIUI, etc., with the devices to allow the FML services to run locally.

   3) Responsible for deploying the necessary components of FML to enable the devices to perform the operations of clients.

A.11.3 Security and privacy requirement

During the end-to-end federated modeling procedure, any raw data leakage is not allowed including data generation, storage, access, intermediate data transferring and model training. The whole system should prevent data inferring and privacy exposure of individuals from both outsiders and malicious participants. (Security requirement level: 4; Privacy requirement level: 2.)

Annex B

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] Nilsson, A., S. Smith, G. Ulm, E. Gustavsson, and M. Jirstrand, "A Performance Evaluation of Federated Learning Algorithms," in Proceedings of the Second Workshop on Distributed Infrastructures for Deep Learning - DIDL '18, Rennes, France, 2018, pp. 1–8, http://dx.doi.org/10.1145/3286490.3286559.

[B2] Benavoli, A. et al., "Time for a change: A tutorial for comparing multiple classifiers through Bayesian analysis," Journal of Machine Learning Research, vol. 18, no. 1, pp. 2653–2688, 2017.

[B3] Nadeau, C. and Y. Bengio, "Inference for the Generalization Error," Machine Learning, vol. 52, no. 3, pp. 239–281, 2003.

[B4] Corani, G. and A. Benavoli, "A Bayesian approach for comparing cross-validated algorithms on multiple data sets," Machine Learning, vol. 100, no. 2–3, pp. 285–304, September 2015.

[B5] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," ArXiv160205629 Cs, Feb. 2016.

[B6] Feng, J., Q.-Z. Cai, and Z.-H. Zhou, "Learning to Confuse: Generating Training Time Adversarial Data with Auto-Encoder," Advances in Neural Information Processing Systems, 2019.

[B7] J. Konečný, H. B. McMahan, D. Ramage, and P. Richtárik, "Federated Optimization: Distributed Machine Learning for On-Device Intelligence," ArXiv161002527 Cs, Oct. 2016.

[B8] Kairouz, P. et al., "Advances and open problems in federated learning." arXiv preprint arXiv:1912 .04977, 2019.

[B9] K. Cheng, T. Fan, Y. Jin, Y. Liu, T. Chen, and Q. Yang, "SecureBoost: A Lossless Federated Learning Framework," ArXiv190108755 Cs Stat, Jan. 2019.

[B10] Konečný, J., H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, (2016). "Federated learning: Strategies for improving communication efficiency". *arXiv preprint arXiv:1610.05492*.

[B11] LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton. "Deep learning." nature 521.7553 (2015): 436–444.

[B12] Payman Mohassel and Peter Rindal, "ABY3: A Mixed Protocol Framework for Machine Learning," https://eprint.iacr.org/2018/403.pdf, 2018.

[B13] Yang, Q. and Y. Liu et al., "Federated machine learning: Concept and applications," ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 2, pp. 1–19, 2019. [TIST].

[B14] Cheng, R. and F. Zhang, An Overview on the Secure Program Obfuscation. Netinfo Security, 2015.

[B15] S. Caldas et al., "LEAF: A Benchmark for Federated Settings," ArXiv181201097 Cs Stat, Dec. 2018.

[B16] T. Lepoint, M. Naehrig. “A Comparison of the Homomorphic Encryption Schemes FV and YASHE”. Cryptology ePrint Archive, Report 2014 /062.

[B17] Vasudevan, Prashant Nalini. “A study of efficient secret sharing.” 2015.

[B18] Kolesnikov, V. and T. Schneide, “Improved Garbled Circuit: Free XOR Gates and Applications”. In Proceedings of the 35th international colloquium on Automata, Languages and Programming, Part II. 2008.

[B19] Huang, W., M. Langberg, J. Kliewer, and J. Bruck, “Communication Efficient Secret Sharing,” IEEE Transactions on Information Theory, vol. 62, no. 12, pp. 7195–7206, December 2016.

[B20] Yang, K. et al., “Federated learning via over-the-air computation,” IEEE Transactions on Wireless Communications, 2020.

[B21] Yang, Q. et al., “Federated learning,” Synthesis Lectures on Artificial Intelligence and Machine Learning, vol. 13, no. 3, pp. 1–207, 2019.

[B22] Zhu, L., Z. Liu, and S. Han, “Deep leakage from gradients,” Advances in Neural Information Processing Systems, 2019.

IEEE SA
STANDARDS ASSOCIATION

RAISING THE WORLD'S STANDARDS

Connect with us on:

Twitter: twitter.com/ieeesa
Facebook: facebook.com/ieeesa
LinkedIn: linkedin.com/groups/1791118
Beyond Standards blog: beyondstandards.ieee.org
YouTube: youtube.com/ieeesa

standards.ieee.org
Phone: +1 732 981 0060

IEEE