IEEE SA
STANDARDS
ASSOCIATION

IEEE Guide for Architectural Framework and Application of Federated Machine Learning

STANDARDS

IEEE Computer Society

Developed by the
Learning Technology Standards Committee

IEEE Std 3652.1™-2020

IEEE

IEEE Std 3652.1™-2020

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,