تحلیل جامع یادگیری فدرال

محمدرضا باقرنژاد

۲۹ اسفند ۱۴۰۳

فهرست مطالب

۱ مقدمه

هوش مصنوعی (AI) و یادگیری عمیق (Deep Learning) تحولی عظیم در فناوری ایجاد کرده‌اند و در حوزه‌های مختلفی از پزشکی تا صنایع خودروسازی کاربرد دارند. اما این مدل‌های یادگیری اغلب به **حجم عظیمی از داده‌ها** و **قدرت پردازشی بالا** نیاز دارند که منجر به استفاده گسترده از **مدل‌های متمرکز** (Centralized ML) شده است.

با ظهور **نگرانی‌های امنیتی و حریم خصوصی**، جمع‌آوری داده‌های کاربران به چالش کشیده شده و روش‌های سنتی با مشکلاتی روبه‌رو هستند. در پاسخ به این چالش‌ها، **یادگیری فدرال (Federated Learning - FL)** معرفی شده است که به مدل‌ها اجازه می‌دهد **بدون ارسال داده به سرور مرکزی، یادگیری را به‌صورت توزیع‌شده انجام دهند**.

۱.۱ دلایل استفاده از یادگیری فدرال

برخی از دلایل اصلی نیاز به FL عبارتند از:

- افزایش **نگرانی‌های حریم خصوصی** در پردازش داده‌های کاربران.
- کاهش **هزینه‌های انتقال داده** بین سرور مرکزی و دستگاه‌ها.
- بهره‌گیری از **محاسبات لبه‌ای (Edge Computing)** برای کاهش تأخیر در پاسخ‌دهی.
- افزایش **مقیاس‌پذیری سیستم‌های یادگیری ماشین**.

۲ معرفی یادگیری فدرال

در این بخش، به اصول یادگیری فدرال پرداخته می‌شود.

۱.۲ مؤلفه‌های کلیدی در یادگیری فدرال

یادگیری فدرال به عنوان یک پارادایم توزیع‌شده در یادگیری ماشین، امکان توسعه‌ی یک مدل یادگیری ماشین را بدون نیاز به اشتراک‌گذاری مستقیم داده‌ها میان شرکت‌کنندگان فراهم می‌کند. این فرایند شامل دو مرحله‌ی اصلی است:

۱. **مرحله‌ی آموزش مدل:** در این مرحله، هر مشتری (مالک داده) بدون افشای داده‌های خود، اطلاعات را مبادله کرده و به‌طور مشترک یک مدل یادگیری ماشین را آموزش می‌دهد. هر مشتری یک مدل یادگیری محلی را روی داده‌های خود آموزش داده و به‌جای اشتراک‌گذاری داده‌ها، تنها اطلاعات مدل یادگیری خود را ارسال می‌کند. سپس مدل‌های محلی آموزش‌دیده‌شده تجمیع شده و یک مدل یادگیری جهانی ایجاد می‌شود.

۲. **مرحله‌ی استنتاج:** در این مرحله، مدل یادگیری جهانی آموزش‌یافته برای تحلیل داده‌های جدید استفاده می‌شود. این فرایند می‌تواند به‌صورت **همگام** یا **ناهمگام** انجام شود که وابسته به در دسترس بودن داده‌های هر گره و مدل آموزش‌دیده است.

۲.۲ فرایند یادگیری فدرال

فرایند یادگیری فدرال شامل چهار مرحله‌ی اصلی است:

۱. **آموزش محلی (Local Training)**: هر مشتری، مدل محلی خود را با استفاده از داده‌های خصوصی خود آموزش داده و پارامترهای مدل را به‌روزرسانی می‌کند.

۲. **ارتباطات (Communication)**: به‌روزرسانی‌های مدل از مشتریان محلی به سرور مرکزی یا شبکه‌ی توزیع‌شده منتقل می‌شود. ارتباطات نقش مهمی در هماهنگی به‌روزرسانی‌ها و حفظ حریم خصوصی داده‌ها ایفا می‌کنند.

۳. **تجمیع مدل‌ها (Aggregation)**: سرور مرکزی یا شبکه‌ی توزیع‌شده، مدل‌های محلی را با استفاده از الگوریتم‌های تجمیع ترکیب کرده و مدل جهانی را تولید می‌کند.

۴. **به‌روزرسانی محلی (Local Update)**: مدل جهانی سراسری به مشتریان محلی ارسال می‌شود تا جایگزین مدل قبلی آن‌ها شود یا با آن ترکیب گردد.

فرایند فوق تا زمانی که یک **معیار توقف** مشخص برآورده شود، تکرار می‌شود.

۳.۲ معماری‌های مختلف یادگیری فدرال

ترکیب مؤلفه‌های کلیدی یادگیری فدرال منجر به ایجاد چندین معماری مختلف می‌شود که تعامل بین اجزا را تعریف می‌کند. این معماری‌ها به دو دسته‌ی اصلی تقسیم می‌شوند: معماری **مشتری-سرور** و معماری **نظیر-به-نظیر**.

۱. **معماری مشتری-سرور**: در این معماری، یک گره‌ی مرکزی به نام **سرور** مسئول هماهنگی و تجمیع به‌روزرسانی‌های مدل است. سایر گره‌ها که مالک داده‌ها هستند و مدل‌های محلی خود را آموزش می‌دهند، به عنوان **مشتری** شناخته می‌شوند. این معماری پیاده‌سازی آسانی دارد، اما به دلیل وابستگی زیاد به سرور مرکزی، در برابر حملات آسیب‌پذیر است. به‌عنوان مثال، اگر سرور مورد حمله قرار گیرد، کل فرآیند یادگیری مختل خواهد شد. شکل 3 این معماری را نمایش می‌دهد.

۲. **معماری نظیر-به-نظیر**: در این معماری، تمامی گره‌ها هم مالک داده هستند و هم به‌روزرسانی‌های مدل سایر گره‌ها را تجمیع می‌کنند. برخلاف روش مشتری-سرور، در این روش هیچ هماهنگ‌کننده‌ی ثابتی وجود ندارد. در حالی که این معماری پیچیدگی پیاده‌سازی بیشتری دارد و هزینه‌های ارتباطی بالاتر است، اما امنیت و حفظ حریم خصوصی داده‌ها را بهبود می‌بخشد. در این معماری، هر گره به‌صورت محلی داده‌های خود را آموزش داده و مدل خود را به‌روزرسانی می‌کند، سپس این مدل‌ها در فرآیند تجمیع بین گره‌ها ادغام می‌شوند. شکل 4 این معماری را نمایش می‌دهد.

به‌طور کلی، معماری **مشتری-سرور** رایج‌ترین معماری در یادگیری فدرال است و در اغلب موارد به عنوان معماری پیش‌فرض در نظر گرفته می‌شود.

۴.۲ دسته‌بندی‌های یادگیری فدرال

یادگیری فدرال بسته به ویژگی‌های عناصر کلیدی، به چندین دسته تقسیم می‌شود. یکی از مهم‌ترین این ویژگی‌ها، **ماهیت داده‌های توزیع‌شده** است که تأثیر مستقیمی بر دسته‌بندی‌های مختلف یادگیری فدرال دارد.
بر اساس شیوه‌ی توزیع داده‌ها در میان مشتریان، یادگیری فدرال در سه دسته‌ی اصلی زیر طبقه‌بندی می‌شود:

۱. **یادگیری فدرال افقی** (HFL): در این روش، داده‌ها بر اساس نمونه‌ها میان مشتریان توزیع شده‌اند، به این معنا که هر مشتری مجموعه‌ای متفاوت از نمونه‌های داده را در اختیار دارد، اما ویژگی‌ها (Feature Space) و برچسب‌ها (Label Space) میان همه‌ی مشتریان یکسان است. به‌صورت ریاضی می‌توان این روش را به‌صورت زیر تعریف کرد:

$$X_i = X_j, \quad Y_i = Y_j, \quad I_i \neq I_j, \quad \forall D_i, D_j, \quad i \neq j$$

که در آن:

- X_i, X_j فضای ویژگی مشتریان i و j را نشان می‌دهد که یکسان هستند.
- Y_i, Y_j فضای برچسب داده‌ها است که میان مشتریان یکسان است.
- I_i, I_j مجموعه نمونه‌های داده است که در بین مشتریان متفاوت است.

این روش مناسب برای آموزش مدل‌هایی است که داده‌های آن‌ها از دستگاه‌های مشابه (مانند گوشی‌های هوشمند یا دستگاه‌های IoT) جمع‌آوری شده است.

۲. **یادگیری فدرال عمودی** (VFL): در این روش، داده‌ها بر اساس ویژگی‌ها میان مشتریان توزیع شده‌اند، به این معنا که هر مشتری مجموعه‌ی یکسانی از نمونه‌های داده را دارد، اما ویژگی‌های داده‌ها میان مشتریان متفاوت است. به‌صورت ریاضی می‌توان این روش را به‌صورت زیر تعریف کرد:

$$X_i \neq X_j, \quad Y_i \neq Y_j, \quad I_i = I_j, \quad \forall D_i, D_j, \quad i \neq j$$

در این روش، داده‌های هر مشتری بخشی از اطلاعات را در مورد یک نمونه‌ی خاص ارائه می‌دهد. این نوع یادگیری فدرال برای حالاتی مفید است که در آن اطلاعات از منابع مختلف با ویژگی‌های متفاوت جمع‌آوری شده‌اند. به عنوان مثال، بیمارستان‌های مختلف ممکن است داده‌های پزشکی متفاوتی درباره‌ی بیماران یکسان داشته باشند که با ترکیب آن‌ها، دقت مدل بهبود می‌یابد.

۳. **یادگیری فدرال انتقالی** (FTL): در این روش، دانش از یک دامنه‌ی داده‌ای به دامنه‌ای دیگر منتقل می‌شود، بدون اینکه نمونه‌ها یا ویژگی‌های داده‌ای میان مشتریان هم‌پوشانی داشته باشند. این روش به‌صورت ریاضی به‌صورت زیر تعریف می‌شود:

$$X_i \neq X_j, \quad Y_i \neq Y_j, \quad I_i \neq I_j, \quad \forall D_i, D_j, \quad i \neq j$$

این روش معمولاً در ترکیب با تکنیک‌های Fine-Tuning و مدل‌های از پیش آموزش‌دیده‌شده (Pretrained Models) در مجموعه داده‌های متمرکز استفاده می‌شود.

هر یک از این سه نوع یادگیری فدرال، بسته به نوع داده‌ها و کاربرد موردنظر، در شرایط مختلف مورد استفاده قرار می‌گیرند.

۳ مجموعه داده‌های فدرال و چارچوب‌های نرم‌افزاری پیشرفته

این بخش، اکوسیستم موجود برای طراحی مدل‌ها و مطالعات در سناریوهای فدرال را معرفی می‌کند.

۱.۳ مجموعه داده‌های فدرال

مجموعه داده‌های مربوط به وظایف سنتی یادگیری ماشین متمرکز می‌توانند برای شبیه‌سازی‌های مقاصد مختلف مورد استفاده قرار گیرند، با تقسیم مصنوعی و اشتراک‌گذاری داده‌ها بین طرف‌های مختلف برای تطبیق با سناریوهای فدرال. با این حال، برخی از مجموعه داده‌ها به طور ذاتی فدرال محسوب می‌شوند به دلیل ویژگی‌ها یا توزیع داده‌های آن‌ها.

مجموعه داده‌های فدرال

مجموعه داده	وظیفه	مجموعه داده‌ها	مشتری‌ها	توزیع فدرال
CelebA	طبقه‌بندی تصویر	200,288	9343	بله
Cifar100	طبقه‌بندی تصویر	60,000	-	خیر
Fashion MNIST	طبقه‌بندی تصویر	70,000	-	خیر
FEMNIST	طبقه‌بندی تصویر	805,263	3550	بله
Google landmark v2	طبقه‌بندی تصویر	164,172	1262	بله
iNaturalist	طبقه‌بندی تصویر	155,941	9275	بله
MedMNIST	طبقه‌بندی تصویر	708,069	-	خیر
MNIST	طبقه‌بندی تصویر	70,000	-	خیر
Shakespeare	پیش‌بینی متن	4,226,150	1129	بله
Reddit	پیش‌بینی متن	56,587,343	1,660,820	بله
Stack Overflow	پیش‌بینی متن	168,895,995	585,323	بله
Sentiment140	تحلیل احساسات	1,600,498	660,120	بله
Adult	طبقه‌بندی	48,842	-	خیر
Credit2	طبقه‌بندی	30,000	-	خیر

۲.۳ چارچوب‌های نرم‌افزاری پیشرفته برای Federated Learning

در هنگام توسعه آزمایش‌ها برای یک سناریوی فدرال، چارچوب‌های متعددی برای این کار طراحی شده‌اند. ما به دنبال چارچوب‌های متن‌باز پیشرفته موجود در این زمینه بوده و برخی جنبه‌های مهم FL را برای بررسی میزان پوشش آن‌ها در این چارچوب‌ها انتخاب کرده‌ایم. این جدول می‌تواند به کاربران کمک کند تا چارچوب مناسب برای آزمایش‌های خود را انتخاب کنند. به دلیل محدودیت فضا و تعداد زیاد چارچوب‌ها، نام آن‌ها در جدول به شکل اختصاری آورده شده است.

چارچوب‌های بررسی‌شده عبارتند از: PySyft (PyS)، TensorFlow Federated (TFF)، FATE (FAT)، PaddleFL (Pad)، Flower (Flo)، Xaynet (Xay)، IBM FL (IBM)، Substra (Sub)، OpenFL (OFL)، FedML (FML)، FedJax (FJx)، Backdoors 101 (101)، FedLab (FLb)، SimFL (SFL)، easyFL (EFL)، TorchFL (TFL)، APPFL (AFL)، NVFlare (NVF).

۱.۲.۳ الف) میزان تطابق هر چارچوب

سه سطح تطابق برای مشخص کردن اینکه آیا یک ویژگی توسط چارچوب پشتیبانی می‌شود یا خیر در نظر گرفته شده است:

- **نقاط سبز:** نشان‌دهنده پشتیبانی کامل از ویژگی مربوطه هستند.
- **نقاط نارنجی:** نشان می‌دهند که ویژگی تا حدی در چارچوب پوشش داده شده است، یعنی برخی موارد را پشتیبانی می‌کند اما نه همه را.
- **نقاط قرمز:** نشان‌دهنده این هستند که ویژگی در چارچوب پشتیبانی نمی‌شود.
- **نقاط خاکستری:** نشان می‌دهند که تعیین دقیق پشتیبانی یا عدم پشتیبانی این ویژگی ممکن نبوده است.

۲.۲.۳ ب) جنبه‌های پوشش داده‌شده توسط هر چارچوب

جدول به چهار گروه افقی تقسیم شده است:

- در گروه اول، جنبه‌های اصلی FL بررسی می‌شوند، از جمله پشتیبانی از اجرای الگوریتم‌های HFL، VFL و FTL.
- گروه دوم بررسی می‌کند که آیا چارچوب‌ها از فریم‌ورک‌های یادگیری ماشین رایج مانند TensorFlow، PyTorch یا Scikit-Learn پشتیبانی می‌کنند.
- گروه سوم بررسی می‌کند که آیا چارچوب‌ها از نمونه‌گیری داده‌های IID و non-IID پشتیبانی می‌کنند و آیا شامل طیف وسیعی از مکانیزم‌های تجمیع فدرال ارائه‌شده در ادبیات هستند.
- در گروه چهارم، ویژگی‌های پیشرفته‌تری بررسی می‌شوند، مانند قابلیت تفسیرپذیری مدل‌ها، پشتیبانی از شخصی‌سازی مدل در سمت مشتری، مستندات جامع یا API سطح بالا، قابلیت گسترش چارچوب توسط کاربر، و میزان نگهداری و به‌روزرسانی فعال چارچوب.

پدث

	PyS	TFF	FAT	Pad	Flo	Xay	IBM	Sub	OFL	FML	FJx	101	FLb	SFL	EFL	TFL	AFL	NVF
Federated Learning:																		
Horizontal Federated Learning	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Vertical Federated Learning	◑	×	●	●	×	×	×	×	◑	●	×	×	×	×	×	×	×	×
Federated Transfer Learning	×	×	◑	◑	×	×	×	×	×	×	×	×	×	×	×	×	×	●
Support other ML frameworks	●	●	×	×	●	●	●	●	●	●	×	×	◑	×	×	◑	◑	●
Sampling IID or non-IID distribution	●	◑	×	–	×	×	×	×	×	×	×	×	◑	◑	●	●	×	◑
Federated aggregation mechanisms	◑	◑	◑	◑	◑	◑	◑	◑	◑	◑	◑	–	◑	◑	●	◑	●	◑
Adversarial Attacks in FL:																		
Privacy attacks	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Defenses against Privacy attacks	◑	×	◑	◑	×	◑	◑	×	×	×	×	×	×	×	×	×	×	×
Attacks to the federated model	×	×	×	×	×	×	×	×	×	◑	×	●	×	×	×	×	×	×
Defenses against attacks to the model	◑	×	◑	◑	×	◑	◑	×	×	×	×	◑	×	×	×	×	×	×
Differential Privacy (DP):																		
Mechanisms: Exponential, Laplacian...	◑	◑	×	◑	◑	×	×	×	◑	×	×	×	×	×	×	×	◑	●
Subsampling methods to increase privacy	×	◑	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Advanced (DP) Composition	×	●	×	×	×	×	×	●	×	×	×	×	×	×	×	×	×	×
Advanced Properties:																		
Interpretability / Explainability	×	×	◑	×	×	×	◑	×	×	×	×	×	×	×	×	×	×	×
Personalization	×	×	×	×	×	×	×	×	×	×	×	×	◑	×	×	×	×	×
Documentation and tutorials	●	●	●	◑	●	×	●	◑	●	●	●	×	◑	×	×	●	◑	◑
High-level API	×	●	●	–	●	×	●	◑	●	●	●	●	●	◑	●	●	●	◑
Ability to extend the framework	●	●	◑	–	●	–	–	◑	●	●	●	●	◑	×	–	●	●	◑
Actively maintained	●	●	●	●	●	×	●	●	●	●	●	◑	●	×	●	●	●	●

شکل ۱: جدول مربوط به چارچوب‌های نرم‌افزاری یادگیری فدرال

۴ مطالعه مقایسه‌ای بین سناریوهای فدرال و غیر فدرال

در این بخش مقایسه‌ای بین آموزش مدل فدرال و مدل‌های محلی ایزوله در شرایطی که داده‌ها بین چندین مشتری توزیع شده‌اند، انجام می‌شود. مدل فدرال مدل مشترکی است که بین تمامی مشتریان آموزش داده می‌شود بدون اینکه داده‌ها به اشتراک گذاشته شوند. سه سناریو مقایسه می‌شوند:

- مدل متمرکز: استفاده از داده‌های تمام مشتریان برای آموزش یک مدل.
- مدل‌های محلی: هر مشتری مدل خود را با داده‌های محلی خود آموزش می‌دهد.
- مدل فدرال: یک مدل مشترک که بدون افشای داده‌ها بین مشتریان آموزش داده می‌شود.

نتایج نشان می‌دهند که مدل فدرال در اکثر مواقع عملکرد بهتری نسبت به مدل‌های محلی دارد، به‌ویژه در مواردی که داده‌ها IID نیستند.

۱.۴ الف) سناریوی IID

در این سناریو داده‌ها IID هستند و نتایج نشان می‌دهند که مدل متمرکز بهترین عملکرد را دارد. مدل فدرال بهتر از مدل‌های محلی است، اما زمان اجرای بیشتری نیاز دارد.

مقایسه مدل فدرال با مدل‌های پایه با داده‌های IID

مدل	از دست دادن آموزش	دقت آموزش	زمان اجرا (ثانیه)
مدل متمرکز	0.026	0.992	140.7
مدل‌های محلی (IID)	0.064	0.983	16.1
مدل فدرال (IID)	0.043	0.989	749.5

۲.۴ ب) سناریوی غیر IID

در این سناریو داده‌ها غیر IID هستند. مدل فدرال در این شرایط عملکرد بهتری نسبت به مدل‌های محلی دارد، به‌ویژه زمانی که تعداد مشتریان بیشتر می‌شود.

مقایسه مدل فدرال با مدل‌های محلی با داده‌های غیر IID

مدل	از دست دادن آموزش	دقت آموزش	زمان اجرا (ثانیه)
مدل‌های محلی (غیر IID) - 10 مشتری 10 دوره	2.173	0.311	2.4
مدل فدرال (غیر IID) - 10 مشتری 10 دوره	0.658	0.851	27.9
مدل‌های محلی (غیر IID) - 20 مشتری 20 دوره	4.119	0.869	4.6
مدل فدرال (غیر IID) - 20 مشتری 20 دوره	0.257	0.928	75.9

۳.۴ ج) نتایج نهایی

نتایج نشان می‌دهند که مدل فدرال در مقایسه با مدل‌های محلی عملکرد بهتری دارد و به‌ویژه در شرایط داده‌های غیر IID مفید است. همچنین، مدل فدرال زمان بیشتری برای آموزش نیاز دارد.

۵ بررسی روندهای کلیدی در Federated Learning

Federated Learning (FL) رویکردی نوین در یادگیری ماشین است که کارایی، امنیت و حفظ حریم خصوصی را بهبود می‌بخشد. این بخش روندهای کلیدی در این حوزه را بررسی می‌کند و آنها را به دو دسته‌ی اصلی تقسیم می‌کند:

۱. چالش‌های مشترک با یادگیری ماشین

۲. چالش‌های منحصربه‌فرد FL

روندهای مهم شامل **حملات و دفاع‌ها، شخصی‌سازی، یادگیری انتقالی، وظایف جدید یادگیری ماشین و کاربردهای FL در NLP و تحلیل احساسات** هستند.

۱.۵ حملات و دفاع‌ها در Federated Learning:

مشابه دیگر روش‌های یادگیری ماشین، FL نیز در معرض **حملات خصمانه** قرار دارد. با این حال، ماهیت غیرمتمرکز آن این حملات را متمایز می‌کند. دو دسته‌ی اصلی حملات عبارتند از:

۱. **حملات مدل** : دستکاری مدل جهانی برای تغییر رفتار آن.

۲. **حملات حریم خصوصی** : تلاش برای استخراج اطلاعات از داده‌های کاربران، شامل:

- حملات **استنتاج ویژگی** (Feature Inference Attacks) : بازسازی ویژگی‌های اصلی داده‌ها.
- حملات **بازسازی داده‌ها** (Feature Reconstruction Attacks) : بازسازی داده‌های اولیه از به‌روزرسانی‌های اشتراک‌گذاری شده.
- حملات **استنتاج عضویت** (Membership Inference Attacks) : تشخیص این که آیا نمونه‌ای در مجموعه داده‌ی آموزشی بوده است.

مکانیزم‌های دفاعی: FL از مکانیزم‌های مختلفی برای مقابله با این تهدیدات استفاده می‌کند که در سه گروه زیر طبقه‌بندی می‌شوند:

۱. **دفاع‌های سمت سرور** : استفاده از روش‌های تجمیع مقاوم، تشخیص ناهنجاری و Differential Privacy (DP).

۲. **دفاع‌های سمت کاربر** : پیاده‌سازی DP در سطح کاربر.

۳. **دفاع‌های کانال ارتباطی** : استفاده از رمزنگاری چندطرفه‌ی امن (SMC) در FL.

۲.۵ یادگیری فدرال شخصی‌سازی‌شده (Personalized Federated Learning):

چالش اصلی FL، **عدم توازن داده‌ها** و **عدم شخصی‌سازی مدل‌ها** برای کاربران مختلف است. **انحراف مشتری (Client Drift)** زمانی رخ می‌دهد که مدل جهانی برای برخی از کاربران به درستی عمل نمی‌کند.

رویکردهای شخصی‌سازی:

۱. **شخصی‌سازی مدل جهانی**:

- رویکردهای مبتنی بر داده: کاهش ناهمگونی آماری برای کاهش انحراف مشتری.
- رویکردهای مبتنی بر مدل: منظم‌سازی مدل جهانی جهت بهبود تطبیق محلی.

۲. **آموزش مدل‌های شخصی‌سازی‌شده**:

- روش‌های مبتنی بر معماری: ترکیب لایه‌های مشترک و اختصاصی برای هر کاربر.
- روش‌های مبتنی بر شباهت: استفاده از یادگیری چندوظیفه‌ای برای کشف ارتباط بین مشتریان.

۳.۵ یادگیری انتقالی فدرال (Federated Transfer Learning):

زمانی که مجموعه داده‌های مشتریان دارای ویژگی‌های کاملاً همپوشان نیستند، FL عملکرد ضعیفی دارد. Federated Transfer Learning (FTL) یادگیری انتقالی را در FL ادغام می‌کند.

کاربردهای FTL:

۱. **تحلیل نهان‌نگاری تصاویر** (FedSteg) : شناسایی اطلاعات پنهان در تصاویر.

۲. **NLP در سامانه‌های ثبت سرطان** : آموزش مدل‌ها بدون اشتراک‌گذاری واژگان.

۳. **تقطیر دانش برای دستگاه‌های لبه‌ای** : بهینه‌سازی مدل‌های Edge AI.

۴.۵ پردازش زبان طبیعی (NLP) و تحلیل احساسات (Sentiment Analysis) در FL:

چالش‌های FL در NLP و تحلیل احساسات:

۱. **ناهمگونی داده‌ها** : مدل باید با منابع متنوع سازگار شود.

- **عدم تعادل داده‌ها** : حجم داده‌های آموزش بین مشتریان یکسان نیست.

راهکارها:

- **یادگیری انتقالی** : پیش‌آموزش مدل روی داده‌های متمرکز و تنظیم نهایی در سطح محلی.
- **روش‌های حفظ حریم خصوصی** : استفاده از DP برای محافظت از داده‌های کاربران.
- **یادگیری نمایش متضاد** (Contrastive Representation Learning) : بهره‌گیری از داده‌های مشارکتی با حفظ حریم خصوصی.

۶ نتیجه‌گیری:

FL مسیر آینده‌ی یادگیری ماشین را شکل می‌دهد و امکان **یادگیری غیرمتمرکز و حفظ حریم خصوصی** را فراهم می‌کند. روندهای کلیدی تحقیق در این حوزه بر **امنیت، شخصی‌سازی، یادگیری انتقالی، تشخیص ناهنجاری و پردازش زبان طبیعی** متمرکز است. با وجود چالش‌های موجود، راهکارهای نوآورانه به توسعه‌ی بیشتر FL کمک می‌کنند.