

FEDERATIV O'QITISH ASOSIDA MAXFIY MA'LUMOTLAR BILAN ISHLASHDA SUN'IY INTELLEKT MODELLARINI XAVFSIZ HAMKORLIKDA O'QITISH METODOLOGIYASI

Qurtov M.X.

E-pochta: kurtov.mansur@gmail.com

Maqola turi: metodologik-tahliliy maqola

Annotatsiya

Sun'iy intellekt tizimlarini yuqori sifatli ma'lumotlar asosida o'qitish ko'pincha ma'lumotlarni markazlashtirishni talab qiladi. Biroq tibbiyot, moliya, davlat boshqaruvi va telekommunikatsiya kabi sohalarda ma'lumotlar maxfiyligi, huquqiy cheklovlar va tashkilotlararo ishonch masalalari ularni yagona bazaga yig'ishni qiyinlashtiradi. Ushbu maqolada xom ma'lumotlarni tashkilotlar tashqarisiga chiqarmasdan birgalikda model o'qitishga imkon beruvchi federativ o'qitish (federated learning, FL) uchun xavfsizlik va boshqaruvga yo'naltirilgan metodologik arxitektura taklif qilinadi. Yondashuv mahalliy o'qitish, vaznlarni agregatsiya qilish, xavfsiz agregatsiya, differensial maxfiylik, ma'lumotlar taqsimotining notekisligi, model sifati va auditni yagona jarayonda ko'rib chiqadi. Maqola mavjud ilmiy ishlar sinteziga asoslanadi va yangi empirik tajriba o'tkazilganini da'vo qilmaydi. Uning asosiy hissasi federativ o'qitish loyihalarini rejalashtirish uchun bosqichma-bosqich protokol, xavf modeli va baholash mezonlarini tizimlashtirishdir. Taklif etilgan metodologiya maxfiylikni saqlashni mutlaq kafolat deb emas, balki texnik, tashkiliy va statistik nazoratlar bilan boshqarilishi lozim bo'lgan xavf sifatida talqin qiladi.

Kalit so'zlar: *sun'iy intellekt, federativ o'qitish, ma'lumotlar maxfiyligi, differensial maxfiylik, xavfsiz agregatsiya, model xavfsizligi, mashinaviy o'qitish.*



Abstract

Training artificial intelligence systems often requires access to large and diverse datasets. In healthcare, finance, public administration, and telecommunications, however, privacy obligations, legal restrictions, and inter-organizational trust can make centralizing raw data impractical. This article proposes a security- and governance-oriented methodological architecture for federated learning (FL), which enables collaborative model training while keeping raw data at participating organizations. The framework integrates local training, model aggregation, secure aggregation, differential privacy, non-identically distributed data, model utility evaluation, and auditability. It synthesizes established research and does not claim new empirical experiments. Its contribution is a structured protocol, threat model, and evaluation criteria for planning federated learning projects. Privacy is treated not as an automatic guarantee of FL, but as a risk that must be managed through technical, organizational, and statistical controls.

Keywords: *artificial intelligence, federated learning, data privacy, differential privacy, secure aggregation, model security, machine learning.*

1. Kirish

Sun'iy intellekt modelining sifati ko'p jihatdan o'qitish ma'lumotlarining hajmi, xilma-xilligi va reprezentativligiga bog'liq. Biroq amaliy tizimlarda ma'lumotlar turli tashkilotlarda saqlanadi va ularni bir joyga yig'ish huquqiy, iqtisodiy yoki axloqiy jihatdan maqbul bo'lmasligi mumkin. Masalan, tibbiyot muassasalari bemor ma'lumotlarini, banklar tranzaksiya tarixlarini, davlat idoralari esa fuqarolarga oid yozuvlarni tashqi tizimga uzatishda qat'iy cheklavlarga duch keladi.

Federativ o'qitish ma'lumotlarni markazlashtirish o'rniga modelni ma'lumotlar saqlanayotgan joylarda o'qitish va mahalliy yangilanishlarni birlashtirish g'oyasiga asoslanadi. McMahan va hammualliflar FedAvg usulini taklif qilib, model yangilanishlarini agregatsiya qilish orqali taqsimlangan



qurilmalarda o'qitish mumkinligini ko'rsatgan [1]. Keyingi keng qamrovli tahlillar FLning maxfiylik, aloqa xarajatlari, statistik heterogenlik va mustahkamlik bilan bog'liq ochiq muammolarini tizimlashtirgan [2].

Shunga qaramay, xom ma'lumotlarning serverga yuborilmasligi maxfiylik to'liq ta'minlanganini anglatmaydi. Model yangilanishlari orqali ma'lumotlarni taxmin qilish, zararli ishtirokchilarning noto'g'ri yangilanish yuborishi, markaziy serverning ortiqcha ma'lumot to'plashi va noto'g'ri konfiguratsiya kabi xatarlar mavjud. Shuning uchun federativ o'qitish texnik algoritm sifatida emas, balki xavfsizlik, boshqaruv va baholash talablarini qamrab olgan tizim sifatida loyihalanishi kerak [2, 3].

Maqolaning maqsadi — tashkilotlararo hamkorlikda federativ o'qitish tizimini yaratish uchun maxfiylik va model sifatini birgalikda nazorat qiladigan metodologik yondashuvni ishlab chiqish. Maqolaning hissasi xavf modeli, arxitektura, joriy etish bosqichlari va baholash ko'rsatkichlarini bitta takror ishlab bo'ladigan protokolga birlashtirishdan iborat.

2. Muammo va tadqiqot savollari

Markazlashtirilgan o'qitishda barcha ishtirokchilar ma'lumotlari yagona muhitga ko'chiriladi. Bu yondashuv ma'lumotlarni boshqarish va hisoblashni soddalashtirishi mumkin, biroq ma'lumotlar nusxalari sonini ko'paytiradi va buzilish sodir bo'lganda ta'sir doirasini kengaytiradi. Federativ o'qitish ma'lumotlar joylashuvini saqlab qoladi, ammo ishonchli hisoblash, yangilanishlarni himoyalash va ishtirokchilar o'rtasidagi farqlarni boshqarish zaruratini tug'diradi.

Tadqiqot quyidagi savollarni ko'rib chiqadi:

- TQ1: Federativ o'qitishda qanday maxfiylik va xavfsizlik xatarlarini tizimli ravishda hisobga olish kerak?
- TQ2: Mahalliy o'qitish, xavfsiz agregatsiya va differensial maxfiylikni qanday arxitektura doirasida birlashtirish mumkin?



- TQ3: Model sifati, maxfiylik xarajati va aloqa samaradorligi o'rtasidagi muvozanatni qanday baholash lozim?

3. Adabiyotlar tahlili

3.1. Federativ o'qitishning asosiy tamoyili

McMahan va hammualliflarning FedAvg yondashuvida har bir mijoz o'z mahalliy ma'lumotlarida bir necha o'qitish qadamini bajaradi, so'ng yangilanishlar serverda birlashtiriladi [1]. Bu yondashuv xom ma'lumotlarni uzatish ehtiyojini kamaytiradi va aloqa xarajatlarini pasaytirishi mumkin. Biroq samaradorlik mijozlarning ma'lumot hajmi, tarmoq barqarorligi va ma'lumotlar taqsimotining bir-biridan farq qilishiga bog'liq.

3.2. Maxfiylik va xavfsizlik muammolari

Kairouz va hammualliflar federativ o'qitishning nazariy va amaliy muammolarini keng tahlil qilib, maxfiylik, aloqa, statistik heterogenlik, adolat va mustahkamlikni muhim yo'nalishlar sifatida ko'rsatadi [2]. FL xom ma'lumotlarni markazlashtirmasligi bilan ma'lumotlar minimallashtirish tamoyiliga mos keladi, lekin model yangilanishlari o'zlari ham nozik axborot haqida ma'lumot berishi ehtimoli bor. Shu sababli xavfsizlikni faqat ma'lumotlarning joyida qolishi bilan o'lchash yetarli emas.

3.3. Tibbiyot va maxfiy ma'lumotlar bilan ishlash

Kaissis va hammualliflar tibbiy tasvirlar kontekstida federativ va maxfiylikni saqlovchi mashinaviy o'qitish yondashuvlari, tahdidlar va istiqbollarni ko'rib chiqadi [3]. Tibbiy ma'lumotlar bilan ishlash tajribasi boshqa tartibga solinadigan sohalar uchun ham foydali: texnik arxitektura bilan bir qatorda ma'lumotlardan foydalanish huquqi, xavfsizlik auditi va operatsion boshqaruv muhim bo'lib qoladi.

3.4. Differensial maxfiylik va xavfsiz agregatsiya

Differensial maxfiylik (DP) algoritm natijasi alohida bir yozuvning mavjudligiga qanchalik bog'liqligini matematik tarzda cheklash uchun



ishlatiladi. Amaliy FL tizimida DP ko'pincha gradientlarni kesish va nazoratli shovqin qo'shish orqali qo'llanishi mumkin, biroq maxfiylik darajasi bilan model aniqligi o'rtasida murosasiz yuzaga keladi. Xavfsiz agregatsiya esa serverga individual yangilanishlarni emas, ularning yig'indisini ko'rish imkonini berishga qaratilgan kriptografik protokollar oilasidir. Ushbu mexanizmlar turli tahdidlarga qarshi ishlaydi; birini qo'llash ikkinchisiga bo'lgan ehtiyojni avtomatik yo'q qilmaydi.

4. Tadqiqot metodologiyasi

4.1. Tadqiqot dizayni

Maqola metodologik-tahliliy sintez sifatida ishlab chiqildi. Asosiy ilmiy manbalar federativ o'qitishning asosiy algoritmi, ochiq muammolari va maxfiylikni saqlovchi mashinaviy o'qitish bo'yicha ko'p iqtibosli tadqiqotlardan tanlandi. Maqsad tizimli sharh yoki meta-tahlil o'tkazilganini da'vo qilish emas; mavjud natijalardan amaliy joriy etish protokolini shakllantirishdir. Ushbu maqolada yangi model o'qitilmagan va empirik ko'rsatkichlar o'lchanmagan.

4.2. Tahdid modeli

Tahdid	Tavsif	Tavsiya etiladigan nazorat
Yangilanishlardan axborot sizishi	Model yangilanishlari ayrim xususiyatlar yoki o'qitish namunalarini oshkor qilishi mumkin.	Tahdidga mos DP, xavfsiz agregatsiya, kirish nazorati va audit.
Zararli yoki nosoz ishtirokchi	Mijoz ataylab yoki xato tufayli noto'g'ri yangilanish yuboradi.	Yangilanishlarni tekshirish, anomaliya tahlili, ishtirokchilarni autentifikatsiya qilish.
Serverning ortiqcha kuzatuvi	Markaziy koordinator individual yangilanishlarni	Secure aggregation, minimal loglash, rollarga





	ko'rishi yoki saqlashi mumkin.	asoslangan kirish.
Ma'lumotlar heterogenligi	Tashkilotlarda ma'lumotlar miqdori va taqsimoti farq qiladi.	Mijoz kesimidagi baholash, mos agregatsiya va adolat tahlili.
Operatsion yoki konfiguratsion xato	Kalitlar, model versiyalari yoki ruxsatlar noto'g'ri boshqariladi.	Kalitlar hayotiy sikli, versiyalash, monitoring va mustaqil xavfsizlik auditi.

1-jadval. Federativ o'qitish tizimi uchun namunaviy tahdid modeli.

4.3. Taklif etilayotgan tizim arxitekturası

Tizim besh mantiqiy qatlamdan tashkil topadi: (1) ma'lumotlar egasi bo'lgan tashkilotlar; (2) mahalliy o'qitish muhiti; (3) yangilanishlarni himoyalash qatlami; (4) agregatsiya va global modelni tarqatish; (5) baholash, audit va boshqaruv. Har bir ishtirokchi xom ma'lumotni o'z nazorati ostida saqlaydi. Mahalliy jarayon faqat model yangilanishlarini tayyorlaydi; ushbu yangilanishlar belgilangan himoya protokoli orqali koordinatorga uzatiladi. Koordinator umumlashtirilgan modelni hisoblab, keyingi raund uchun ishtirokchilarga yuboradi.

Bosqich	Kirish	Amal	Chiqish
1. Mahalliy tayyorlash	Mahalliy, ruxsat etilgan ma'lumotlar	Sifat tekshiruvi, tozalash, ma'lumotlar siyosatini qo'llash	Mahalliy o'qitishga tayyor to'plam
2. Mahalliy o'qitish	Joriy global model va mahalliy to'plam	Belgilangan epoch/iteratsiyalar bo'yicha o'qitish	Mahalliy model yangilanishi
3. Yangilanishni himoyalash	Mahalliy yangilanish	Kesish, shifrlash yoki xavfsiz agregatsiya protokoliga	Himoyalangan yangilanish

		tayyorlash; kerak bo'lsa DP	
4. Agregatsiya	Bir nechta ishtirokchining yangilanishlari	Ruxsat etilgan agregatsiya algoritmini bajarish	Yangilangan global model
5. Tekshirish va tarqatish	Global model va audit jurnali	Sifat, maxfiylik budjeti va xavfsizlik nazorati	Qabul qilingan model yoki qaytarish qarori

2-jadval. Federativ o'qitishning taklif etilayotgan operatsion sikli.

4.4. Algoritmik jarayon

Tavsiya etiladigan umumiy jarayon quyidagicha: server dastlabki global modelni va konfiguratsiyani belgilaydi; har bir tanlangan mijoz modelning nusxasini oladi va o'z ma'lumotlarida mahalliy o'qitishni bajaradi; yangilanishlar himoyalash qatlamidan o'tadi; server belgilangan qoidalar asosida ularni birlashtiradi; yangi global model mustaqil tekshiruv to'plamida baholanadi; mezonlar bajarilsa keyingi raund boshlanadi, aks holda model qaytariladi yoki konfiguratsiya qayta ko'rib chiqiladi.

Oddiy FedAvg agregatsiyasini quyidagicha ifodalash mumkin: $w_{(t+1)} = \sum_k (n_k / \sum_j n_j) w_{(t+1)}^k$, bunda $w_{(t+1)}^k$ — k-mijozning mahalliy o'qitishdan keyingi parametrlari, n_k — uning mahalliy namunalar soni. Ushbu formula asosiy tushuntirish uchun keltirilgan; amaliy xavfsiz agregatsiya, differensial maxfiylik yoki zararli mijozlardan himoya uchun qo'shimcha mexanizmlar talab qilinishi mumkin.

4.5. Maxfiylik va xavfsizlik nazoratlari

- Ma'lumotlarni minimallashtirish: faqat vazifa uchun zarur va qonuniy foydalanish huquqi mavjud ma'lumotlarni mahalliy muhitda ishlatish.
- Autentifikatsiya va ruxsatlar: ishtirokchi tashkilotlar hamda servislar uchun o'zaro autentifikatsiya va eng kam vakolat tamoyili.



- Xavfsiz agregatsiya: individual yangilanishlarni koordinatorga ochmaslikka qaratilgan protokolni tanlangan tahdid modeliga muvofiq joriy etish.
- Differensial maxfiylik: zarur bo'lganda maxfiylik parametrlarini, kompozitsiya hisobini va maxfiylik budjetini hujjatlashtirish.
- Model yangilanishlarini tekshirish: o'lcham, norma, yo'nalish va kutilmagan o'zgarishlarni monitoring qilish; bu tekshiruvlar barcha hujumlarni aniqlashini kafolatlamasligini hisobga olish.
- Audit va versiyalash: model, ma'lumotlar siyosati, konfiguratsiya, ishtirokchi ro'yxati va o'qitish raundlarini qayd etish.

5. Baholash metodologiyasi

Federativ o'qitish muvaffaqiyati faqat global model aniqligi bilan o'lchanmasligi kerak. Baholash kamida to'rt yo'nalishni qamrab olishi tavsiya etiladi: model foydaliligi, maxfiylik, tizim samaradorligi va ishtirokchilar o'rtasidagi natijalar farqi.

Yo'nalish	Ko'rsatkichlar	Talqin
Model foydaliligi	Vazifaga mos metrikalar: F1, AUC, MAE/RMSE yoki tegishli ko'rsatkich	Markazlashtirilgan boshlang'ich model va FL natijasi bilan bir xil test to'plamida taqqoslash.
Maxfiylik	DP ishlatilsa ϵ va δ ; xavfsiz agregatsiya sozlamalari; ma'lumot sizishi sinovlari	Parametrlar faqat model sifati bilan birga va tahdid modeli doirasida talqin qilinadi.
Tizim samaradorligi	Raundlar soni, aloqa hajmi, o'qitish vaqti, uzilishlar	Amaliy infratuzilma xarajatlari va kengayish imkoniyatini baholash.
Ishtirokchilar kesimidagi adolat	Har bir tashkilot bo'yicha metrikalar, eng yomon guruh natijasi, dispersiya	Global o'rtacha ko'rsatkich zaif ishtirokchilar natijasini yashirmasligi kerak.



Mustahkamlik	Nosoz mijozlar, notekis taqsimot va uzilishlar ostidagi natijalar	Model va jarayonning real sharoitlarga chidamliligini tekshirish.
--------------	---	---

3-jadval. Federativ o'qitishni baholash uchun ko'rsatkichlar to'plami.

5.1. Tajriba dizayni bo'yicha tavsiya

Metodologiyani amaliy sinash uchun kamida uchta konfiguratsiyani taqqoslash mumkin: (A) markazlashtirilgan o'qitish — faqat ma'lumotlarni qonuniy va xavfsiz birlashtirish mumkin bo'lgan nazorat sharoitida; (B) himoya mexanizmlarisiz bazaviy FL; (C) xavfsiz agregatsiya va zarur bo'lsa differensial maxfiylik bilan FL. Agar markazlashtirilgan ma'lumotlar bazasini yaratish huquqiy yoki axloqiy jihatdan mumkin bo'lmasa, A konfiguratsiyasi real joriy etish emas, balki mavjud bo'lsa simulyatsion yuqori chegara sifatida ko'rilishi kerak.

Tajriba uchun ma'lumotlar hajmi, mijozlar soni, har bir mijozdagi namunalar soni, taqsimot heterogenligi, o'qitish raundlari, model arxitekturasi, optimizator, boshlang'ich urug' (seed), apparat va tarmoq sharoitlari qayd etiladi. Natijalar bir necha mustaqil ishga tushirish bo'yicha o'rtacha va dispersiya bilan e'lon qilinishi, sinov to'plami esa o'qitish jarayonidan ajratilishi kerak.

Ushbu maqolada bunday tajriba bajarilmagan. Shu bois hech qanday aniqlik, tezlik yoki maxfiylik bo'yicha raqamli ustunlik da'vo qilinmaydi.

6. Muhokama

Taklif etilgan metodologiya federativ o'qitishni faqat algoritm tanlash vazifasi sifatida emas, balki ko'p tashkilotli boshqaruv tizimi sifatida ko'radi. Har bir tashkilot ma'lumotlardan foydalanish huquqi, mahalliy xavfsizlik, o'qitish resurslari va modeldan foydalanish shartlari bo'yicha aniq javobgarlikka ega bo'lishi kerak. Markaziy koordinator esa konfiguratsiya va agregatsiya jarayonini boshqarsa-da, barcha xom ma'lumotlarga egalik qiluvchi markazga aylanmasligi lozim.



Maxfiylik mexanizmlarini tanlash tahdid modeliga bog'liq. Xavfsiz agregatsiya serverning individual yangilanishlarni ko'rish imkoniyatini kamaytiradi, ammo yakuniy modelning o'zidan kelib chiqadigan barcha axborot sizishi xavflarini yo'q qilmaydi. Differensial maxfiylik matematik kafolat beradi, lekin uning foydasi maxfiylik parametrlari, shovqin mexanizmi va takroriy o'qitish raundlari bilan bog'liq. Shuning uchun mexanizmlar bir-birini to'ldirishi mumkin, ammo har biri alohida hujjatlashtirilishi zarur [2, 3].

Yana bir muhim masala — ma'lumotlar heterogenligi. Tashkilotlarning ma'lumotlari bir xil taqsimotdan kelmasligi mumkin; ayrim mijozlarda namuna soni kam, ayrimlarida esa noyob guruhlar ko'p bo'ladi. Global o'rtacha ko'rsatkich barcha ishtirokchilar uchun foyda bir xil ekanini bildirmaydi. Shu sababli model sifati tashkilotlar va muhim guruhlar kesimida baholanishi lozim.

Metodologiyaning cheklovlari mavjud. Birinchidan, maqola konseptual protokol bo'lib, amaliy samaradorligi hali tajribada tekshirilmagan. Ikkinchidan, xavfsiz agregatsiya va differensial maxfiylikni amalga oshirish aniq platforma, model, tahdid modeli va qonunchilikka moslashtirishni talab qiladi. Uchinchidan, federativ o'qitish ma'lumotlar sifati, noto'g'ri yorliqlar yoki tashkilotlararo nomuvofiq siyosatlarni avtomatik ravishda hal qilmaydi.

7. Amaliy joriy etish bo'yicha tavsiyalar

- Avval vazifani va ma'lumotlardan foydalanish huquqini aniqlash; FLni faqat “moda” bo'lgani uchun tanlamaslik.
- Tashkilotlar, server, mijozlar va potensial zararli ishtirokchilarni o'z ichiga olgan aniq tahdid modelini hujjatlashtirish.
- Kichik pilotda bazaviy model, FL konfiguratsiyasi va mustaqil test to'plamini tayyorlash.
- Xavfsiz agregatsiya va DP zaruratini xavf tahliliga ko'ra tanlash; maxfiylik parametrlarini asoslash.
- Global metrikalar bilan birga mijozlar kesimidagi natijalar, aloqa xarajatlari va muvaffaqiyatsiz raundlarni kuzatish.



- Model versiyalari, audit jurnallari, ma'lumotlar siyosati va hodisalarga javob berish tartibini belgilash.

- Joriy etishdan oldin mustaqil xavfsizlik tekshiruvi, huquqiy ko'rib chiqish va modelning real foydalanish sharoitidagi monitoringini tashkil etish.

8. Xulosa

Maqolada maxfiy ma'lumotlarni markazlashtirmasdan sun'iy intellekt modelini hamkorlikda o'qitish uchun federativ o'qitishga asoslangan metodologik yondashuv taklif qilindi. Yondashuv mahalliy o'qitish, yangilanishlarni himoyalash, agregatsiya, global modelni tekshirish va auditni yagona operatsion siklga birlashtiradi. Shuningdek, model foydaliligi, maxfiylik, tizim samaradorligi va ishtirokchilar kesimidagi adolatni alohida baholash zarurligi asoslandi.

Asosiy xulosa shuki, federativ o'qitish xom ma'lumotlarni markazlashtirish ehtiyojini kamaytirishi mumkin, biroq o'z-o'zidan to'liq maxfiylik yoki xavfsizlik kafolati bermaydi. Amaliy tizimda xavfsiz agregatsiya, zarur holatda differensial maxfiylik, qat'iy autentifikatsiya, audit va statistik baholash birgalikda ko'rib chiqilishi lozim. Keyingi tadqiqot bosqichida ushbu protokolni real yoki sintetik taqsimlangan ma'lumotlar muhitida sinash, turli himoya sozlamalarining model foydaliligiga ta'sirini o'lchash va natijalarni takror ishlab bo'ladigan shaklda e'lon qilish tavsiya etiladi.

Foydalanilgan adabiyotlar

[1] McMahan, B., Moore, E., Ramage, D., Hampson, S., & Agüera y Arcas, B. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 54, 1273–1282. <https://proceedings.mlr.press/v54/mcmahan17a.html>





[2] Kairouz, P., McMahan, H. B., Avent, B., et al. (2021). Advances and Open Problems in Federated Learning. *Foundations and Trends in Machine Learning*, 14(1–2), 1–210. <https://doi.org/10.1561/22000000083>

[3] Kaissis, G. A., Makowski, M. R., Rückert, D., & Braren, R. F. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. *Nature Machine Intelligence*, 2, 305–311. <https://doi.org/10.1038/s42256-020-0186-1>

[4] Dwork, C., & Roth, A. (2014). The Algorithmic Foundations of Differential Privacy. *Foundations and Trends in Theoretical Computer Science*, 9(3–4), 211–407. <https://doi.org/10.1561/04000000042>

[5] Bonawitz, K., Ivanov, V., Kreuter, B., et al. (2017). Practical Secure Aggregation for Privacy-Preserving Machine Learning. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1175–1191. <https://doi.org/10.1145/3133956.3133982>

[6] Rieke, N., Hancox, J., Li, W., et al. (2020). The future of digital health with federated learning. *npj Digital Medicine*, 3, Article 119. <https://doi.org/10.1038/s41746-020-00323-1>

[7] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated Learning: Challenges, Methods, and Future Directions. *IEEE Signal Processing Magazine*, 37(3), 50–60. <https://doi.org/10.1109/MSP.2020.2975749>