

Federated Learning con Privacy Differenziale: proteggere i dati nell'era dell'AI Collaborativa



Nel panorama attuale dell'intelligenza artificiale, il rapido sviluppo degli algoritmi di machine learning si scontra con una crescente preoccupazione per la privacy dei dati. I modelli di AI più avanzati richiedono enormi quantità di informazioni per essere addestrati efficacemente, ma questi dati sono spesso sensibili e difficili da condividere a causa di normative sempre più stringenti come il GDPR o semplicemente per le legittime preoccupazioni degli utenti riguardo la privacy. In questo contesto complesso, due tecnologie emergono come potenziali soluzioni complementari: il Federated Learning (FL) e la Privacy Differenziale (DP).

Il Federated Learning rappresenta un paradigma di addestramento innovativo che consente a molteplici dispositivi o entità di collaborare nell'addestramento di un modello senza condividere direttamente i dati grezzi. Invece di centralizzare tutti i dati in un unico server, FL permette l'addestramento distribuito dove i dispositivi elaborano localmente i propri dati e condividono solo gli aggiornamenti del modello. La Privacy Differenziale, d'altra parte, fornisce un quadro matematico formale per limitare la fuga di informazioni derivate dai dati privati, garantendo che l'output di un algoritmo non riveli troppo sui dati di input individuali.

Quando queste due tecnologie si incontrano, creano un approccio potente per l'apprendimento collaborativo preservando la privacy. Tuttavia, implementare efficacemente

questa combinazione pone numerose sfide tecniche che richiedono una comprensione approfondita di entrambi i campi. Il presente articolo esplora l'intersezione di queste tecnologie, analizzando le sfide, le soluzioni e le applicazioni emergenti nell'ambito della sicurezza informatica e della protezione dei dati.

La promessa del Federated Learning: collaborazione senza compromettere la Privacy

Il Federated Learning rappresenta un cambiamento paradigmatico nel modo in cui concettualizziamo l'addestramento dei modelli di machine learning. Introdotto da Google nel 2016, FL consente ai dispositivi di apprendere collettivamente un modello condiviso mantenendo i dati di addestramento sui dispositivi locali. Il processo tipicamente si articola in diverse fasi iterate:

Fase 1: Distribuzione del modello iniziale. Un modello iniziale viene distribuito a tutti i dispositivi partecipanti, che rappresentano i client nel sistema federato.

Fase 2: Addestramento locale. Ogni dispositivo addestra il modello sui propri dati locali, utilizzando algoritmi standard come la discesa stocastica del gradiente (SGD).

Fase 3: Condivisione degli aggiornamenti. Solo gli aggiornamenti del modello, che possono essere gradienti o parametri del modello aggiornati, vengono inviati a un server centrale. Questo server non ha mai accesso ai dati grezzi, ma solo agli aggiornamenti che riflettono ciò che il modello ha appreso.

Fase 4: Aggregazione. Il server aggrega questi aggiornamenti, tipicamente attraverso una media pesata, per migliorare il modello globale.

Fase 5: Ridistribuzione. Il modello globale aggiornato viene ridistribuito ai dispositivi, e il processo continua iterativamente.

Questo approccio offre vantaggi significativi per la privacy, poiché i dati sensibili rimangono sul dispositivo dell'utente. È particolarmente utile in scenari come la previsione delle parole nelle tastiere mobili, l'analisi delle immagini personali o l'elaborazione di dati sanitari dove la sensibilità dei dati è elevata. Inoltre, il FL risolve anche problemi pratici come i requisiti di larghezza di banda e le limitazioni di archiviazione centralizzata, poiché solo gli aggiornamenti del modello, non i dati grezzi, vengono trasmessi.

Tuttavia, nonostante i miglioramenti intrinseci alla privacy, il Federated Learning da solo non fornisce garanzie formali contro attacchi sofisticati. Ricerche condotte da Zhu et al. hanno dimostrato che i gradienti condivisi possono ancora rivelare informazioni sui dati di addestramento. Ad esempio, un'entità malintenzionata potrebbe essere in grado di ricostruire dati di input esaminando attentamente gli aggiornamenti del modello attraverso tecniche come gli attacchi di inversione del gradiente. Anche con l'aggregazione delle informazioni di più dispositivi, non esiste una garanzia teorica che le informazioni sensibili non possano essere estratte.

Altre minacce alla privacy nel contesto del FL includono attacchi di inferenza di appartenenza, che tentano di determinare se un particolare record è stato utilizzato nell'addestramento del modello, e attacchi di inferenza di proprietà, che mirano a dedurre caratteristiche statistiche dei dati di addestramento. Questi rischi evidenziano la necessità di integrare FL con tecniche più robuste di preservazione della privacy come la Privacy Differenziale.

Privacy Differenziale: una garanzia matematica per la Protezione dei Dati

La Privacy Differenziale fornisce un framework matematico rigoroso per proteggere le informazioni individuali in un dataset. Introdotta da Cynthia Dwork nel 2006, la DP offre una definizione formale di privacy che può essere dimostrata matematicamente, a differenza di approcci ad hoc che potrebbero contenere vulnerabilità nascoste.

Il concetto fondamentale è che un algoritmo differenzialmente privato dovrebbe produrre risultati statisticamente simili indipendentemente dal fatto che un singolo record sia incluso o meno nel dataset. Questa proprietà garantisce che un osservatore esterno non possa dedurre con certezza se un particolare individuo ha contribuito ai dati, anche avendo accesso all'output dell'algoritmo e a informazioni ausiliarie.

Formalmente, un meccanismo M soddisfa la (ϵ, δ) -privacy differenziale se, per qualsiasi coppia di dataset D e D' che differiscono per un singolo elemento, e per qualsiasi sottoinsieme di output S :

$$Pr[M(D) \in S] \leq e^{\epsilon} \cdot Pr[M(D') \in S] + \delta$$

Dove ϵ rappresenta il "budget di privacy" (valori più piccoli significano maggiore privacy) e δ è una probabilità di fallimento molto piccola, tipicamente scelta in modo da essere inferiore a $1/n$, dove n è la dimensione del dataset.

Per raggiungere la privacy differenziale, i meccanismi più comuni aggiungono rumore calibrato alla sensibilità dei dati. La sensibilità misura quanto l'output di una funzione può cambiare quando un singolo record nel dataset cambia. I meccanismi comuni includono:

- Il **meccanismo di Laplace**, che aggiunge rumore estratto da una distribuzione di Laplace con scala proporzionale alla sensibilità L1 della funzione divisa per ϵ .
- Il **meccanismo gaussiano**, che aggiunge rumore estratto da una distribuzione normale con varianza proporzionale al quadrato della sensibilità L2 della funzione e inversamente proporzionale al quadrato del parametro di privacy ϵ .

Nel contesto dell'apprendimento automatico, l'approccio più diffuso è DP-SGD (Differentially Private Stochastic Gradient Descent), che aggiunge rumore gaussiano ai gradienti clippati durante l'addestramento. Questo consente di addestrare modelli complessi come le reti neurali profonde con garanzie di privacy differenziale.

La DP offre diverse proprietà importanti che la rendono particolarmente adatta per l'integrazione con il Federated Learning:

- **Proprietà di post-elaborazione:** qualsiasi elaborazione aggiuntiva su un output differenzialmente privato rimane differenzialmente privata, senza degradare la garanzia di privacy. Questo significa che le trasformazioni dei modelli dopo l'aggregazione non compromettono la privacy.
- **Composizione:** la combinazione di più meccanismi differenzialmente privati dà ancora un risultato differenzialmente privato, anche se con un parametro di privacy degradato. Questa proprietà è cruciale per analizzare la perdita di privacy cumulativa durante le iterazioni di addestramento.
- **Amplificazione tramite sottocampionamento:** selezionare casualmente un sottoinsieme di dati prima di applicare un meccanismo di privacy differenziale migliora la garanzia di privacy, permettendo di ottenere la stessa utilità con meno rumore.

Queste proprietà forniscono un framework rigoroso per analizzare e garantire la privacy in sistemi complessi come quelli di Federated Learning, permettendo una quantificazione precisa del compromesso tra privacy e utilità.

Matrimonio di tecnologie: Federated Learning con Privacy Differenziale

L'integrazione del Federated Learning con la Privacy Differenziale combina il meglio di entrambi i mondi: la natura distribuita e rispettosa della privacy di FL con le garanzie matematiche formali della DP. Questa combinazione può essere implementata in diversi modi, a seconda del modello di fiducia e delle specifiche esigenze dell'applicazione.

Paradigmi di Implementazione

Dalla letteratura emergono diversi approcci per implementare FL con DP, ognuno con i propri compromessi tra fiducia, privacy e utilità del modello:

FL con DP centralizzata (CDP): Questo approccio assume un server centrale fidato che aggiunge rumore calibrato agli aggiornamenti aggregati dei client. Gli algoritmi come DP-FedAvg e DP-FedSGD rientrano in questa categoria. Il server centrale deve essere affidabile poiché ha accesso agli aggiornamenti non rumorosi dei modelli dei client. Sebbene questa configurazione richieda meno rumore rispetto ad altre, impone un'ipotesi forte sulla fiducia nel server.

FL con DP locale (LDP): In questo paradigma, ogni client aggiunge rumore ai propri aggiornamenti del modello prima di inviarli al server. Algoritmi come LDP-FedSGD implementano questa strategia. Il vantaggio principale è che non richiede un server fidato, poiché i dati sono già protetti prima di lasciare il dispositivo. Tuttavia, questo approccio generalmente richiede più rumore per ottenere la stessa

garanzia di privacy, con conseguente riduzione dell'utilità del modello.

FL con DP distribuita (DDP): Questo approccio innovativo cerca di colmare il divario di utilità-fiducia tra LDP e CDP eliminando l'assunzione di un aggregatore fidato tramite tecniche crittografiche. Esistono due principali paradigmi DDP:

- Basato su shuffling: utilizza canali di comunicazione anonimi per attenuare i rischi di identificazione dei messaggi, amplificando così le garanzie di privacy;
- Basato su aggregazione sicura: sostituisce l'aggregatore fidato con protocolli di calcolo sicuro multiparty (MPC), consentendo l'aggregazione senza rivelare i singoli contributi.

f-DP federata: Un approccio più recente introdotto da Zheng et al. che opera a livello di record, proteggendo i singoli record dei dati di un client contro gli avversari. Questa nozione di privacy opera al livello più granulare, proteggendo singoli elementi anziché interi set di dati dei client. È particolarmente utile quando la partecipazione del client non è informazione sensibile, ma i dati individuali lo sono, come nel caso di ospedali che collaborano per addestrare modelli predittivi per malattie.

Il framework PriFedSync rappresenta un esempio di un approccio generico per FL con DP che può adattarsi a una vasta famiglia di algoritmi FL all'avanguardia, incorporando meccanismi di privacy differenziale e supportando modelli sia personalizzati che globali.

Sfide tecniche e compromessi

L'implementazione di FL con DP comporta diverse sfide tecniche significative che devono essere affrontate per ottenere un sistema pratico ed efficace:

Calibrazione della soglia di clipping: Per limitare la sensibilità dei gradienti, è comune applicare una tecnica di “clipping” che limita la norma dei gradienti a un valore massimo. Determinare la soglia ottimale è cruciale: una soglia di clipping sottostimata può causare bias nel gradiente e persino divergenza del modello, mentre una soglia sovrastimata comporta l’aggiunta di rumore eccessivo. Tecniche di clipping adattivo basate sull’analisi della divergenza o sulla stima euristica possono ridurre il rumore e produrre modelli con maggiore utilità.

Ottimizzazione della distribuzione del rumore: La forma della distribuzione del rumore utilizzata per garantire la privacy differenziale può influenzare significativamente l’equilibrio tra privacy e utilità. Oltre alle comuni distribuzioni di Laplace e Gaussiana, distribuzioni discrete o a gradini attraverso tecniche di segmentazione possono essere utilizzate per ridurre la scala del rumore necessario mantenendo i requisiti di DP.

Composizione della perdita di privacy: Il monitoraggio preciso della perdita di privacy accumulata durante le iterazioni di addestramento è fondamentale. Approcci avanzati come il “moment accountant” analizzano la distribuzione dettagliata della variabile di perdita di privacy composta e derivano un limite molto più stretto utilizzando momenti di ordine superiore, consentendo di addestrare modelli con una perdita di privacy accettabile.

Compressione dei parametri del modello: Un vettore di parametri lungo consuma pesantemente il budget di privacy e appesantisce i canali di comunicazione limitati. Tecniche di compressione come il filtraggio dei parametri, l’approssimazione di rango basso, la proiezione casuale e la quantizzazione del gradiente possono ridurre entrambi i problemi. Queste tecniche possono ridurre empiricamente sia il consumo di larghezza di banda di comunicazione che la varianza del rumore, sebbene possano anche portare a una perdita di

utilità poiché alcune informazioni sui parametri vengono eliminate.

Campionamento dei client partecipanti: Il campionamento dei client nell'addestramento FL basato su DP è un approccio promettente per risparmiare budget di privacy, overhead di comunicazione e consumo energetico. L'effetto di amplificazione del campionamento per DP, in cui l'inclusione casuale dei client in ogni round di addestramento rafforza le garanzie di privacy, permette di ottenere una protezione più forte della privacy minimizzando il consumo medio di comunicazione, calcolo e privacy.

Applicazioni pratiche e implementazioni

Le applicazioni di FL con DP stanno emergendo in diversi settori dove la privacy dei dati è cruciale ma esiste anche la necessità di modelli di apprendimento avanzati. Diverse piattaforme software e implementazioni pratiche stanno rendendo queste tecnologie accessibili agli sviluppatori.

Sanità e dati medici

Nel settore sanitario, l'accesso ai dati dei pazienti è fortemente regolamentato da normative come HIPAA negli Stati Uniti o GDPR in Europa, ma questi dati sono essenziali per sviluppare modelli diagnostici e terapeutici avanzati. FL con DP può consentire a ospedali e istituti di ricerca di collaborare nell'addestramento di modelli predittivi per condizioni come il COVID-19, proteggendo al contempo la privacy di ciascun paziente.

Un esempio significativo è la collaborazione tra più ospedali per addestrare modelli di diagnosi precoce o predizione dell'evoluzione della malattia. Piuttosto che preoccuparsi se un ospedale partecipa alla collaborazione (che raramente è

un'informazione sensibile), la vera preoccupazione è proteggere i dati individuali dei pazienti. In questo contesto, la f-DP federata che opera a livello di record è particolarmente adatta.

I ricercatori della University of Pennsylvania hanno dimostrato l'efficacia di questo approccio, ottenendo modelli con un'accuratezza comparabile ai metodi centralizzati tradizionali, pur mantenendo forti garanzie di privacy per i singoli pazienti.

Riconoscimento immagini su dispositivi mobili

Gli esperimenti condotti su dataset come MNIST (riconoscimento di cifre scritte a mano) e CIFAR-10 (classificazione di oggetti) mostrano che è possibile addestrare modelli di visione artificiale con FL e DP mantenendo un'accuratezza ragionevole. Questi esperimenti rivelano importanti compromessi tra privacy, accuratezza e costi computazionali.

Su MNIST, modelli privati con diversi livelli di rumore ($\sigma = 0.75, 0.9, 1.0$) possono raggiungere un'accuratezza del 90% dopo un numero variabile di round di sincronizzazione, con una perdita di accuratezza relativamente contenuta rispetto ai modelli non privati. Su CIFAR-10, che è un dataset più complesso, i modelli privati possono raggiungere un'accuratezza del 52% rispetto al 64.7% dei modelli non privati.

Queste tecnologie sono particolarmente rilevanti per applicazioni come il riconoscimento di oggetti o la classificazione di immagini sui dispositivi mobili, dove i dati delle immagini personali devono rimanere privati per evitare violazioni della privacy visiva.

Modelli linguistici e previsione testo

Google ha implementato FL con DP per addestrare modelli di previsione delle parole per la tastiera Gboard. In un recente

studio pubblicato da Xu et al., hanno dimostrato che tutti i modelli di predizione delle parole successive in Gboard ora hanno garanzie DP, e tutti i futuri lanci di modelli linguistici neurali Gboard richiederanno garanzie DP.

Questo permette ai modelli di migliorare in base all'uso reale senza esporre il comportamento di digitazione individuale degli utenti, che potrebbe contenere informazioni sensibili come password, informazioni personali o conversazioni private.

Con l'avvento dei grandi modelli linguistici (LLM) come ChatGPT, l'applicazione di FL con DP per il fine-tuning su domini specifici rappresenta un'area di ricerca promettente. Questi modelli potrebbero beneficiare dell'apprendimento da dati di utenti reali senza compromettere la privacy individuale.

Strumenti e framework per implementare FL con DP

Per facilitare l'implementazione pratica di queste tecnologie, sono stati sviluppati numerosi framework e piattaforme software. Alcuni dei più rilevanti includono:

TensorFlow Privacy e TensorFlow Federated: Librerie di Google che si integrano perfettamente con i modelli TensorFlow esistenti e consentono l'addestramento di modelli personalizzati con DP. Tuttavia, i meccanismi DP integrati sono relativamente fissi nel design e non supportano ottimizzazioni personalizzate flessibili.

Opacus: Una libreria scalabile ed efficiente per l'addestramento di modelli PyTorch con DP. Introduce un'astrazione di un "*privacy engine*" che si collega all'ottimizzatore PyTorch standard, rendendo molto più semplice l'implementazione di DP-SGD senza chiamare esplicitamente API di basso livello.

PySyft: Una libreria Python che supporta FL e DP, e disaccoppia l'addestramento del modello dai dati privati. La versione attuale si concentra principalmente sul calcolo

multi-party sicuro (SMC) e sulla crittografia omomorfa (HE) piuttosto che sull'implementazione DP.

FedML: Una libreria di ricerca aperta e benchmark standardizzato con diversi paradigmi e configurazioni FL. La versione attuale integra solo DP debole ma fornisce API di basso livello per primitive di sicurezza.

Sherpa.ai FL: Un framework unificato per FL con DP, che presenta un supporto completo per meccanismi DP e tecniche di ottimizzazione. Tuttavia, si concentra principalmente sull'ottimizzazione a livello di algoritmo e non considera l'implementazione del sistema pratico.

Questi strumenti stanno rendendo più accessibile l'implementazione di FL con DP, anche se c'è ancora spazio per framework più completi che supportino tutte le varianti di questi approcci con ottimizzazioni flessibili.

Sfide emergenti e direzioni future

Nonostante i significativi progressi nell'integrazione di FL con DP, rimangono diverse sfide aperte che richiedono ulteriori ricerche:

Federated Learning verticale e di trasferimento

Mentre il FL orizzontale (dove i client hanno dati con le stesse caratteristiche ma esempi diversi) è stato ampiamente studiato, il FL verticale (dove diverse parti detengono caratteristiche diverse degli stessi campioni) pone sfide uniche per l'integrazione della DP.

Il FL verticale ha guadagnato crescente attenzione, ma molti studi esistenti si basano sul calcolo multi-party sicuro (SMC) per proteggere la riservatezza senza considerare la perdita di privacy nei risultati finali. Per ottenere una resistenza dimostrabile agli attacchi di inferenza di appartenenza o ricostruzione, è essenziale impiegare la DP anche nel VFL.

Questa integrazione è più impegnativa per due motivi principali: in primo luogo, il design degli algoritmi VFL varia per diverse attività e modelli, spesso richiedendo uno sviluppo caso per caso; in secondo luogo, le correlazioni tra attributi distribuiti sono più difficili da identificare senza diffondere informazioni individuali ad altre parti.

Grandi Modelli Linguistici (LLM)

Con l'emergere di modelli linguistici di grandi dimensioni come ChatGPT, sia FL che DP mostrano un futuro promettente nel fine-tuning di LLM preservando la privacy rispetto ai dati di dominio privato. Tuttavia, questi modelli possono avere da diversi miliardi a centinaia di miliardi di parametri, ponendo sfide significative.

Quando si applicano DP e FL a LLM, ci saranno molteplici sfide riguardanti l'enorme numero di parametri, al di là degli oneri aggiuntivi di comunicazione e calcolo sui partecipanti con risorse limitate. Indipendentemente dal modello DP, la quantità totale di rumore per la privacy deve essere proporzionale al numero di parametri per applicare DP sui modelli, il che porterebbe a enormi perdite di utilità senza tecniche specializzate.

Inoltre, il fine-tuning di LLM pre-addestrati è diverso dall'addestramento convenzionale dei modelli. La garanzia di privacy teorica nell'ML (ad esempio, DP-SGD) spesso presuppone che i modelli siano appresi da zero con molte iterazioni di addestramento, invece di una modalità di fine-tuning con molte meno iterazioni.

Federated Learning su stream di dati

In molti scenari realistici, i dati di addestramento vengono generati continuamente sotto forma di stream sui client distribuiti. In tali casi, i sistemi FL devono condurre analisi ripetitive su stream distribuiti. Ereditando l'apprendimento automatico online (OL), il federated learning

online può essere derivato naturalmente per evitare di riaddestramento i modelli da zero ogni volta che arriva un nuovo frammento di dati.

Tuttavia, ottenere DP per questo scenario porta molteplici sfide. La prima è come definire la privacy nell'impostazione OFL, poiché la nozione generale di DP funziona solo per dataset statici. Sebbene le nozioni di privacy esistenti per i flussi di dati e FL sembrano applicabili qui, devono ancora essere chiarite e formulate rigorosamente nell'impostazione OFL.

La seconda sfida riguarda l'efficienza algoritmica. Prendendo come esempio la LDP a livello di evento (cioè, garantire ϵ -LDP in ogni istanza temporale), il frequente caricamento degli aggiornamenti del modello locale accumula enormi costi di comunicazione e grande perdita di utilità, poiché il rumore è proporzionale alla dimensione dei dati di comunicazione.

Robustezza, equità e diritto all'oblio

Un sistema FL robusto dovrebbe essere resiliente a vari guasti e attacchi causati da partecipanti che si comportano male. A causa delle capacità limitate (ad esempio, limiti della batteria), i client FL (ad esempio, smartphone) potrebbero abbandonare l'addestramento FL in modo imprevisto in qualsiasi momento. I dropout casuali dei client presentano gravi sfide per la progettazione pratica di FL con privacy differenziale.

La protezione della privacy è solo il primo passo per incoraggiare la condivisione dei dati tra una grande popolazione. L'applicazione dell'equità (fairness) aiuta a mitigare il bias involontario su individui con dati eterogenei. Tuttavia, il dilemma è che la DP mira a oscurare attributi identificabili mentre l'equità richiede la conoscenza dei valori degli attributi sensibili degli individui per evitare risultati distorti. Il clipping del gradiente e l'aggiunta di rumore nella DP possono peggiorare

l'iniquità diminuendo l'accuratezza del modello per classi e sottogruppi sottorappresentati.

Inoltre, i diritti alla privacy includono il “diritto all'oblio”, cioè gli utenti possono scegliere di non contribuire con dati privati senza lasciare traccia. Poiché i modelli ML memorizzano molte informazioni specifiche sui campioni di addestramento, il concetto di “unlearning” della macchina è proposto per eliminare la sua influenza sui modelli addestrati. Tuttavia, l'unlearning federato affronta sfide distinte, poiché è molto più difficile cancellare l'influenza dei dati di un client quando il modello globale ha iterativamente trasportato le informazioni di tutti i client partecipanti.

Un Futuro di apprendimento collaborativo e privato

L'integrazione del Federated Learning con la Privacy Differenziale rappresenta una frontiera promettente per l'apprendimento automatico rispettoso della privacy. Questa combinazione permette di sbloccare il potenziale dell'IA superando il problema della frammentazione dei dati su larga scala, consentendo al contempo garanzie di privacy rigorose che possono rispettare sia la consapevolezza della privacy che la conformità normativa.

Abbiamo esplorato i diversi paradigmi per implementare FL con DP, dai modelli centralizzati che richiedono fiducia nel server, agli approcci locali che proteggono i dati prima che lascino il dispositivo, fino ai sistemi distribuiti più avanzati che utilizzano tecniche crittografiche per ottenere alta accuratezza senza un aggregatore fidato. Abbiamo anche discusso le sfide tecniche fondamentali nell'ottimizzazione dell'utilità di questi sistemi, incluse la calibrazione della soglia di clipping, l'ottimizzazione della distribuzione del rumore e la composizione della perdita di privacy.

Le applicazioni pratiche in sanità, visione artificiale e modelli linguistici dimostrano il potenziale di queste tecnologie, mentre gli strumenti e i framework emergenti stanno rendendo più accessibile la loro implementazione. Le sfide future nella gestione di dati verticali, grandi modelli linguistici, stream di dati e bilanciamento tra privacy, robustezza ed equità continueranno a guidare l'innovazione in questo campo.

Con il continuo avanzamento della tecnologia, possiamo aspettarci soluzioni sempre più sofisticate che consentano ai sistemi di apprendimento automatico di operare su dati sensibili distribuiti senza compromettere la privacy individuale. Come dimostrano le implementazioni iniziali in vari campi, dalle tastiere mobili all'assistenza sanitaria, questa combinazione di tecnologie ha il potenziale per trasformare radicalmente il modo in cui utilizziamo i dati per l'addestramento dei modelli di AI, realizzando finalmente la promessa di sistemi di intelligenza artificiale che rispettano pienamente la privacy dei dati personali.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/federated-learning-privacy-differenziale/>