مطالعهٔ مروری نظام‌مند بر مبانی، کاربردها و چالش‌های یادگیری مشارکتی

هاله فاتح[۱]، محسن رضوانی[۲]*، اسماعیل طحانیان[۳]

دانشجوی دکتری دانشکدهٔ مهندسی کامپیوتر، دانشگاه صنعتی شاهرود، شاهرود، ایران[۱]

دانشیار دانشکدهٔ مهندسی کامپیوتر، دانشگاه صنعتی شاهرود، شاهرود، ایران[۲]

استادیار دانشکدهٔ مهندسی کامپیوتر، دانشگاه صنعتی شاهرود، شاهرود، ایران[۳]

چکیده

یادگیری مشارکتی یک طرح یادگیری ماشین در حال رشد است که هدف آن حل مشکل جزیره‌ای‌شدن داده‌ها با حفظ حریم خصوصی آن‌هاست؛ در این روش، چندین مشتری مانند دستگاه‌های تلفن همراه، مؤسسات، سازمان‌ها با یک یا چند سرور مرکزی برای آموزش مدل‌های یادگیری ماشین به‌صورت غیرمتمرکز همکاری می‌کنند. برای نخستین‌بار گوگل در سال ۲۰۱۶ یادگیری مشارکتی را برای پیش‌بینی ورودی متن کاربر در ده‌ها هزار دستگاه اندرویدی و حفظ حریم خصوصی داده‌ها در دستگاه‌ها معرفی کرد که در واقع یک فناوری یادگیری ماشین توزیع‌شدهٔ رمزگذاری‌شده است که به شرکت‌کنندگان اجازه می‌دهد مدل آموزشی مشترکی را بسازند؛ درحالی‌که داده‌های اصلی را به‌صورت محلی حفظ می‌کنند. در سال‌های اخیر، مفهوم اصلی یادگیری مشارکتی به طیف وسیع‌تری از روش‌های یادگیری ماشین غیرمتمرکز و حفظ حریم خصوصی گسترش یافته‌است. در این مقاله، مروری نظام‌مند بر مقالات مروری، مقالات منتخب و کتب منتشرشده در زمینهٔ یادگیری مشارکتی ارائه می‌دهیم. در ابتدا یک نمای کلی از یادگیری مشارکتی ترسیم می‌کنیم که شامل معرفی و تشریح فرایند آن است؛ سپس به معرفی الگوریتم‌های موجود و سیر تکامل آن‌ها می‌پردازیم؛ همچنین، طبقه‌بندی و کاربرد انواع ساختارهای یادگیری مشارکتی در سه گروه یادگیری مشارکتی افقی، یادگیری مشارکتی عمودی و یادگیری انتقال مشارکتی را مورد بررسی قرار می‌دهیم. در ادامه، با استناد به منابع منتخب این مقاله، به بررسی کاربردهای یادگیری مشارکتی در اینترنت اشیا، شهر هوشمند، امنیت، حفظ حریم خصوصی مدل و داده‌ها، انفورماتیک سلامت و مراقبت‌های بهداشتی می‌پردازیم؛ سپس روش‌های مختلف در هر یک از این زمینه‌ها مقایسه و مزایا، محدودیت‌ها و چالش‌های پیش‌روی هر کدام را مورد بحث قرار می‌دهیم. علاوه‌براین، به بررسی کاربردها و تفاوت‌های یادگیری ماشین مشارکتی، یادگیری عمیق مشارکتی و بلاک‌چین مشارکتی در اینترنت صنعتی اشیا می‌پردازیم وکاربردهای این فناوری‌ها در حوزه‌های ذخیره‌سازی، مدیریت‌داده‌ها و مدیریت منابع را نیز بررسی می‌کنیم. در پایان، به بررسی چالش‌ها، چشم‌اندازها و زمینه‌های پژوهشی آینده حوزهٔ یادگیری مشارکتی می‌پردازیم.

واژگان کلیدی: یادگیری مشارکتی، یادگیری ماشین غیرمتمرکز، حفظ حریم خصوصی، هوش مصنوعی توزیع‌شده، اینترنت اشیا.

A systematic review of the foundations, applications, and challenges of federated learning.

Haleh Fateh[1], Mohsen Rezvani[2]*, Esmaeel Tahanian[3]

Phd Student of Faculty of Computer Engineering Shahrood University of Technology[1]

associate professor of Faculty of Computer Engineering Shahrood University of Technology[2]

Assistant Professor of Faculty of Computer Engineering Shahrood University of Technology[3]

Abstract

Federated Learning (FL) is an innovative machine learning paradigm that tackles the challenge of data island while safeguarding data privacy. It enables decentralized model training by allowing multiple clients—such as mobile devices, institutions, or organizations—to collaboratively build models without transferring local data to a central server. This paradigm gained significant attention following

* نویسندهٔ عهده‌دار مکاتبات

* Corresponding author

• تاریخ ارسال مقاله: ۱۴۰۲/۵/۱ • تاریخ پذیرش: ۱۴۰۳/۵/۳۱ • تاریخ انتشار: ۱۴۰۳/۱۰/۲۹ • نوع مطالعه: ترویجی

[DOI: 10.61186/jsdp.21.3.23]

Google's 2016 initiative to predict user text input on Android devices while maintaining the privacy of locally stored data.
A core feature of FL is its distributed and encrypted framework, enabling participants to contribute to a collective learning process without revealing their original data to a central entity or other participants. In recent years, FL has evolved to encompass a broader spectrum of decentralized machine learning techniques, while still maintaining privacy as a central tenet. This evolution has positioned FL as a critical technology in sectors where data privacy, security, and sovereignty are paramount.
This paper presents a systematic review of the literature on federated learning, synthesizing insights from review articles, Books, key documents, and published research. The review is structured as follows:
Overview of Federated Learning: This section introduces the foundational concepts of FL, detailing its origins, core principles, and operational processes. The decentralized structure and privacy-preserving techniques employed in FL are examined, along with real-world applications as examples.
Algorithms and Evolution: This section explores the state-of-the-art algorithms driving FL and traces their development over time. Key innovations in aggregation techniques, optimization methods, and client-server communication protocols are highlighted, demonstrating how they have enhanced FL's scalability and efficiency.
Classification and Applications of FL Architectures: Federated learning architectures are categorized into three main types: horizontal federated learning, vertical federated learning, and federated transfer learning. This section analyzes the application of these architectures across various domains, highlighting their distinctive features and associated challenges.
Applications in IoT, Smart Cities, and Healthcare: Using selected case studies, this section evaluates the deployment of FL in the Internet of Things (IoT), smart cities, and healthcare. It assesses how FL enhances data privacy, security, and operational efficiency in these domains, focusing on practical implementations.
Comparative Analysis: This section offers a comparative evaluation of the various methods and algorithms used in the aforementioned fields, identifying their relative strengths and weaknesses. Special attention is given to the challenges posed by large-scale FL deployments, including communication overhead, data heterogeneity, and model convergence.
Federated Learning and Related Technologies: This section explores the integration of FL with related technologies, such as federated deep learning and federated blockchain, particularly within the context of the Industrial Internet of Things (IIoT). The potential of these technologies to improve storage, data management, and resource optimization is discussed in detail.
Challenges and Future Directions: The final section addresses the ongoing challenges facing FL, including scalability, model accuracy, communication costs, and compliance with regulatory frameworks. Additionally, it proposes future research directions aimed at improving the practicality and widespread adoption of FL in industrial and commercial applications.
This systematic review provides a comprehensive examination of federated learning's current state, including its foundational concepts, applications, and challenges. It also outlines a forward-looking perspective on the advancements needed to establish FL as a key technology in privacy-centric, decentralized machine learning.

Keywords: **Federated learning, decentralized machine learning, privacy-preserving, Distributed artificial intelligence, Internet of Things.**

۱-مقدمه

هوش مصنوعی توزیع‌شده عنوان شاخه‌ای نوظهور از هوش مصنوعی، بر همکاری و تعامل میان چندین عامل مستقل متمرکز است؛ در این رویکرد، هر عامل به‌صورت محلی داده‌های خود را پردازش می‌کند و از طریق تبادل اطلاعات و دانش با سایر عوامل، به‌طور جمعی به یک مدل یادگیری ماشین دست می‌یابند. این نگرش به هوش مصنوعی توزیع‌شده، با تسهیل هماهنگی و همکاری میان عوامل مختلف در پردازش داده‌ها و یادگیری ماشین، به بهبود قابل‌توجهی در کارایی و گسترهٔ کاربردهای هوش مصنوعی منجر می‌شود.

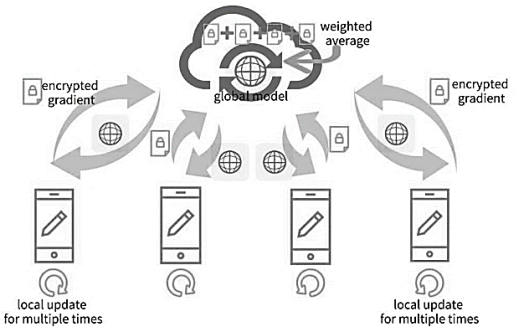
یادگیری مشارکتی[1] به‌عنوان رویکرد نوآورانه در حوزهٔ هوش مصنوعی توزیع‌شده یک طرح یادگیری ماشین در حال رشد است که هدف آن حل مشکل جزیرهٔ داده‌ها با حفظ حریم خصوصی داده‌هاست[۱]؛ در این روش، الگوریتم یادگیری ماشین بدون انتقال داده، در دستگاه‌ها یا سرورهای مختلف داده‌های محلی را آموزش می‌بینند. متفاوت از روش‌های سنتی که تمام داده‌ها را در یک سرور متمرکز جمع‌آوری می‌کنند، داده‌ها به‌صورت محلی

[1] Federated learning (FL)

[DOI: 10.61186/jsdp.21.3.23]

آموزش می‌بینند؛ این رویکرد با روش‌های غیرمتمرکز کلاسیک که فرض می‌کنند نمونه‌های دادهٔ محلی توزیع یکسان می‌شوند، متفاوت است. یادگیری مشارکتی به چندین مشتری[1] این امکان را می‌دهد که بدون نیاز برای به اشتراک‌گذاشتن داده‌ها، یک مدل یادگیری ماشین مشترک و اثربخش بسازند؛ همچنین امکان پردازش مفاهیم اساسی مانند حریم خصوصی، امنیت‌داده‌ها و دسترسی به داده‌های ناهمگن را فراهم می‌کند.

این روش را نخستین‌بار گوگل در سال ۲۰۱۶ به‌منظور پیش‌بینی ورودی متن کاربر در ده‌ها هزار دستگاه اندروید با ذخیرهٔ اطلاعات در دستگاه ارائه کرد[۲]؛ در این روش چندین مشتری مانند دستگاه‌های تلفن همراه، مؤسسات، سازمان‌ها و غیره وجود دارد که با یک یا چند سرور مرکزی برای تنظیمات یادگیری ماشین غیرمتمرکز هماهنگ شده‌اند. درحقیقت، یادگیری مشارکتی ارائه‌شدهٔ گوگل یک فناوری یادگیری ماشین توزیع‌شدهٔ رمزگذاری شده‌است که به شرکت‌کنندگان امکان ساخت یک مدل آموزشی مشترک با حفظ داده‌های اساسی به‌صورت محلی می‌دهد. امروزه مفهوم یادگیری مشارکتی گسترش یافته‌است و به تمام روش‌های یادگیری ماشین غیرمتمرکز و مشترک در حفظ حریم‌خصوصی اشاره‌دارد[۳]. روند اصلی یادگیری مشارکتی در (شکل-۱) شرح داده‌شده‌است[۴].



(شکل-۱): فرایند یادگیری مشارکتی[۴]

(Figure -1) Process of Federated learning

حوزهٔ یادگیری مشارکتی در سال‌های اخیر شاهد رشد چشمگیری در انتشار مقالات مروری بوده‌است؛ بااین‌حال، مقالهٔ حاضر رویکردی متمایز از سایر مقالات این حوزه دارد. این مقاله مروری نظام‌مند با ارائهٔ یک بررسی جامع و نظام‌مند از پژوهش‌های مروری موجود در حوزهٔ یادگیری مشارکتی، از سطح لیست‌کردن و خلاصه‌سازی مقالات فراتر رفته و به واکاوی عمیق و تحلیلی این حوزه می‌پردازد؛ علاوه‌براین، در این مقالهٔ مروری، پژوهش‌های بررسی‌شده از نظر کاربرد، مزایا، محدودیت‌ها و چالش‌ها با یکدیگر مقایسهٔ عمیق و دقیق می‌شوند؛ این امر به خوانندگان در زمینهٔ درک عمیق‌تر و دقیق‌تری از چشم‌انداز پژوهشی در این زمینه کمک می‌کند. از دیگر ویژگی‌های این مقاله، تمرکز بر کاربردهای یادگیری مشارکتی در حوزه‌های مختلف است؛ اینترنت اشیا، شهر هوشمند، امنیت، حفظ حریم خصوصی مدل و داده‌ها، انفورماتیک سلامت و مراقبت‌های بهداشتی تنها تعدادی از حوزه‌هایی هستند که در این مقاله به آن‌ها پرداخته می‌شود. علاوه‌براین، به کاربردها و تفاوت‌های یادگیری ماشین و یادگیری عمیق مشارکتی و بلاک‌چین مشارکتی در اینترنت صنعتی اشیا[2] پرداخته می‌شود. این موضوع با توجه به اهمیت روزافزون این فناوری‌ها در زمینه‌های مختلف، از جمله یادگیری مشارکتی، بسیار حائز اهمیت است. در نهایت، تفاوت‌های یادگیری مشارکتی با پارادایم‌های مشابه مانند یادگیری گروهی و یادگیری توزیع‌شده کامل تشریح می‌شود؛ این امر به خوانندگان کمک می‌کند تا به درک روشن‌تری از ماهیت و جایگاه یادگیری مشارکتی در میان سایر روش‌های یادگیری دست یابند. درکل، این مقالهٔ مروری به ارائهٔ یک بررسی جامع، عمیق و نظام‌مند از پژوهش‌های مروری موجود در حوزهٔ یادگیری مشارکتی، در این زمینه عمل می‌کند.

این مقاله به شرح زیر تنظیم شده‌است: در مقدمه، نمایی کلی از یادگیری مشارکتی ترسیم می‌شود که شامل معرفی و شرح فرایند آن است. در بخش دوم به مرور پیشینهٔ پژوهش، معرفی الگوریتم‌های موجود و بررسی سیر تکامل الگوریتم‌های یادگیری مشارکتی پرداخته می‌شود. در بخش سوم، به طبقه‌بندی انواع ساختارهای یادگیری مشارکتی و بررسی کاربرد هر کدام از آن‌ها پرداخته می‌شود. در بخش چهارم روش پژوهش، ارائهٔ استراتژی جست‌وجو، تشریح نحوهٔ انتخاب منابع و تشریح مفاهیم مستخرج از مقاله‌ها معرفی می‌شود. در

[1] client

[2] Industrial Internet of Things (IIoT)

[DOI: 10.61186/jsdp.21.3.23]

بخش پنجم به مسائل باز و چشم‌اندازهای آینده پرداخته می‌شود. بخش انتهایی نیز ارائهٔ نتیجه‌گیری از پژوهش و پیشنهادها برای پژوهش‌های آینده را شامل می‌شود.

۲-پیشینهٔ پژوهش

امروزه مفهوم یادگیری مشارکتی به‌طور گسترده مطرح شده‌است و در زمینه‌های مختلف اجرا و اعمال می‌شود[۵]. بیشترین پژوهش‌ها در حوزهٔ یادگیری توزیع‌شده در توسعهٔ داده‌های بزرگ [۶] و رایانش ابری [۷] بوده‌است. در سال‌های اخیر، داده‌ها و منابع محاسباتی معمولاً در دستگاه‌های کاربران نهایی، مناطق یا سازمان‌های مختلف توزیع می‌شوند. به‌دلیل قوانین یا مقررات، داده‌های توزیع‌شده و منابع محاسباتی را نمی‌توان جمع‌آوری کرد یا مستقیم بین مناطق یا سازمان‌های مختلف برای وظایف یادگیری ماشین به اشتراک گذاشت[۸].

هستهٔ اصلی یادگیری مشارکتی در ساخت مدل یادگیری ماشین از داده‌های توزیع‌شده در چندین دستگاه استفاده می‌کند. این رویکرد به‌عنوان یک راه‌کار کارآمد برای بهره‌برداری از داده‌های توزیع‌شده و منابع محاسباتی مشترک، مدل‌های یادگیری ماشین را با اطمینان از امنیت اطلاعات، حریم خصوصی داده‌ها و انطباق با قوانین مختلف در حین فرایند یادگیری مدل‌ها، به‌صورت مشترک آموزش می‌دهد[۹].

درحالی‌که شبکه‌های عصبی از محبوب‌ترین الگوریتم‌ها در یادگیری مشارکتی هستند، تنوع عظیمی از الگوریتم‌های یادگیری ماشین وجود دارد که می‌توان از آن‌ها در این روش استفاده کرد؛ الگوریتم‌های مهمی مانند جنگل تصادفی[1] نیز می‌توانند در این زمینه مفید باشند. این الگوریتم به‌دلیل دقت بالا و مقاومت در برابر ناهنجاری‌ها شناخته شده‌است[۱۰]. علاوه بر جنگل تصادفی، الگوریتم‌های دیگری مانند k نزدیک‌ترین همسایه[2]، ماشین‌های بردار پشتیبان[3] و الگوریتم‌های یادگیری تقویتی[4] نیز می‌توانند در یادگیری مشارکتی مورد استفاده قرارگیرند. انتخاب الگوریتم مناسب به عوامل مختلفی مانند نوع داده‌ها، وظیفهٔ یادگیری ماشین، محدودیت‌های محاسباتی و نیازهای امنیتی بستگی دارد.

ظهور این فناوری تناقض بین حریم خصوصی داده‌ها و اشتراک داده‌ها را برای دستگاه‌های پراکنده حل خواهد کرد. با توجه به استفاده از داده‌های چندجانبه در این روش، یکی از کاربردهای این مفهوم در پردازش اطلاعات شرکت‌های بیمه است که همواره نگران محافظت از داده‌های خود هستند و تمایلی به اشتراک‌گذاری داده‌ها با سایر نهادها ندارند[۱۱]؛ همچنین یادگیری مشارکتی نقش مهمی در توسعهٔ شهرهای هوشمند دارد. با توسعهٔ داده‌های بزرگ و هوش مصنوعی، این مفهوم می‌تواند مشکلاتی که در زمینهٔ حفاظت از حریم خصوصی داده‌ها ایجاد می‌شود، را حل کند[۱۲].

یکی دیگر از کاربردهای این روش در حوزهٔ سلامت و دستگاه‌های همراه است؛ جایی‌که داده‌ها به‌طور ذاتی در دسترس نیستند. در این زمینه، از یادگیری مشارکتی می‌توان برای جمع‌آوری و تحلیل داده‌ها از دستگاه‌های مختلف مانند گوشی‌های هوشمند، ساعت‌های هوشمند و حس‌گرهای زیستی استفاده کرد. به‌تازگی، دانشمندان این حوزه مقالات متعددی در زمینهٔ بررسی پیشرفت‌ها و چالش‌های یادگیری مشارکتی در حوزهٔ سلامت منتشر کرده‌اند[۱۳].

پژوهش‌های اخیر بیشتر در خصوص چالش‌های آماری یادگیری مشارکتی [۱۴] و مسائل امنیتی [۱۵] در جهت حفظ حریم خصوصی و شخصی‌شدن داده‌ها [۱۶] ارائه شده‌است. پژوهش‌گران در تلاش‌اند به‌منظور بهبود کیفیت و کارایی سیستم‌های یادگیری، مداوم بر چالش‌های مربوط به حریم خصوصی داده‌ها، توزیع نامتوازن داده‌ها، محدودیت‌های محاسباتی و هزینه‌های ارتباطی غلبه کنند. با وجود چالش‌های موجود، یادگیری مشارکتی ابزاری قدرتمند برای بهبود فرایندها و ارتقای کیفیت خدمات ارائه‌شده در نظام‌های سلامت است. با تلاش‌های پژوهش‌گران برای غلبه بر این چالش‌ها، شاهد کاربردهای جدید و نوآورانهٔ این فناوری در حوزهٔ سلامت خواهیم بود.

پایهٔ یادگیری مشارکتی در بسیاری از پژوهش‌ها، رویکردی به‌نام میانگین مشارکتی[5] است. در مرحلهٔ نخست این روش، هر دستگاه یک مدل جهانی کلی را برای

[1] Random Forest
[2] K-Nearest Neighbors
[3] Support Vector Machines
[4] Reinforcement Learning
[5] FedAvg

[DOI: 10.61186/jsdp.21.3.23]

آموزش محلی بارگیری می‌کند؛ در مرحلهٔ دوم، مدل جهانی با به‌روزرسانی محلی انجام‌شده بر روی داده‌های محلی، متعلق به مشتری‌های مختلف بهبود می‌یابد؛ سپس اطلاعات شیب مربوطه در حالت رمزگذاری برای ابر بارگذاری می‌شوند؛ درنهایت، میانگین به‌روزرسانی مدل‌های محلی پیاده‌سازی‌شده در فضای ابری، به عنوان یک مدل جهانی تازه به دستگاه ارسال می‌شود و در انتها روش‌های بالا تکرار می‌شوند تا مدل هم‌گرا شود. میانگین مشارکتی به‌عنوان چارچوب ابتدایی یادگیری مشارکتی، اگرچه می‌تواند با برخی از داده‌های غیرمستقل ناهمگن[1] مقابله کند، اما هنوز با چالش‌هایی مانند سربار بالای ارتباطات و ناهمگنی ساختاری روبه‌روست.

پژوهش‌های اخیر در زمینهٔ یادگیری مشارکتی بر بهینه‌سازی الگوریتم‌ها متمرکز شده‌است. هدف این مطالعات، ارتقای کارایی، دقت و حفظ حریم خصوصی شرکت‌کنندگان در این فرایند است. افزایش حفاظت از داده‌ها، نقشی اساسی در افزایش مشارکت در این روش نوین جمع‌آوری و تحلیل‌داده‌ها دارد. در این راستا، بسیاری از پژوهش‌گران به بررسی پیشرفت‌ها و چالش‌های موجود در زمینهٔ یادگیری مشارکتی پرداخته‌اند[۱۳]. هزینهٔ ارتباطی بالا، ناهمگنی آماری و ساختاری از مهم‌ترین چالش‌ها و مسائلی هستند که پژوهش‌گران در زمینهٔ بهینه‌سازی یادگیری مشارکتی برای حل و بهبود آن‌ها تمرکز دارند[۹].

علاوه بر بهینه‌سازی تخصیص منابع یا طراحی معماری جدید، ایجاد سازوکار تشویقی برای افزایش تعداد مشتری‌های شرکت‌کننده در آموزش نیز یک روش مؤثر برای بهبود عملکرد سامانه است؛ در حالت پایه، میانگین مشارکتی مشتری‌ها را به‌طور تصادفی انتخاب می‌کند. در این رویکرد این فرض وجود دارد که تمام مشتری‌ها تمایل یکسانی به شرکت در آموزش دارند؛ بااین‌حال، در واقعیت این‌طور نیست. برخی از مشتری‌های تنبل دارای کیفیت بالا یا برخی از مشتری‌های خودخواه، به‌دلیل نگرانی از مصرف منابع شخصی، ممکن است در تمام مراحل آموزش شرکت نکنند؛ بنابراین، ایجاد یک سازوکار تشویقی می‌تواند انگیزهٔ مشتریان را برای مشارکت در آموزش افزایش دهد. سرور ابری می‌تواند با توجه به سهم هر شرکت‌کننده، پاداشی به آن‌ها اختصاص دهد. این پاداش می‌تواند به‌صورت اعتبار، امتیاز یا سایر مزایا باشد. پاداش‌ها باید به‌گونه‌ای طراحی شوند که انگیزهٔ تمام مشتریان را برای مشارکت در آموزش، صرف‌نظر از سطح کیفیت یا تمایل آن‌ها، افزایش دهد. این اقدام باعث می‌شود که شرکت‌کنندگان سودمندی خود در فرایند آموزش را برای به‌دست‌آوردن درآمد بیشتر به بیشینه برسانند.

چارچوب‌هایی مانند تئوری بازی مبتنی بر استاکلبرگ[2] از محبوبیت گسترده‌ای در طراحی سازوکار انگیزه برخوردارند[۱۷]. پژوهش‌گران به بررسی دیدگاه استاکلبرگ پرداختند تا مشتری‌ها را به اختصاص CPU بیشتر برای آموزش محلی الهام دهند و همچنین سازوکار تشویقی برای تنظیم زمان تکرار محلی به‌صورت سازگار افزایش یابد[۱۸]. چارچوب تأمین منابع‌انسانی برای دستیابی به حداکثر استفاده دربین مشتری‌ها و سرورها، یک مدل دو مرحله‌ای استاکلبرگ را اتخاذ می‌کند[۱۹]. نخستین الگوریتم‌های بهینه‌سازی متحد مبتنی بر تجمع شیب مشتری در سال ۲۰۱۶ ارائه شد[۲۲-۲۰].

یادگیری مشارکتی مجزا از مسائل حریم خصوصی نیست؛ از یک‌سو، در به‌روزرسانی‌های مدل ارسال‌شدهٔ مشتری‌ها در هر دورهٔ آموزشی ممکن است اطلاعات مربوط به داده‌های خصوصی مشتری‌ها افشا شود، از سوی دیگر، مدل آموزش‌دیده به‌وسیلهٔ سرور ممکن است مورد حملهٔ مشتری‌های مخرب قرارگیرد؛ این حملات می‌توانند به مسمومیت مدل، جلوگیری از هم‌گرایی و کاهش دقت آن منجر شوند[۴]. هرگونه نفوذ مخرب و حمله سبب آسیب‌پذیری شبکه و اطلاعات می‌شود که نقض سیاست‌های امنیتی از جمله محرمانگی، یکپارچگی و در دسترس‌بودن را به‌دنبال دارد[۲۳]. در سال‌های اخیر موارد بسیاری از آسیب‌پذیری شبکه‌های عصبی عمیق نسبت به حملاتی مطرح شده‌است که بیشتر، بر دادهٔ ورودی ایجاد می‌شوند و خروجی شبکهٔ آموزش دید را تغییر می‌دهند[۲۴].

با وجود چالش‌هایی که پیش‌روی این روش است، یادگیری مشارکتی فرصتی برای ارتقای کیفیت مدل‌های

[1] Non-Independent and Identically Distributed(non-iid)

[2] Stackelberg game theory

[DOI: 10.61186/jsdp.21.3.23]

یادگیری ماشین و ارائهٔ خدمات بهتر به کاربران ارائه می‌دهد. با استفاده از راه‌کارهای مناسب می‌توان از حریم خصوصی داده‌ها محافظت کرد و از مزایای این روش نوین بهره‌مند شد. پژوهش‌گران در مرجع [۲۵] اجرای کارآمدتر ارتباطات با میانگین مشارکتی را توصیف کردند، که در آن پارامترهای مدل با میانگین وزنی از پارامترهای مدل ارسال‌شده توسط مشتری‌ها در هر تکرار به‌روز می‌شوند.

تأیید اعتبار یک مدل بازگشتی در یادگیری مشارکتی با استفاده از روش‌های حفظ حریم خصوصی، بر پایهٔ فرضیه‌ای استوار است که بر صداقت نسبی مشتریان در تعامل با سیستم تأکید دارد. این فرضیه به این معناست که مشتریان ملزم به رعایت دقیق قوانین آموزشی‌اند و انتظار می‌رود که صادقانه و بدون سوءاستفاده از داده‌ها، به یادگیری مشارکتی بپردازند. بااین‌حال، درعمل، چالش‌هایی ممکن است به‌وجود آید که این فرض را نقض کند. برخی از مشتریان ممکن است به‌دنبال استنباط اطلاعات خصوصی دیگران از طریق مدل باشند؛ علاوه‌براین، برخی مشتریان ممکن است عمدی یا سهوی، مدل‌های نادرستی را به اشتراک بگذارند که می‌تواند منجر به انحراف مدل جهانی از حالت بهینه و ایجاد خطاهای جدی شود؛ برای مثال، در سامانه‌های حساس به حریم خصوصی مانند اطلاعات پزشکی محرمانه، مهاجمان ممکن است با تولید داده‌های به‌ظاهر معتبر اما نادرست، به کل مدل حمله کنند و دقت و صحت آن را به‌طور جدی تحت‌تأثیر قراردهند[۲۶].

مواجهه با مسائل بیزانسی همواره یکی از چالش‌های اساسی در یادگیری مشارکتی بوده‌است؛ این مسائل زمانی بروز می‌کنند که برخی مشتریان از پروتکل‌های آموزشی تعیین‌شده پیروی نمی‌کنند یا عمدی به مدل جهانی حمله می‌کنند. برای مقابله با این چالش‌ها، توسعهٔ مدل‌هایی با مقاومت بالا در برابر خطاهای بیزانسی ضروری است. چنین مدل‌هایی قادر خواهند بود تا فرایند آموزش مشترک را به‌طور صحیح و مؤثر ادامه دهند و کیفیت یادگیری را حتی در مواجهه با نداشتن صداقت برخی از مشتریان حفظ کنند. این رویکرد تضمین می‌کند که مدل جهانی از مسیر بهینهٔ خود منحرف نشده و دقت آن تحت‌تأثیر حملات بیزانسی قرارنگیرد.

روش‌های پیشین برای مقابله با مسائل بیزانسی در یادگیری مشارکتی، درحضور مشتریان معیوب یا مخرب، شکننده‌اند؛ به‌همین‌دلیل، روش‌های جدید و قدرتمندتری در ادبیات پژوهش برای حل این مشکل ارائه شده‌است. انتخاب روش مناسب به عوامل مختلفی مانند نوع داده‌ها، تعداد مشتریان و بودجهٔ موجود بستگی دارد. پژوهش‌گران در منبع[۲۷] روش KRUM را به‌عنوان یک قانون تجمع بیزانسی قوی ارائه دادند؛ این روش بر اساس شباهت شیب‌ها یا به‌روزرسانی‌های ارائه‌شده به‌وسیلهٔ تمام مشتریان در هر تکرار عمل می‌کند؛ همچنین یک تحلیل نظری ارائه‌دادند که استحکام مدل را تحت فرضیات خاص تضمین می‌کند. از آنجا که KRUM در مقایسه با سایر قوانین تجمع به آهستگی هم‌گرا می‌شود، نویسندگان همچنین MKRUM را معرفی کردند که عملکرد مشابهی را با سرعت هم‌گرایی سریع‌تر به‌دست می‌آورد[۲۸].

قوانین تجمع قوی نوعی از قوانین تجمع در یادگیری مشارکتی‌اند که در برابر حملات بیزانسی مقاوم‌اند. این روش‌ها از محاسبهٔ میانه برای به‌روزرسانی‌های مدل استفاده می‌کنند. پژوهش‌گران در منبع [۲۹] الگوریتم میانهٔ مختصات[1] را پیشنهاد دادند. در ادامه پژوهش‌گران الگوریتم بازگشتی Bulyan را پیشنهاد کردند[۳۰]. این الگوریتم از قوانین تجمیع قوی بیزانس، مانند KRUM یا COMED پیروی می‌کند[۲۹]. در سال ۲۰۱۹ پژوهش‌گران برای بهبود مقاومت در برابر حملات مسمومیت[2]، سازوکار تجمیع قوی Zeno را پیشنهاد دادند. این سازوکار هدف خود را رتبه‌بندی برآورد گرادیان مشتریان قرارمی‌دهد[۳۱]. پژوهش‌گران برای شناسایی به‌روزرسانی‌های غیرعادی در یادگیری مشارکتی، از روش‌های مختلفی استفاده می‌کنند؛ یکی از این روش‌ها، استفاده از رمزگذار خودکار است. این رمزگذار خودکار می‌تواند پارامترهای مدل را با یک بردار در ابعاد کم جایگزین کند. این امر شناسایی به‌روزرسانی‌های وزن نامنظم که توسط مشتریان مخرب ارسال می‌شوند را آسان‌تر می‌کند[۳۲]. گروهی دیگر از پژوهش‌گران، روش

[1] COMED
[2] Poisoning

[DOI: 10.61186/jsdp.21.3.23]

یادگیری مشارکتی انطباقی را برای شناسایی به‌روزرسانی‌های غیرعادی ارائه داده‌اند. در این روش، از یک مدل مخفی مارکوف[1] برای ارزیابی کیفیت مدل استفاده می‌شود[۳۳].

مدل مخفی مارکوف به تخمین احتمال تولید هر به‌روزرسانی به‌وسیلهٔ یک مدل سالم می‌پردازد. بر مبنای این تخمین، به‌روزرسانی‌هایی با احتمال پایین، غیرعادی تلقی می‌شوند. در پژوهش دیگری برای مقابله با حملات مسمومیت و شناسایی و حذف به‌روزرسانی‌های بد ارائه‌شده توسط مشتریان یک الگوریتم میانگین‌گیری مشارکتی مبتنی بر بازی معرفی می‌شود. سرور با استفاده از ویژگی تعادل نش، احتمال ارائهٔ به‌روزرسانی‌های خوب توسط هر مشتری را تعیین می‌کند[۳۴]. سامانه‌های سنتی تحمل خطای بیزانسی، قادر به شناسایی تمام کاربران مخرب نیستند. این نقص باعث کاهش دقت مدل در محیط یادگیری مشارکتی و ظهور تهدیدات امنیتی می‌شود؛ به‌منظور رفع این مشکل، طراحی سامانه‌های تحمل خطای بیزانسی با دقت تشخیص خطای بالاتر، ضرورتی اجتناب‌ناپذیر است. در سال‌های اخیر، پژوهش‌های متعددی در این زمینه صورت‌گرفته که به پیشرفت‌های قابل توجهی در زمینهٔ مقابله با حملات بیزانسی و حفظ دقت مدل در یادگیری مشارکتی دست یافته‌است.

با وجود اینکه در یادگیری مشارکتی شاهد بهبود چالش‌های سنتی یادگیری متمرکز مانند نقض حریم خصوصی داده و هزینه‌های بالای نگهداری در محیطی متمرکز هستیم، اما در سناریوهای دنیای واقعی، استقرار یادگیری مشارکتی با چالش‌هایی مواجه است؛ از جملهٔ این چالش‌ها می‌توان به تنظیم پارامترها و ساختارهای مرتبط با مشتری به‌دلیل پراکندگی و تنوع داده‌ها اشاره‌کرد. این مسائل باعث شده‌است که مطالعات متعددی به بررسی و ارائهٔ راه‌حل‌های مناسب برای غلبه بر این چالش‌ها بپردازند.

پژوهش‌گران در مرجع [۳۵] رویکردی نوآورانه مبتنی بر الگوریتم‌های ژنتیک[2] برای تنظیم خودکار ساختارها و پارامترها در یادگیری مشارکتی پیشنهاد کرده‌اند؛ در این پژوهش با ادغام الگوریتم ژنتیک با مشتریان مبتنی بر فرایادگیری مدل آگنوستیک [3] جنبه‌های مختلفی مانند ساختار طبقه‌بندی نمودار، نرخ یادگیری و نوع تابع بهینه‌سازی به‌صورت خودکار تنظیم شده‌است. این رویکرد به بهبود عملکرد سیستم‌های یادگیری مشارکتی از طریق بهینه‌سازی پارامترها و ساختارهای مورد استفاده در فرایند یادگیری کمک می‌کند.

۳-مفاهیم پایه

۳-۱-مقایسهٔ یادگیری مشارکتی با یادگیری گروهی[4] و یادگیری توزیع‌شده[5]

با وجود پیشرفت‌های چشمگیر در حوزهٔ کشف دانش، روش‌های سنتی یادگیری ماشین در مواجهه با داده‌های پیچیده، از جمله داده‌های نامتعادل، داده‌های با ابعاد بالا، داده‌های نوفه‌ای و موارد مشابه، به‌دلیل پیچیدگی ذاتی، کارایی مطلوبی ارائه نمی‌دهند؛ علت این مسئله ناتوانی این روش‌ها در مقابله با چالش‌های مرتبط با ویژگی‌ها و ساختار داده‌هاست؛ به‌ویژه در مواجهه با داده‌های نامتعادل که دارای ابعاد بالا یا حاوی نوفه‌اند، این روش‌ها عملکرد مطلوبی ندارند[۳۶].

چالش‌های پیش‌رو در حوزهٔ داده‌کاوی، ضرورت ایجاد یک مدل کارآمد برای کشف دانش و پردازش داده‌ها را بیش‌ازپیش آشکار کرده‌است؛ به‌منظور رفع این چالش، از سه پارادایم یادگیری ماشین، یعنی یادگیری مشارکتی، یادگیری گروهی و یادگیری توزیع‌شده استفاده می‌شود. هر یک از این پارادایم‌ها با ویژگی‌ها و اهداف منحصربه‌فرد خود، ابزارهای متنوعی را برای تحلیل‌داده‌ها فراهم می‌آورند. انتخاب پارادایم بهینه به متغیرهای مختلفی نظیر اهداف پژوهش، حجم داده‌ها و نیازهای خاص پروژه وابسته است.

یادگیری مشارکتی یک رویکرد نوین در یادگیری ماشین توزیع‌شده است که به‌واسطهٔ آن، انبوهی از دستگاه‌های محاسباتی لبه می‌توانند بدون به اشتراک گذاشتن داده‌های خصوصی، به‌طور مشترک یک مدل یادگیری را آموزش ببینند[۳۷]. در فرایند یادگیری

[1] Hidden Markov Model (HMM)
[2] Genetic Algorithms (GA)
[3] Model Agnostic Meta-Learning (MAML)
[4] Ensemble Learning
[5] Distributed Learning

[DOI: 10.61186/jsdp.21.3.23]

مشارکتی، داده‌ها بین چندین مشتری و دستگاه به اشتراک گذاشته می‌شوند. هر دستگاه مدل محلی خود را بر اساس داده‌های محلی آموزش می‌دهد و به‌طور دوره‌ای پارامترهای مدل‌های محلی خود را با سرور مرکزی به اشتراک می‌گذارند؛ سپس، سرور مرکزی پارامترها را جمع‌آوری و مدل جهانی را به‌روزرسانی می‌کند. این رویکرد برجسته، حفظ حریم خصوصی را در اولویت قرارمی‌دهد؛ به این ترتیب که هر کاربر بدون نیاز به انتقال مستقیم داده‌ها، با به اشتراک‌گذاری پارامترهای مدل خود، به ارتقای مدل جهانی کمک می‌کند[۳۱].

یادگیری گروهی به‌عنوان یک حوزهٔ پژوهشی پویا، با هدف ادغام داده‌ها، مدل‌سازی داده و داده‌کاوی در یک چارچوب یکپارچه مورد استفاده قرارمی‌گیرد؛ در این رویکرد، داده‌ها بین چندین مدل تقسیم می‌شوند و هر مدل مستقل بر روی بخش مشخصی از داده‌ها آموزش می‌بینند. پس از اتمام فرایند آموزش، مدل‌ها پیش‌بینی‌های خود را با یکدیگر به اشتراک می‌گذارند و پیش‌بینی نهایی با ترکیب پیش‌بینی‌های مدل‌های مختلف محاسبه می‌شود. سادگی در پیاده‌سازی و افزایش دقت مدل از طریق بهره‌گیری از تنوع مدل‌ها، از مزایای برجستهٔ این روش است؛ همچنین، به‌دلیل آموزش مستقل هر مدل، این رویکرد به‌خوبی با محیط‌هایی سازگار است که در آن‌ها مدل‌ها به‌صورت مستقل قابل استفاده‌اند[۳۶, ۳۸].

اگرچه آموزش مدل‌های یادگیری ماشین کوچک با حجم متوسطی از داده امکان‌پذیر است، اما با افزایش ابعاد مدل‌ها، به‌ویژه در شبکه‌های عصبی، با رشد چشم‌گیری در تعداد پارامترها همراه است. از آنجا که تقاضا برای پردازش داده‌های آموزشی از توان محاسباتی ماشین‌ها پیشی گرفته‌است، توزیع بار پردازش یادگیری ماشین بین چندین ماشین و تبدیل سامانه متمرکز به یک سامانه توزیع‌شده ضرورتی اجتناب‌ناپذیر به‌نظر می‌رسد[۳۹].

در یادگیری توزیع‌شده، داده‌ها بین چندین مشتری یا دستگاه توزیع می‌شوند و یک مدل واحد هم‌زمان و موازی بر روی تمام بخش‌های داده‌ها آموزش می‌بینند؛ در این رویکرد مدل‌ها مداوم پارامترها و به‌روزرسانی‌های خود را با یکدیگر به اشتراک می‌گذارند. این الگو به‌دلیل سرعت بالای آموزش و کارآمدی در پردازش مجموعه‌داده‌های بزرگ، با استفاده از قدرت پردازشی چندین ماشین یا دستگاه، شناخته می‌شود. از مزایای اصلی این روش می‌توان به کاهش زمان آموزش و توانایی مدیریت داده‌های بزرگ اشاره کرد؛ زیرا بار محاسباتی بین چندین دستگاه تقسیم می‌شود. بااین‌حال، نیاز به زیرساخت قوی و مشکلات هماهنگ‌سازی[1] از جمله چالش‌های اصلی این روش محسوب می‌شوند و می‌توانند بر عملکرد نهایی مدل تأثیر بگذارند[۴۰]. دست‌یابی به تعادل بین توان محاسباتی و کارایی شبکه، برای موفقیت این روش ضروری است.

(جدول-۱): مقایسهٔ یادگیری مشارکتی، یادگیری گروهی و یادگیری توزیع‌شده

(Table-1): Comparing Federated Learning, Ensemble Learning, and Distributed Learning.

پارادایم	توزیع داده‌ها	تبادل اطلاعات	مزایا	معایب
یادگیری مشارکتی	بین دستگاه‌ها	پارامترها	حریم خصوصی، دقت بالا	پیاده‌سازی پیچیده، آموزش کندتر
یادگیری گروهی	بین مدل‌ها	پیش‌بینی‌ها	پیاده‌سازی ساده، دقت بالا، آموزش سریع	نیاز به قدرت پردازش، بیش برازش[2]
یادگیری توزیع‌شده	بین دستگاه‌ها	پارامترها	سرعت بالا آموزش، مناسب برای داده‌های بزرگ	نیاز به زیرساخت قوی، مشکلات هماهنگ‌سازی

درکل، یادگیری مشارکتی با تمرکز بر حفظ حریم خصوصی و دقت بدون اشتراک‌گذاری مستقیم داده‌ها، یادگیری گروهی با سهولت در پیاده‌سازی، توانایی افزایش دقت مدل و سرعت بالا در آموزش از طریق ترکیب نتایج چندین مدل و یادگیری توزیع‌شده با سرعت بالا در آموزش و توانایی مدیریت مجموعه‌داده‌های بزرگ از طریق پردازش موازی، مزایای منحصربه‌فرد خود را دارند. انتخاب رویکرد مناسب به ویژگی‌های خاص هر پروژه و نیازهای آن بستگی دارد.

۳-۲-طبقه‌بندی یادگیری مشارکتی

بر اساس مقالهٔ ارائه‌شده در سال ۲۰۱۹، یادگیری مشارکتی بیشتر به سه گروه تقسیم می‌شود: یادگیری

[1] synchronization
[2] overfitting

[DOI: 10.61186/jsdp.21.3.23]

مشارکتی افقی[1]، یادگیری مشارکتی عمودی[2] و یادگیری انتقال مشارکتی[3][۴۱]؛ از آنجا که داده‌های ذخیره‌شده بیشتر به‌صورت ماتریس ویژگی وجود دارند، شامل مقادیر متعددی هستند. در این سناریو محور افقی صفحه به‌عنوان مشتری درنظر گرفته‌می‌شود؛ در حالی که محور عمودی نشان‌دهندهٔ ویژگی‌های مرتبط با مشتری است؛ بنابراین می‌توان یادگیری مشارکتی را بر اساس حالت افراز[4] داده تقسیم کرد.

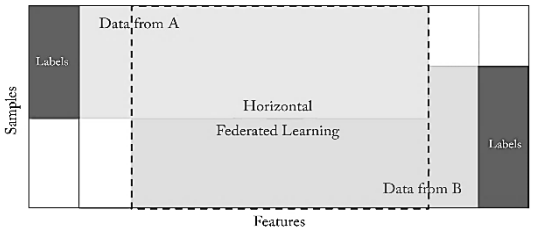
۳-۲-۱-یادگیری مشارکتی افقی

یادگیری مشارکتی افقی نوعی یادگیری مشارکتی است که در آن گره‌ها داده‌های متفاوتی دارند، اما ویژگی‌های مشترکی بین داده‌ها وجود دارد؛ به‌عبارت‌دیگر، فضای نمونه‌داده‌ها در گره‌های مختلف متفاوت، اما فضای ویژگی آن‌ها مشابه است. یادگیری مشارکتی افقی برای استفاده در دستگاه‌های هوشمند و دستگاه‌های متصل به اینترنت اشیا [۴۲] طراحی شده‌است. الگوریتم یادگیری مشارکتی که گوگل ارائه داده[۲]، در واقع نوعی یادگیری مشارکتی افقی است؛ زیرا با وجود اختلاف قابل توجه داده‌ها در فضای نمونه، دارای فضای ویژگی مشابه‌اند[۴۳].

الگوریتم یادگیری مشارکتی گوگل نمونه‌ای موفق از کاربرد یادگیری مشارکتی افقی در دستگاه‌های هوشمند است و نشان می‌دهد که یادگیری مشارکتی افقی می‌تواند برای آموزش مدل‌های یادگیری ماشین در مقیاس‌های بزرگ مفید باشد؛ این روش به‌دلیل عدم حاشیه‌نویسی داده‌ها[5] در طبقه‌بندی الکتروانسفالوگرافی[6] مفید است. روش‌های یادگیری عمیق در حوزهٔ رابط‌های مغز و رایانه (BCI)[7] برای طبقه‌بندی الکتروانسفالوگرافی[8] به‌دلیل کمبود مجموعه‌داده‌های بزرگ محدودیت دارند. امنیت داده یکی از بزرگ‌ترین چالش‌های پیش‌روی BCI مبتنی بر EEG است. سیگنال‌های EEG، به‌عنوان داده‌های خصوصی شخصی که فعالیت‌های مغز را نشان می‌دهند، نگرانی‌هایی را در مورد حفاظت از داده‌ها ایجاد می‌کنند؛ همچنین مسائل حفظ حریم خصوصی مرتبط با سیگنال‌های EEG ساخت مجموعه‌داده‌های بزرگ EEG-BCI را با استفاده از مجموعه‌های کوچک‌تر برای آموزش مشترک مدل‌های یادگیری ماشین محدود می‌کنند[۴۴, ۴۵, ۴۷].

(شکل-۲): نمایی از یادگیری مشارکتی افقی یا یادگیری مشارکتی با بخش‌بندی نمونه، که ویژگی‌های هم‌پوشان از نمونه‌های داده از شرکت‌کنندگان گرفته‌شده و برای آموزش مشترک یک مدل به‌کار می‌روند[۴۱].

(Figure -2): llustration of HorizontalFederated Learning, a.k.a. sample-partitioned federated learning where the overlapping features from data samples held by different participants are taken to jointly train a model.



حاشیه‌نویسی داده‌ها به‌معنای افزودن برچسب‌ها یا توصیف‌های مرتبط به داده‌ها به‌منظور آموزش مدل‌های یادگیری ماشین است و فرایندی پرهزینه و زمان‌بر است. در یادگیری مشارکتی، که داده‌ها از منابع مختلف و توزیع‌شده جمع‌آوری می‌شوند، بی‌نیازبودن به حاشیه‌نویسی داده‌ها به مدل این امکان را می‌دهد که از داده‌های متنوع و توزیع‌شده در گره‌های مختلف بهره‌مند شود؛ همچنین حاشیه‌نویسی داده‌ها مقیاس‌بندی روش‌های یادگیری عمیق را در مقیاس‌های بزرگ محدود می‌کند. این ویژگی به مدل این امکان را می‌دهد که با استفاده از ویژگی‌های مشابه داده‌ها در فضای نمونه، از اطلاعات مفیدی برای بهبود یادگیری و طبقه‌بندی در حوزه‌هایی مانند الکتروانسفالوگرافی بهره‌مند شود؛ این ویژگی باعث افزایش دقت و عملکرد مدل‌های یادگیری ماشین در زمینه‌های پزشکی مانند تشخیص بیماری‌ها می‌شود[۴۵, ۴۶].

در زمینهٔ مراقبت‌های پزشکی، جمع‌آوری داده‌ها بخش بزرگی از هر پروژهٔ پژوهشی است و یادگیری مشارکتی می‌تواند برای بهبود مدل مشترک همان‌طورکه (شکل-۳) نشان می‌دهد، یک شبکهٔ مشارکتی برای بیمارستان‌های منطقه‌ای با اطلاعات پزشکی مشابه ایجاد کند که با تبادل اطلاعات مشابه و بهره‌مندی از تجربیات گسترده از منابع مختلف، دقت و قابلیت پیش‌بینی مدل‌ها را افزایش دهد که درنتیجه می‌توانند منجر به تشخیص دقیق‌تر بیماری‌ها، بهینه‌سازی تراکم بخش‌های درمانی، و ارتقای مداخلات پزشکی شوند.

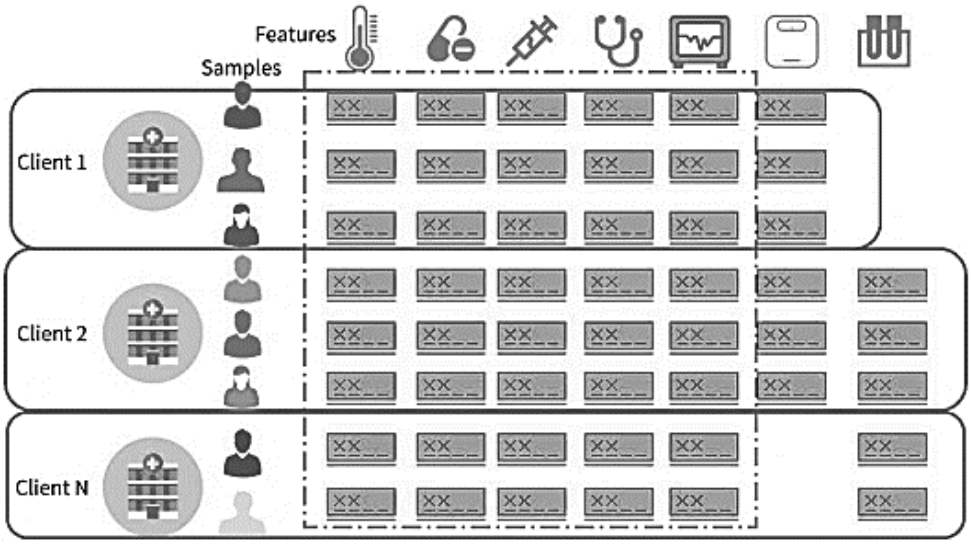
این امر بیانگر آن است که یادگیری مشارکتی می‌تواند به‌عنوان یک ابزار مؤثر در حوزهٔ سلامت جهت ارتقای

[1] horizontal federated learning
[2] Vertical Federated Learning
[3] Federated transfer learning (FTL)
[4] Partition
[5] Data annotation
[6] EEG
[7] Brain-Computer Interfaces (BCI)
[8] Electroencephalographic (EEG)

[DOI: 10.61186/jsdp.21.3.23]

سامانه‌های مراقبت‌های پزشکی و توسعهٔ مدل‌های پیشرفته در این زمینه، نقش بسیار حیاتی و مهمی را ایفا کند.

(شکل-۳): نمونه‌ای کاربردی از یادگیری مشارکتی افقی[۴]
(Figure -3): A practical example of horizontal federated learning

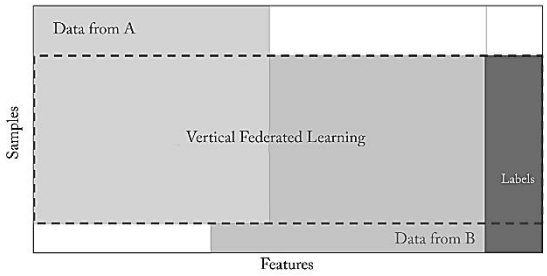


در شکل (۳) از یادگیری مشارکتی افقی برای حفظ حریم خصوصی داده‌های پزشکی بیماران استفاده شده‌است؛ در این رویکرد مشتری‌ها شامل چندین بیمارستان با داده‌های پزشکی مشابه و داده‌های محلی شامل سوابق پزشکی بیماران هر بیمارستان است. مدل محلی بر اساس داده‌های محلی هر بیمارستان آموزش داده می‌شود. سرور پارامترهای مدل را جمع‌آوری و به‌روزرسانی می‌کند مدل جهانی را بر اساس پارامترهای به‌روزرسانی‌شده آموزش می‌دهد.

۳-۲-۲-یادگیری مشارکتی عمودی

یادگیری مشارکتی عمودی یک رویکرد مؤثر در شرایطی است که داده‌ها به‌طور عمودی بر اساس بعد ویژگی تقسیم می‌شوند؛ به‌عبارت دیگر، در این روش داده‌ها بر اساس ویژگی‌های مختلف به دسته‌های مجزا تفکیک می‌شوند. در یادگیری مشارکتی عمودی، تمام طرفین دارای داده‌های همگنی هستند؛ به این معنا که در شناسهٔ نمونه‌ها هم‌پوشانی جزئی وجود دارد، اما از نظر فضای ویژگی، داده‌ها متفاوت و مستقل از یکدیگرند. این نوع یادگیری به‌ویژه برای موقعیت‌هایی که داده‌ها به‌طور طبیعی در دسته‌های مختلف ویژگی توزیع شده‌اند، مناسب است.
یک مثال کاربردی در حوزهٔ پزشکی، در یک مؤسسهٔ پژوهشی و درمانی که قصد دارد بیماری‌هایی مانند دیابت را از طریق پیش‌بینی شناسایی کند، می‌توان از یادگیری مشارکتی عمودی بهره برد.

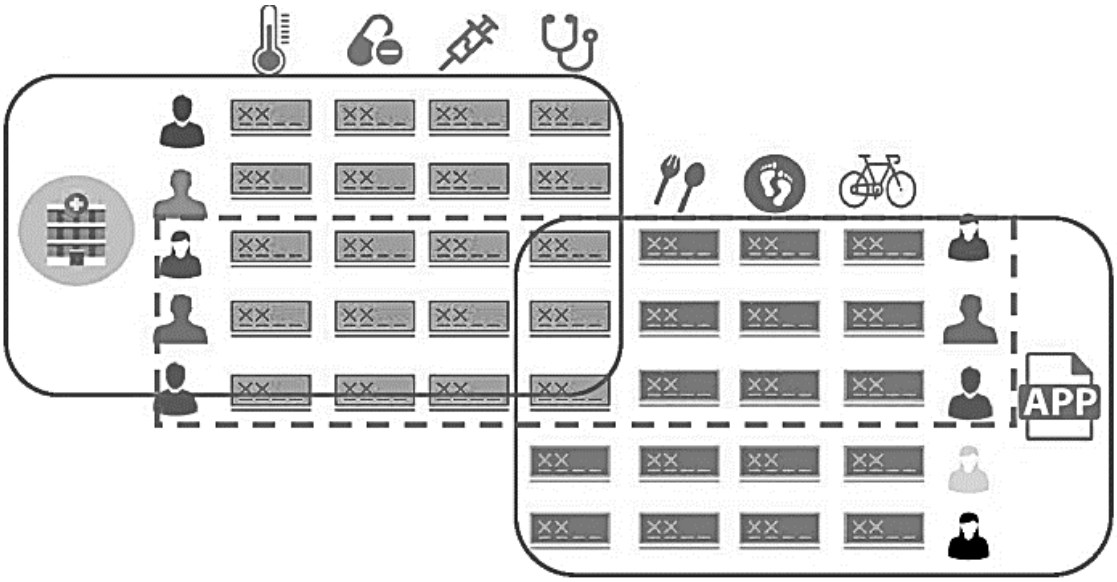
(شکل-۴): نمایی از یادگیری مشارکتی عمودی یا یادگیری مشارکتی با بخش‌بندی ویژگی، جایی‌که نمونه‌های دادهٔ هم‌پوشان با ویژگی‌های غیرهم‌پوشان از شرکت‌کنندگان گرفته‌شده‌است و برای آموزش مشترک یک مدل به‌کار می‌روند[۴۱].
Illustration of Vertical Federated Learning, (Figure -4): a.k.a feature-partitioned federated learning where the overlapping data samples that have non-overlapping or partially overlapping features held by multiple participants are taken to jointly train a model.



بر اساس پژوهش‌ها، افرادی‌که از فشارخون بالا و چاقی رنج می‌برند، مستعد ابتلا به دیابت نوع دو هستند[۴۸]؛ بنابراین، با توجه به اطلاعات مرتبط با سن، وزن و همچنین سابقهٔ پزشکی افراد می‌توان داده را تجزیه‌وتحلیل کرد؛ برای مثال ممکن است مرد جوانی که چاقی یا فشارخون ندارد، اما کالری بیشتری دریافت کرده‌است و فعالیت بدنی ندارد، مستعد ابتلا به دیابت باشد؛ بااین‌حال، به‌دلیل کمبود اطلاعات نمی‌توان آن را پیش‌بینی و شخصی‌سازی کرد؛ امروزه، از یادگیری مشارکتی می‌توان همراه با شرکت‌هایی که دارای مجموعه‌داده‌های برنامه‌های کاربردی تلفن‌های هوشمند مانند شمارندهٔ گام یا رژیم

غذایی هستند، برای بهبود عملکرد در زمینه‌های مختلف استفاده کرد.

همان‌طورکه در (شکل-۵) نشان داده‌شده‌است؛ این روش بدون نیاز به انتقال داده‌های خام، فرایند یادگیری را تکمیل می‌کند[۴۹]. فرایند یادگیری مشارکتی عمودی پیچیدگی‌های بیشتری نسبت به یادگیری مشارکتی افقی دارد. در یادگیری مشارکتی عمودی تجمیع تمام مجموعه‌داده‌ها در یک سرور مشترک برای آموزش یک مدل جهانی، امکان‌پذیر نیست؛ برای رفع این مشکل، الگوریتم‌های اصلاح‌شده‌ای مبتنی بر رمزنگاری برای پیش‌پردازش داده‌های تقسیم‌شده به‌طور عمودی توسعه یافته‌است[۵۰].



(شکل-۵): نمونه‌ای کاربردی از یادگیری مشارکتی عمودی[۴]
(Figure -5): A practical example of vertical federated learning

این الگوریتم‌ها موجب ایجاد فرایندهای بهینه‌تری برای جمع‌آوری و پردازش داده‌ها در یک محیط عمودی شده‌است و از امنیت بالاتری نیز برخوردارند؛ بر این اساس، پژوهش‌گران یک چارچوب امن به‌نام Secure Boost را برای تنظیم مجموعه‌داده‌های تقسیم‌شدهٔ عمودی طراحی کردند[۵۱]. بااین‌حال، این روش‌های امنیتی تاکنون تنها در مدل‌های سادهٔ یادگیری ماشین مانند رگرسیون ترابری به‌کار رفته‌اند؛ بنابراین، یادگیری مشارکتی عمودی هنوز نیاز به پیشرفت بیشتر دارد تا بتواند به‌طور مؤثر در رویکردهای پیچیده‌تر یادگیری ماشین مورد استفاده قرارگیرد.

شکل (۵) نمونه‌ای از کاربرد یادگیری مشارکتی عمودی را در حوزهٔ سلامت نشان می‌دهد؛ در این تصویر دو بیمارستان به‌عنوان مشتری در سیستم مشارکت دارند که هر کدام مجموعه‌داده‌های خود را با ویژگی‌های متفاوت در مورد بیماران خود دارند. برای مثال، بیمارستان A ممکن است اطلاعات دقیق‌تری در مورد جمعیت‌شناسی و سابقهٔ پزشکی بیماران داشته باشد، در حالی‌که بیمارستان B ممکن است داده‌های غنی‌تر در مورد نتایج آزمایشگاهی و نتایج درمان داشته باشد؛ در این رویکرد، در آموزش مدل بیمارستان‌ها داده‌های خام خود را به اشتراک نمی‌گذارند؛ بلکه مدل‌های محلی جداگانه را در مجموعه‌داده‌های مربوطهٔ خود آموزش می‌دهند. پس از آموزش، بیمارستان‌ها تنها وزن‌ها یا گرادیان‌ها را از مدل‌های محلی خود با سرور مرکزی به اشتراک می‌گذارند. سرور پارامترها را به‌گونه‌ای جمع‌آوری می‌کند که حفظ حریم خصوصی را تضمین کرده و در عین حال دانش جمعی هر دو بیمارستان را ثبت می‌کند. درنهایت، سرور مرکزی از پارامترهای جمع‌آوری‌شده برای به‌روزرسانی یک مدل جهانی استفاده می‌کند. این مدل جهانی از بینش‌های ترکیبی داده‌های هر دو بیمارستان بهره می‌برد، اگرچه خود داده‌های خام به اشتراک گذاشته نشده باشند.

این رویکرد به سازمان‌های فعال در حوزهٔ سلامت این امکان را می‌دهد تا از داده‌های متنوع بهره‌برداری بیشتری کنند که دقت و تعمیم‌پذیری مدل‌های خود را در

[DOI: 10.61186/jsdp.21.3.23]

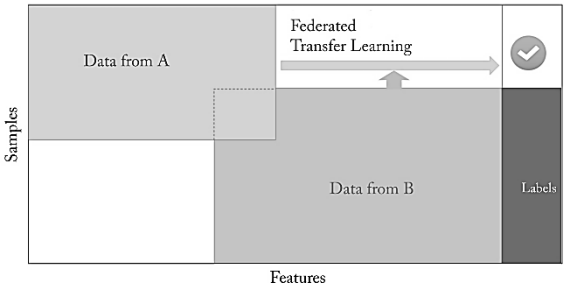
وظایفی نظیر تشخیص بیماری یا پیش‌بینی نتایج درمان افزایش دهند، در حالی‌که به‌طور مؤثر چالش‌های حفظ حریم خصوصی و مدیریت داده‌ها را با به اشتراک‌نگذاشتن اطلاعات حساس بیماران برطرف می‌کند.

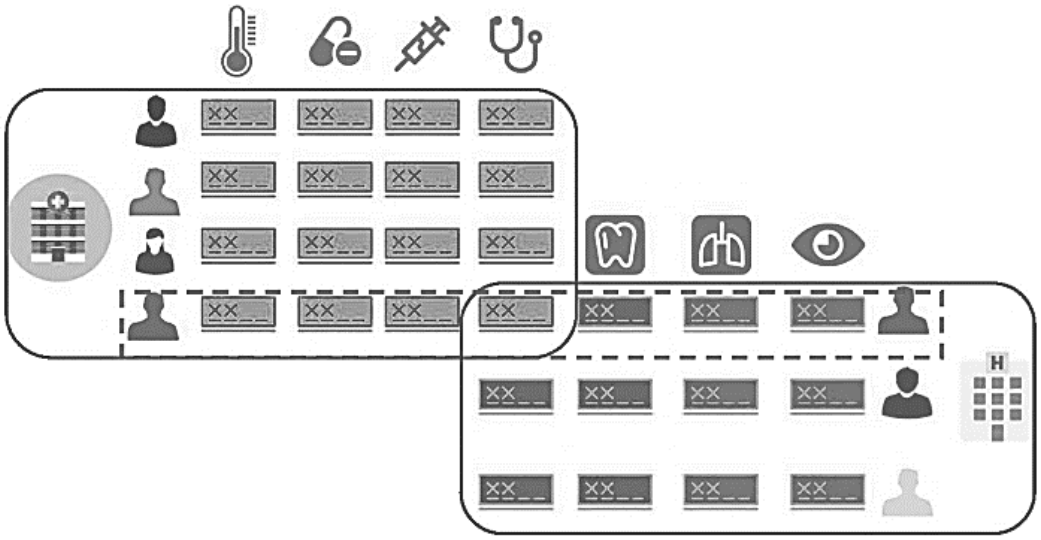
۳-۲-۳-یادگیری انتقال مشارکتی

برخلاف سناریوها در یادگیری مشارکتی افقی و یادگیری مشارکتی عمودی، در بسیاری از موارد، داده‌ها نه در فضای نمونه و نه در فضای ویژگی‌ها به اشتراک گذاشته می‌شوند؛ بنابراین، مشکل اصلی در این تنظیمات فقدان برچسب داده و کیفیت پایین داده‌هاست. یادگیری انتقال مشارکتی امکان انتقال دانش یک دامنه (دامنهٔ منبع) به یک دامنهٔ دیگر (دامنه هدف) را برای دستیابی به نتایج یادگیری بهتر فراهم می‌آورد، که به‌ویژه در شرایطی که داده‌ها در فضای نمونه یا ویژگی‌ها به اشتراک گذاشته نمی‌شوند، کاربردی است[۵۲]. به این ترتیب، پژوهش‌گران دریافتند که یادگیری انتقال مشارکتی می‌تواند به‌طور گسترده‌تری در یادگیری مشارکتی مورد استفاده قرارگیرد و به‌تعمیم یادگیری در این زمینه کمک کند[۵۳].

(شکل-۶): یادگیری انتقال مشارکتی (FTL). یک مدل پیش‌بینی که از نمایش ویژگی‌های نمونه‌های متعلق به طرف A و طرف B آموزش‌دیده و برای پیش‌بینی برچسب‌های نمونه‌های بدون برچسب طرف A استفاده می‌شود[۴۱].

(Figure -6): Federated transfer learning (FTL). A predictive model learned from feature representations of aligned samples belonging to party A and party B is utilized to predict labels for unlabeled samples of party A





(شکل-۷): نمونه‌ای کاربردی از یادگیری انتقال مشارکتی[۴]

(Figure- 7): A practical example of federated transfer learning

این رویکرد نخستین چارچوب جامع برای یادگیری مشارکتی مبتنی بر یادگیری انتقال، شامل آموزش، ارزیابی و اعتبارسنجی را ارائه می‌دهد؛ علاوه بر این، شبکه‌های عصبی که از فناوری رمزنگاری هوموروفیک افزایشی استفاده می‌کنند، قادرند از نشت حریم خصوصی جلوگیری کنند و دقتی قابل مقایسه با روش‌های سنتی بدون حفظ حریم خصوصی ارائه دهند؛ بااین‌حال، کارایی ارتباطات هنوز یک چالش باقی مانده‌است؛ به‌همین‌دلیل، پژوهش‌گران برای بهبود یادگیری انتقال مشارکتی از فناوری اشتراک مخفی به‌جای رمزگذاری هوموروفیک استفاده کردند تا سربار را کاهش دهند و بدون افت دقت، به عملکرد بهتری دست یابند[۵۴]. پژوهش‌گران همچنین برای کاربردهای عمومی یک مدل به‌نام Fed Health توسعه داده‌اند که از طریق یادگیری مشارکتی داده‌های متعلق به سازمان‌های مختلف را جمع‌آوری می‌کند و خدمات شخصی‌سازی‌شده برای مراقبت‌های بهداشتی و سلامت ارائه می‌دهد[۵۵، ۵۶]؛ همان‌طورکه در شکل (۷) نشان داده‌شده‌است، برخی از اطلاعات تشخیص و درمان بیماری در یک بیمارستان می‌تواند به بیمارستان دیگری منتقل شود تا به تشخیص بیماری‌ها از طریق یادگیری انتقال مشارکتی کمک کند؛ بااین‌حال، پژوهش‌ها در زمینهٔ یادگیری انتقال مشارکتی هنوز به بلوغ کامل نرسیده‌است

[DOI: 10.61186/jsdp.21.3.23]

و فضای زیادی برای رشدوبهبود وجود دارد تا این رویکرد با ساختارهای مختلف داده‌ها سازگارتر شود. مسائل مربوط به جزایر داده و حفاظت از حریم خصوصی از چالش‌های برجسته در صنعتی‌سازی گستردهٔ یادگیری ماشین هستند؛ در عین حال، یادگیری انتقال مشارکتی به‌عنوان یک روش مؤثر برای محافظت از امنیت‌داده‌ها و حریم خصوصی کاربران شناخته می‌شود و می‌تواند موانع جزایر داده را نیز کاهش دهد.

شکل (۷) نمونه‌ای از کاربرد یادگیری انتقال مشارکتی در حوزهٔ سلامت را نشان می‌دهد. در این زمینه، بیمارستان‌ها داده‌های سلامت از جمله تصاویر پزشکی و سوابق بیماران را به اشتراک می‌گذارند. هر بیمارستان مدل یادگیری ماشین خود را بر روی داده‌های محلی آموزش می‌دهد و سپس پارامترهای این مدل‌های آموزش‌دیده را به اشتراک می‌گذارد. این پارامترها برای آموزش یک مدل هم‌تراز جهانی[1] مورد استفاده قرار می‌گیرند.

این مدل، دانش عمومی استخراج‌شده از تمام داده‌های محلی را در خود جای می‌دهد و سپس هر بیمارستان با تنظیم دقیق[2] مدل هم‌تراز جهانی را بر روی داده‌های محلی خود تطبیق داده و آن را بهینه‌سازی می‌کند؛ این فرایند در زمینه‌های مختلف سلامت، از جمله تشخیص بیماری، پیش‌بینی نتایج درمان و تجزیه و تحلیل داده‌های پزشکی به‌کار گرفته می‌شود.

این رویکرد علاوه بر حفظ حریم خصوصی داده‌ها، امکان آموزش مدل‌ها را سریع‌تر و مقرون‌به‌صرفه‌تر نسبت به آموزش در یک سرور مرکزی فراهم می‌آورد و در کل می‌تواند به بهبود دقت پروژه‌های حوزهٔ سلامت از طریق بهره‌برداری از دانش عمومی استخراج‌شده از مجموعه‌داده‌های متنوع کمک کند[۴۴].

۴-روش پژوهش مقاله

۴-۱-انتخاب منابع

انتخاب مقالات مرتبط و با کیفیت، گامی اساسی در هر پژوهش است که به دقت و روش‌شناسی نیاز دارد. در این مطالعه، فرایند انتخاب مقالات به‌طور نظام‌مند و در دو مرحلهٔ مجزا با استفاده از معیارهای دقیق و تحت‌نظر متخصصان انجام شد. این فرایند مطابق با دستورالعمل استاندارد Kitchenham [۵۷] و به‌عنوان بخشی از یک بررسی ادبیات نظام‌مند پیاده‌سازی شد تا نمای کاملی از فعالیت‌های پژوهشی و موضوعات مختلف در زمینهٔ توسعهٔ یادگیری مشارکتی ارائه دهد.

در این مقاله، به جست‌وجوی جامع مقالات مروری مرتبط با موضوع در پایگاه‌های داده‌های علمی معتبر شامل IEEE Xplorer، ACM Digital Library، ScienceDirect، Springer Link، ArXiv، Google Scholar در بازه زمانی ۲۰۱۹ الی ۲۰۲۳ پرداخته شده‌است. مقالات پس از جست‌وجوی اولیه با توجه به معیارهای ورود و خروج از پیش تعیین‌شده، مانند تناسب با موضوع، نوع مطالعه، روش‌شناسی و کیفیت نگارش انتخاب می‌شوند.

روند انتخاب مقالات در این پژوهش شامل دو مرحله است: در مرحلهٔ نخست مقالات توسط دو پژوهش‌گر از طریق ارزیابی عنوان، چکیده و کلیدواژه‌ها به‌طور مستقل و بر اساس معیارهای ورود و خروج از پایگاه‌های علمی معتبر انتخاب شدند. در مرحلهٔ دوم مقالات انتخاب‌شدهٔ مرحلهٔ نخست از طریق غربال‌گری متن کامل بررسی شدند. در این مرحله، محتوا، روش‌شناسی و یافته‌های مقالات مورد ارزیابی دقیق قرارگرفت. نتایج این ارزیابی توسط هر دو پژوهش‌گر مجدداً مورد بررسی و تأیید قرارگرفت. همچنین در صورت بروز اختلاف‌نظر بین پژوهش‌گران در هر دو مرحله، با یک پژوهش‌گر سوم به‌عنوان داور مشورت شد و تصمیم نهایی بر اساس نظر جمع پژوهش‌گران اتخاذ شد؛ در نهایت پس از انتخاب نهایی مقالات، داده‌های مربوط به موضوعات پژوهش، روش‌شناسی، یافته‌ها و چالش‌ها از مقالات برگزیده استخراج و تجزیه و تحلیل شده‌اند.

۴-۱-۱-منابع برگزیدهٔ پژوهش

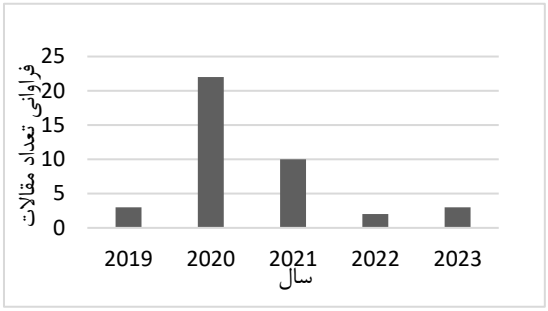
پس از طی مراحل توضیح داده‌شده در بخش انتخاب منابع، که شامل جست‌وجوی جامع در پایگاه‌های علمی معتبر، غربال‌گری اولیهٔ مقالات و انتخاب نهایی بر اساس معیارهای از پیش تعریف‌شده بود؛ درنهایت ترکیب جامعی از ۳۸ مقاله و دو کتاب به‌عنوان منابع نهایی مورد بررسی قرارگرفت. اطلاعات مربوط به منابع بررسی‌شده در این پژوهش در جدول (۲) (در بخش پیوست) ارائه شده‌است؛ این جدول کامل و دقیق به معرفی هر منبع و مشخصات آن می‌پردازد. اطلاعات ارائه‌شده در این جدول شامل عنوان کامل هر منبع، نویسندگان، سال انتشار منبع، خلاصه‌ای از موضوع و محتوای اصلی، زمینهٔ پژوهش و حوزه‌ای که منبع در آن به بررسی موضوع می‌پردازد، است.

[1] Global Model
[2] Fine-Tuning

[DOI: 10.61186/jsdp.21.3.23]

۲-۱-۴-دسته‌بندی منابع

بر اساس جدول (۲) مشاهده می‌شود از میان منابع نهایی، سه منبع در سال ۲۰۱۹، ۲۲ منبع در سال ۲۰۲۰ و ده منبع در سال ۲۰۲۱، دو منبع در سال ۲۰۲۲ و سه منبع در سال ۲۰۲۳ منتشر شده‌است. در (**شکل**شکل (۸) به توزیع فراوانی کتب و مقالات منتشرشده در هر سال پرداخته شده‌است. بررسی توزیع زمانی منابع، گویای رشد و توجه فزاینده به مفهوم یادگیری مشارکتی در سال‌های اخیر است. شواهد حاکی از آن است که یادگیری مشارکتی به‌عنوان یک حوزهٔ پژوهشی و کاربردی در حال رشد و توسعه است.



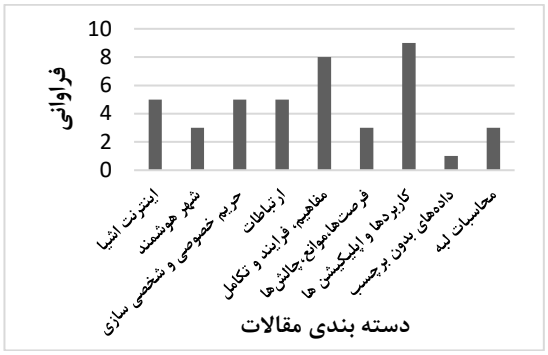
(شکل-۸): تعداد کتب و مقالات منتشرشده در هر سال
(Figure -8): Number of books and articles published in each year

بررسی موضوعی مقالات و کتب نشان می‌دهد که پنج پژوهش به کاربردهای یادگیری مشارکتی در اینترنت اشیا پرداخته‌اند. سه پژوهش به کاربرد آن در شهر هوشمند، پنج پژوهش به بحث کاربردهای آن در حفظ حریم خصوصی و شخصی‌سازی داده‌ها، پنج پژوهش به بررسی این مفهوم در زمینهٔ ارتباطات، هشت پژوهش به بررسی مفاهیم، فرایندها و تکامل یادگیری مشارکتی، سه پژوهش به فرصت‌ها و موانع و چالش‌های این حوزه، نُه پژوهش به کاربردهای آن در زمینه‌های مختلف از جمله سلامت، پهپادها و وسایل نقلیه و یک مطالعه نیز به بررسی داده‌های بدون برچسب در این روش یادگیری و سه مطالعه به محاسبات لبه به‌صورت کلی و در شبکه‌های موبایل پرداختند. شکل (۹) به بررسی عناوین مورد پژوهش در مقالات می‌پردازد. در ادامه به تشریح هر یک از موارد بالا پرداخته می‌شود.

۲-۴-مفاهیم مستخرج از منابع

۱-۲-۴-کاربرد یادگیری مشارکتی

تحلیل موضوعی مقالات و کتب حاضر نشان می‌دهد که ۲۳ پژوهش به کاربرد در زمینه‌های مختلف پرداخته‌اند که از این بین پنج مطالعه به مبحث کاربردهای یادگیری مشارکتی در اینترنت اشیا، سه مطالعه در شهر هوشمند، پنج مطالعه در حفظ حریم خصوصی، یک مطالعه شخصی‌سازی داده‌ها، چهار مطالعه به مراقبت‌های بهداشتی، یک مطالعه در زمینهٔ پهپادها، چهار مطالعه به کاربرد یادگیری مشارکتی در دستگاه‌های تلفن همراه پرداخته‌است؛ در ادامه هر یک از این زمینه‌ها بررسی و جزئیات بیشتر در مورد هر مطالعه ارائه می‌شود.



(شکل-۹): بررسی عناوین مورد پژوهش در مقالات
(Figure -9): Review of research topics in articles

شکل (۹) به بررسی عناوین مورد پژوهش در مقالات می‌پردازد. در ادامه به تشریح هر یک از موارد بالا پرداخته می‌شود.

۲-۴-مفاهیم مستخرج از منابع

۱-۲-۴-کاربرد یادگیری مشارکتی

تحلیل موضوعی مقالات و کتب حاضر نشان می‌دهد که ۲۳ پژوهش به کاربرد در زمینه‌های مختلف پرداخته‌اند که از این بین پنج مطالعه به مبحث کاربردهای یادگیری مشارکتی در اینترنت اشیا، سه مطالعه در شهر هوشمند، پنج مطالعه در حفظ حریم خصوصی، یک مطالعه شخصی‌سازی داده‌ها، چهار مطالعه به مراقبت‌های بهداشتی، یک مطالعه در زمینهٔ پهپادها، چهار مطالعه به کاربرد یادگیری مشارکتی در دستگاه‌های تلفن همراه پرداخته‌است؛ در ادامه هر یک از این زمینه‌ها بررسی و جزئیات بیشتر در مورد هر مطالعه ارائه می‌شود.

۱-۱-۲-۴-کاربرد یادگیری مشارکتی در اینترنت اشیا و شهر هوشمند

اینترنت اشیا با گسترش خدمات و برنامه‌های هوشمند مبتنی بر هوش مصنوعی[1] در بسیاری از جنبه‌های زندگی روزمرهٔ ما نفوذ می‌کند. به‌طورسنتی، روش‌های هوش مصنوعی به جمع‌آوری و پردازش متمرکز داده‌ها احتیاج دارند که به‌دلیل مقیاس‌پذیری بالای شبکه‌های اینترنت اشیا مدرن و

[1] AI

[DOI: 10.61186/jsdp.21.3.23]

نگرانی‌های روبه‌رشد حریم خصوصی داده‌ها، ممکن است در سناریوهای برنامه‌های واقع‌بینانه عملی نباشد.

با افزایش بی‌سابقهٔ تعداد دستگاه‌های اینترنت اشیا[1] و برنامه‌های در حال ظهور، هر روز میزان زیادی ترافیک ایجاد می‌شود که بار زیادی را بر شبکهٔ اینترنت وارد می‌کند. این مسئله سرمایه‌گذاری‌های قابل توجهی را برای ارتقا زیرساخت‌ها می‌طلبد؛ بااین‌حال، به لطف توسعهٔ تجزیه‌وتحلیل داده‌های بزرگ و روش‌های هوش مصنوعی مانند یادگیری عمیق[2] و یادگیری ماشین[3]، داده‌های جمع‌آوری‌شده می‌توانند برای اهداف مختلف مورد بهره‌برداری مؤثر قرار گیرند.

در زمینهٔ ارتباطات، چند سال گذشته شاهد ظهور کاربردهای هوش مصنوعی در زمینه‌های مختلف بوده‌ایم. برای مثال، یادگیری ماشین برای بررسی انتخاب کارآمد آنتن در سیستم‌های بی‌سیم چندآنتن استفاده شده‌است[۹۱].

یادگیری عمیق به‌طور مؤثر برای مدیریت مشکلات بارگذاری محاسبات در سیستم‌های اینترنت اشیا از طریق محاسبات لبه جهت بهینه‌سازی [۹۲] به‌کار گرفته می‌شود؛ همچنین، یادگیری تقویتی عمیق در حل چالش‌های تخصیص منابع در شبکه‌های لبه، شامل طبقه‌بندی ترافیک، ذخیره‌سازی داده در لبه، امنیت شبکه و مدیریت بارگذاری داده‌ها [۹۳] نقشی کلیدی ایفا می‌کند.؛ بااین‌وجود، مدل‌های معمولی هوش مصنوعی به‌طورمعمول به پردازش مرکزی داده‌های جمع‌آوری‌شده از تمام کاربران شبکه نیاز دارند، در این روش‌ها کاربران باید داده‌های خود را برای آموزش مدل یادگیری در یک سرور مرکزی بارگذاری کنند و نگرانی اساسی در مورد حفظ حریم خصوصی داده‌ها وجود دارد؛ برای مثال، برخی از کاربران نمی‌خواهند داده‌های محلی خود را به سرور مرکزی منتقل کنند.

آموزش مدل یادگیری به‌طور متمرکز به یک ابر مرکزی با قابلیت‌های محاسباتی و ظرفیت ذخیره‌سازی بسیار قدرتمند نیاز دارد. در همین حال، پیشرفت‌های اخیر در زمینهٔ سخت‌افزار محاسبات و گسترش دستگاه‌های هوشمند در زندگی روزمرهٔ ما نشان داده‌است که هر دستگاه اینترنت اشیا می‌تواند به سطح محاسبات و ذخیره‌سازی معقولی مجهز باشد، که از نظر مقایسه با رایانه رومیزی ده سال پیش قابل مقایسه است[۹۴]؛ بنابراین، مدل استاندارد یادگیری ماشین به‌راحتی در شبکه‌های اینترنت اشیا در مقیاس بزرگ قابل استفاده نیست. این مدل‌های یادگیری ماشین نمی‌تواند از در دسترس‌بودن محاسبات توزیع‌شده بهره‌برداری کند. این امر یک مدل یادگیری جدید را می‌طلبد که به‌جای متمرکزکردن، داده‌های آموزشی را در دستگاه‌های اینترنت اشیا به‌صورت منحصربه‌فرد و جداگانه توزیع کند.

با انگیزهٔ رفع این مسئله، همان‌طورکه پیش‌تر اشاره شد، گوگل مفهوم یادگیری مشارکتی را برای یادگیری روی دستگاه و حفظ حریم خصوصی داده‌ها ابداع کرد[۲۱]. یادگیری مشارکتی به‌مثابه یک رویکرد هوش مصنوعی مشترک توزیع‌شده پدیدار شده‌است که می‌تواند بسیاری از برنامه‌های اینترنت اشیا هوشمند را با امکان آموزش هوش مصنوعی در دستگاه‌های اینترنت اشیا توزیع‌شده بدون نیاز به اشتراک داده‌ها قادر سازد.

با استفاده از روش یادگیری مشارکتی، هر دستگاه اینترنت اشیا می‌تواند مدل خود را بر اساس داده‌های جمع‌آوری‌شدهٔ محلی آموزش دهد. داده‌های محلی دستگاه‌های اینترنت اشیا نیازی به انتقال به فضای ابری متمرکز ندارند. فضای ابری متمرکز فقط باید مدل آموزش محلی به‌روزشده را از کاربران جمع‌آوری کند. یادگیری مشارکتی به‌سبب ویژگی‌هایی که دارد در بسیاری از برنامه‌ها پذیرفته شده‌است؛ برای مثال، یادگیری مشارکتی برای بهبود پیشنهادهای صفحه‌کلید گوگل [۹۵]، مراقبت‌های بهداشتی‌وسلامت [۸۴]، سنجش شهر هوشمند و در زمینهٔ دارو [۹۶] کاربردهای متعددی دارد.

شکل (۱۰) نمای کلی یادگیری مشارکتی در سامانه‌های اینترنت اشیا را نشان می‌دهد، که به چهار بخش اصلی دستگاه‌های لبه، سرور، مدل‌های محلی و مدل جهانی تقسیم می‌شود.

دستگاه‌های لبه شامل انواع مختلف حس‌گرها، محرک‌ها و سایر دستگاه‌های IoT که داده‌ها را از محیط جمع‌آوری و مدل‌های یادگیری ماشین محلی را بر روی داده‌های محلی آموزش می‌دهند و پارامترهای مدل‌های محلی را به سرور ارسال می‌کنند. سرور مسئول هماهنگی فرایند و آموزش مدل‌ها از دستگاه‌های لبه و جهانی است. مدل‌های محلی بر روی هر دستگاه لبه اجرا می‌شوند و با به‌روزرسانی‌های ارسالی از سرور به‌روز می‌شوند. مدل جهانی بر روی سرور اجرا می‌شود و دانش عمومی از

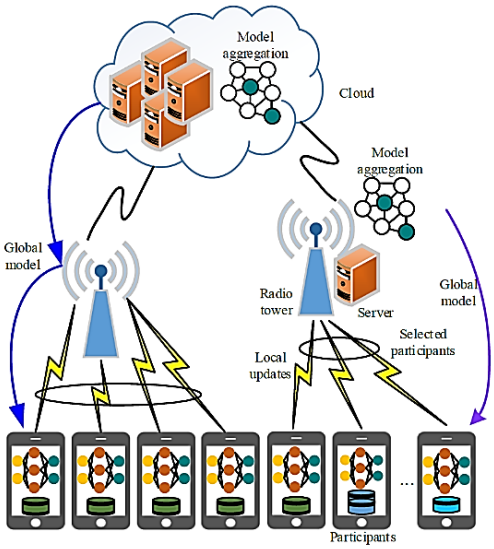
[1] IoT
[2] DL
[3] ML

[DOI: 10.61186/jsdp.21.3.23]

دستگاه‌های لبه را در خود جای‌داده و با استفاده از پارامترهای جمع‌آوری‌شده آموزش داده می‌شوند.

این سامانه از حفظ حریم خصوصی، کارایی بالا در آموزش مدل‌ها به‌صورت محلی و افزایش دقت وظایف مختلف به‌وسیلهٔ مدل‌های جهانی بهره‌مند است.

درکل، هر دستگاه اینترنت اشیا مجموعه‌داده‌های خاص خود را دارد و در سیستم رایانش ابری از راه‌دور، سرور تجمیع را می‌توان در لبهٔ شبکه یا یک ابر مجازی قرارداد[۸۱]. هر مدل یادگیری مشارکتی بسته به عوامل مختلف، مزایا و معایب خاص خود را دارد؛ برای مثال، یادگیری مشارکتی با سرور در لبهٔ شبکه برای برنامه‌هایی که به تأخیر کم، آگاهی از موقعیت مکانی و اطلاعات زمینهٔ شبکه نیاز دارند، مناسب است[۹۴]، در حالی‌که یادگیری مشارکتی مبتنی برفضای ابر، برای برنامه‌هایی با دستگاه‌های گستردهٔ اینترنت اشیا در مناطق مختلف و نیازهای آن‌ها مناسب است.



(شکل-۱۰): نمای کلی FL در سامانه‌های اینترنت اشیا [۴۲]

(Figure 10): Overview of FL in IoT systems

۲-۱-۲-۴-یادگیری مشارکتی برای امنیت در اینترنت اشیا صنعتی IIOT[1]

یادگیری مشارکتی با آموزش مدل بدون نیاز به انتقال داده‌ها از مشتری به سرور اصلی، حفاظت مؤثری از داده‌های کاربر فراهم می‌آورد. دامنهٔ سازوکارهای امنیتی می‌تواند با به اشتراک‌گذاری به‌روزرسانی‌های مدل و تلفیق داده‌های تولیدشده از دستگاه‌های مشابه در صنایع مختلف، به‌طور قابل توجهی تقویت شود؛ در ادامه، پس از بررسی مقالات مرجع دربارهٔ سازوکارهای امنیتی مختلف و ادغام یادگیری مشارکتی با مدل‌های یادگیری ماشین و یادگیری عمیق، به کاربردهای این روش‌ها در چارچوب اینترنت اشیا صنعتی خواهیم پرداخت.

۳-۱-۲-۴-یادگیری ماشین مشارکتی برای ایمن‌سازی IIoT

با توجه به حجم داده‌های تولیدشده در صنعت، استفاده از روش‌های یادگیری ماشین مناسب نخواهد بود[۹۷]. در کل بسیاری از صنایع دارای سامانه‌های نظارتی اینترنت اشیا مشابه‌اند[۹۸]؛ بنابراین، داده‌های تولیدشده را می‌توان از طریق تمام دستگاه‌هایی که منجر به افزایش دقت الگوریتم‌های یادگیری ماشین می‌شود در قالب یادگیری مشارکتی آورد.

بااین‌حال، نگرانی اصلی مربوط به امنیت‌داده‌هاست که در هنگام استفاده از آن‌ها به‌وجود می‌آید[۹۹]. یادگیری ماشین مشارکتی[2] به‌دلیل رویکرد عدم‌تمرکز داده‌های تولیدشده در دستگاه کاربر نهایی و تجمیع مدل‌های یادگیری ماشین در یک سرور متمرکز، توجه زیادی را به‌خود جلب کرده‌است. دو نوع حمله در اینترنت اشیا صنعتی یعنی شنوندگان شنود و هکرها مورد بحث قرارگرفته‌است[۱۰۰].

۱)شنود: حمله هنگامی اتفاق می‌افتد که داده‌ها از طریق کانال‌های ارتباطی منتقل شوند؛ در این حالت، ممکن است بین گره IoT و سینک یا مخزن IoT[3] اتفاق بیفتد، سپس از مخزن IoT به کانال‌های ارتباطی سرور متمرکز انتقال یابد.

۲)هکرها: حمله‌ای که در سرور متمرکز اتفاق می‌افتد؛ یک تعقیب‌کننده[4] در سرور قرار دارد و قادر است موقعیت‌های واقعی کاربر را به‌دست آورد.

در ابتدا داده‌ها از دستگاه‌های اینترنت اشیا از هر صنعت هوشمندی در این زمینه تولید می‌شوند. سینک مخزنی برای جمع‌آوری داده‌ها از گره‌های مختلف اینترنت اشیا در صنعت از طریق ارتباطات سیمی و بی‌سیم است که داده‌هایی را که به سرور متمرکز ارسال می‌شود، رمزگذاری می‌کند؛ سپس سرور اطلاعات چندین مخزن اینترنت اشیا را جمع‌آوری و داده‌ها را مشارکتی می‌کند؛ سرانجام، صنعت هوشمند دانش را به یک قالب قابل درک رمزگشایی می‌کند. در این شرایط، احتمال موفقیت هر دو نوع حمله از جمله شنود و نفوذ هکرها به‌طور چشمگیری کاهش می‌یابد؛ زیرا داده‌های رمزگذاری‌شده در هر دو مورد وجود دارد.

[1] Industrial Internet of Things (IIoT)

[2] Federated ML (FML)
[3] IoT sink
[4] stalker

هدف اصلی یادگیری مشارکتی این است که به‌طور جمعی مدل جهانی را بدون به‌خطرانداختن حریم خصوصی داده‌ها فراگیرد، اما به اشتراک‌گذاشتن به‌روزرسانی‌های مدل در سرور در طی مراحل آموزش، ممکن است به مسئلهٔ نشت داده‌های حساس مانند اطلاعات شخصی کاربر منجر شود؛ به‌منظور حفظ حریم خصوصی در مدل‌های یادگیری ماشین، از روش‌هایی در یادگیری مشارکتی استفاده می‌شود که در ادامه به آن پرداخته می‌شود:

- حفظ حریم خصوصی تفاضلی یا افتراقی[1]: حریم خصوصی تفاضلی مقدار اطلاعات مربوط به داده‌هایی را که می‌تواند برای تجزیه‌وتحلیل شخص ثالث در دسترس باشد، تعریف می‌کند[۱۰۱]. اطلاعات تحت حریم خصوصی تفاضلی را می‌توان به‌عنوان اطلاعات کلی دسته‌بندی کرد که دارای اطلاعات مربوط به کل جمعیت است و نوع دیگر اطلاعات خصوصی شخصی است. برخی از ویژگی‌های چارچوب حریم خصوصی تفاضلی برای ارائهٔ اطلاعات شخصی حساس و محافظت از حریم خصوصی شامل کمی‌سازی ازبین‌رفتن حریم خصوصی، ترکیب، حفظ حریم خصوصی گروه و بسته‌شدن آن پس از پردازش است.
- رمزنگاری هوموورفیک: محاسبه و تجزیه‌وتحلیل بر اساس تکنیک رمزگذاری انجام می‌شود تا مهاجم برای یافتن اطلاعات اصلی بسیار دشوار باشد[۱۰۲].
- محاسبهٔ امن چندجانبه: این مدلی است که در آن چندین طرف به‌صورت مشترک و بدون درج اطلاعات به اشخاص ثالث محاسبه می‌کنند[۱۰۳]. به‌اختصار، حریم خصوصی تفاضلی داده‌های کامل را تضمین نمی‌کند؛ زیرا اگر الگوریتم اطلاعات خصوصی را به اشتباه اطلاعات عمومی طبقه‌بندی کند، الگوریتم نمی‌تواند از داده‌ها محافظت کند. علی‌رغم تمام این اشکالات، ثابت شده که حریم خصوصی تفاضلی در مقایسه با روش متمرکز سنتی، رویکرد حفظ حریم خصوصی کارآمدتری است[۱۰۱].

۴-۱-۲-۴-یادگیری عمیق مشارکتی در اینترنت اشیا صنعتی

در سال‌های اخیر، ادغام مدل‌های یادگیری عمیق با اینترنت اشیا و محاسبات دستگاه‌های لبه[2] به‌دلیل توانایی ارائهٔ تحلیل‌های بلادرنگ با منابع محدود، محبوبیت فزاینده‌ای پیدا کرده‌است[۱۰۴]؛ در این راستا، یادگیری عمیق مشارکتی[3] شرکت‌های صنعتی را قادر می‌سازد تا مدل‌های یادگیری عمیق را به‌طور ایمن در دستگاه‌های اینترنت اشیا ادغام کنند. این رویکرد، چارچوبی امن و غیرمتمرکز را برای آموزش مدل‌های یادگیری عمیق فراهم می‌آورد و به‌ویژه در زمینه‌هایی که نیاز به پردازش و تحلیل داده‌های توزیع‌شده و بلادرنگ وجود دارد، ارزشمند است؛ به همین دلیل، مسئلهٔ عدم‌تمرکز در مدل‌های یادگیری عمیق به یک چالش چندبعدی تبدیل شده که نیازمند توسعه و پیاده‌سازی چارچوب‌های فناوری نوین برای ادغام موفق یادگیری عمیق با محاسبات لبه‌ای و اینترنت اشیای صنعتی است.

هدف اصلی یادگیری عمیق مشارکتی در حوزهٔ اینترنت اشیای صنعتی (IIoT)، ارتقای قابلیت‌های این فناوری از طریق بهینه‌سازی مدل‌های یادگیری عمیق است که قادر به تحول کارخانه‌ها به کارخانه‌های هوشمند است. این رویکرد به‌ویژه بهبود کارایی و بهره‌وری سیستم‌ها را هدف قرار می‌دهد. در ادامه، به بررسی برخی از پارامترهای ضروری برای ساخت مدل یادگیری مشارکتی عمیق در اینترنت اشیا صنعتی پرداخته می‌شود.

۴-۱-۲-۴-۱-مدل یادگیری مشارکتی عمیق FDL

مدل یادگیری مشارکتی عمیق را می‌توان از دو طرف سرویس‌گیرنده یا مشتری و سرور پیاده‌سازی کرد. در سمت مشتری، شبکه‌های خصوصی تعریف می‌شوند که مدل یادگیری عمیق را با استفاده از مدل کلی موجود در فضای ابری تنظیم و بهینه‌سازی می‌کنند؛ سپس مدل‌های بهینه و تنظیم‌شده در سمت مشتری مستقر می‌شوند و با استفاده از داده‌های محلی تولیدشده به‌وسیلهٔ دستگاه‌ها آموزش داده می‌شوند؛ سرانجام دستگاه پایانی شامل مدل یادگیری مشارکتی عمیق بسیار کمی و فشرده است. در سمت سرور، مدل موجود در فضای ابری با ادغام شیب‌های به‌روزرسانی‌شده از هر سرویس‌گیرنده به‌طورمداوم به‌روزرسانی می‌شود.

روش نزولی شیب تصادفی انتخابی توزیع‌شده که در [۲۰] ارائه شده‌است، می‌تواند در مدل ابری برای به‌روزرسانی مکرر مدل خصوصی محلی مورد استفاده قرارگیرد. نخستین مدل غیرمتمرکز با نام "ModelChain" با استفاده از فناوری بلاک‌چین [۱۰۵ , ۱۰۶] طراحی شده‌است تا حریم خصوصی در انتقال داده‌ها را تضمین کند؛ علاوه‌براین، هنگامی‌که یک مدل

[1] Differential Privacy (DP)
[2] edge
[3] FDL

[DOI: 10.61186/jsdp.21.3.23]

واحد به‌طور موازی میان تمامی دستگاه‌ها آموزش داده‌شده و جمع‌آوری و پردازش می‌شود، می‌توان از روش نزول شیب تصادفی ناهم‌زمان استفاده کرد.

۲-۴-۱-۲-۴-ارتباط و شبکهٔ یادگیری مشارکتی عمیق FDL

مزیت اصلی استفاده از یادگیری مشارکتی عمیق در اجرای مدل‌های یادگیری عمیق بر روی دستگاه‌های اینترنت اشیا و درگیرکردن این مدل‌ها در فرایند تصمیم‌گیری نهفته است. این رویکرد، با تمرکززدایی از فرایند یادگیری عمیق، موجب افزایش کارایی عملیاتی و قابلیت اطمینان دستگاه‌های اینترنت اشیا می‌شود.

(جدول-۲): تفاوت بین FDL و FML

(Table 3): Difference between FDL and FML

ویژگی	FDL	FML
ارتباطات	ارتباط مستقیم بین ابر و اینترنت اشیا امکان‌پذیر است.	ارتباط مستقیم بین ابر و اینترنت اشیا امکان‌پذیر نیست.
حریم خصوصی	دلیل تبادل مستقیم اطلاعات بین دستگاه‌ها و ابر، حریم خصوصی کمتر از FML است.	حریم خصوصی بیشتر است.
ذخیرهٔ اطلاعات	مدل عمیق خصوصی در فضای ابری حفظ می‌شود	هیچ داده‌ای در فضای ابری ذخیره نمی‌شود.
به‌روزرسانی‌ها	به‌روزرسانی‌های گرادیان[1] مدل به فضای ابری ارسال می‌شوند.	به‌روزرسانی‌های آمارهای مربوط به داده‌های محلی به ابر ارسال می‌شوند.
دستگاه‌های متصل به ابر	دستگاه‌های اینترنت اشیا مستقیماً با ابر ارتباط دارند.	دستگاه‌های لبه به‌عنوان یک واسط بین دستگاه‌های اینترنت اشیا و ابر عمل می‌کنند
دسترسی به مدل	دسترسی به مدل خصوصی و فقط برای ابر و دستگاه‌های مجاز امکان‌پذیر است.	مدل به‌طور عمومی در دسترس تمام دستگاه‌ها و ابر قراردارد.
کنترل داده‌ها	کنترل داده‌ها به‌صورت متمرکز در ابر انجام می‌شود	کنترل داده‌ها به‌صورت غیرمتمرکز در دستگاه‌ها انجام می‌شود.
بهینه‌سازی	به دلیل پیچیدگی مدل‌های عمیق، به بهینه‌سازی دقیق نیاز دارد	به‌دلیل سادگی مدل‌ها، در کل به بهینه‌سازی کمتری نیاز دارد.

یادگیری مشارکتی عمیق دو نوع ارتباط را ارائه می‌دهد: کانال درون سیستمی و کانال بین‌سیستمی [۵۹]. در یادگیری مشارکتی عمیق، مدل بهینه‌سازی‌شده در فضای ابری روی دستگاه‌های لبه مستقر می‌شود و ارتباط بین دستگاه‌های اینترنت اشیا و فضای ابری برقرار می‌شود؛ بااین‌حال، حفظ امنیت و حریم خصوصی در جریان این ارتباطات ضروری است. در کانال بین‌ارتباطی، اجزای موجود در هر لایه به سه روش مختلف مانند ابر، لبه و دستگاه انتهایی با یکدیگر ارتباط برقرار می‌کنند. هدف اصلی یادگیری مشارکتی عمیق به‌حداقل‌رساندن ارتباطات درون سیستمی و به‌بیشینه‌رساندن ارتباطات بین‌سیستمی است. این مهم در پیشبرد اهداف مختلف شامل بهینه‌سازی عملکرد، افزایش کارایی و کاهش هزینه‌های ارتباطات نقش مهمی ایفا می‌کند.

۳-۴-۱-۲-۴-حریم خصوصی و امنیت یادگیری مشارکتی عمیق

در پژوهش [۶۴] به بررسی تهدیدات امنیتی مختلفی پرداخته شده‌است که در هنگام به اشتراک‌گذاری مدل‌های یادگیری عمیق از دستگاه‌های ابری به دستگاه‌های انتهایی و برعکس بروز می‌کند. یادگیری مشارکتی عمیق مدل‌های یادگیری عمیق را به‌گونه‌ای طراحی می‌کند که اطلاعات مربوط به داده‌ها را در فضای ابری نشان نمی‌دهد.

مسائل امنیتی در سمت سرور شامل چالش‌هایی است که ناشی از به اشتراک‌گذاری مدل‌های یادگیری عمیق در فضای ابری هستند؛ این مسائل می‌توانند به خطرات مربوط به محرمانگی داده‌ها و افزایش ریسک‌های امنیتی منجر شوند.

از سوی دیگر، در سمت مشتری، مسائل امنیتی از طریق رمزگذاری داده‌ها در مراحل آموزش و پیش از ارسال به سرور ابری مدیریت می‌شوند. برای کنترل و محدودکردن میزان داده‌هایی که باید در فضای ابری به اشتراک گذاشته شود، از سازوکارهایی مانند حریم خصوصی تفاضلی و رمزگذاری هوموفیک استفاده می‌شود. این روش‌ها به حفظ حریم خصوصی و کاهش ریسک‌های امنیتی کمک کرده و امنیت فرایندهای یادگیری مشارکتی عمیق را تقویت می‌کنند.

۴-۴-۱-۲-۴-بهینه‌سازی FDL

با توجه به محدودیت‌های حافظه و توان محاسباتی دستگاه‌های نهایی، بهینه‌سازی مدل‌های یادگیری عمیق برای استقرار کارآمد در اینترنت اشیا و دستگاه‌های نهایی امری ضروری است.

[1] Gradient

[DOI: 10.61186/jsdp.21.3.23]

از نظر بهینه‌سازی سخت‌افزاری، استفاده از پردازنده‌های گرافیکی GPU می‌تواند به کاهش زمان محاسباتی و افزایش سرعت پردازش کمک کند؛ علاوه‌براین، استفاده از مدارات برنامه‌پذیر و واحد پردازش تنش گوگل [۱۰۷] نیز به تقویت پردازش شبکه‌های یادگیری عمیق کمک می‌کند و قابلیت‌های پردازشی را بهبود می‌بخشد.

از نظر بهینه‌سازی حافظه، الگوریتم‌هایی مانند تخصیص حافظه مشترک می‌توانند به بهینه‌سازی مصرف حافظه در مدل‌های یادگیری عمیق کمک کنند؛ همچنین، برنامه‌ریزی پویا یکی از فرایندهای کلیدی است که برای بهینه‌سازی عملکرد در سرورهای ابری مورد استفاده قرار می‌گیرد[۱۰۸]. فرایند به تخصیص مؤثر منابع و مدیریت بهتر بارهای کاری کمک می‌کند و از کارایی بالاتری در پردازش‌های ابری و محیط‌های توزیع‌شده اطمینان می‌یابد.

به‌اختصار، جدول (۳) به مقایسهٔ دو رویکرد یادگیری ماشین مشارکتی و یادگیری عمیق مشارکتی می‌پردازد. ویژگی‌های کلیدی مورد بررسی شامل ارتباطات، حریم خصوصی، ذخیرهٔ اطلاعات، به‌روزرسانی‌ها، دستگاه‌های متصل به ابر، دسترسی به مدل، کنترل داده‌ها و بهینه‌سازی هستند. این دو رویکرد در نحوهٔ آموزش و استقرار مدل‌های یادگیری ماشین برای دستگاه‌های اینترنت اشیا (IoT) از یکدیگر متمایزند.

انتخاب بین یادگیری ماشین مشارکتی و یادگیری عمیق مشارکتی به شرایط و نیازهای خاص هر پروژه بستگی دارد. اگر سرعت آموزش سریع و دقت بالا مهم باشد، یادگیری عمیق مشارکتی انتخاب مناسب‌تری است؛ در مقابل، اگر حفظ حریم خصوصی داده‌ها و سادگی پیاده‌سازی از اهمیت بالایی برخوردار باشد، یادگیری ماشین مشارکتی انتخاب مناسب‌تری خواهد بود. به‌تازگی، پژوهش‌گران مدل‌های یادگیری عمیق در یادگیری مشارکتی را برای شبکه‌های IIoT در برنامه‌های متنوعی از جمله شبکه‌های اتومبیل، تلفن همراه، شبکه‌های ترافیک و پردازش تصویر پیشنهاد داده‌اند.

۵-۱-۲-۴-بلاک‌چین در IIoT با استفاده از آموزش مشارکتی

آموزش مشارکتی به‌طورمعمول به یک سرور مرکزی متکی است که تمامی به‌روزرسانی‌های مدل‌های یادگیری ماشین و یادگیری عمیق را جمع‌آوری و این به‌روزرسانی‌ها را به مدل جهانی منتقل می‌کند؛ این فرایند ممکن است در معرض خطرات امنیتی قرارگیرد؛ به‌ویژه زمانی‌که به‌روزرسانی‌ها به سرور منتقل می‌شوند یا مدل جهانی برای مشتریان ارسال می‌شود. برای مقابله با این چالش‌های امنیتی، استفاده از فناوری بلاک‌چین به‌عنوان راه‌حلی مناسب مطرح می‌شود که امکان ذخیرهٔ تغییرناپذیر به‌روزرسانی‌های مدل را فراهم می‌آورد. پژوهش‌گران مدلی ایمن را معرفی کرده‌اند که بلاک‌چین را به‌عنوان چارچوبی غیرمتمرکز برای جایگزینی سرورهای مرکزی سنتی به‌کار می‌برد و اطلاعات تاریخی را به شکل داده‌های مقاوم در برابر دست‌کاری ذخیره می‌کند[۱۰۹]. در مطالعه‌ای دیگر پژوهش‌گران برخی از مسائل امنیتی را در گره، بلوک و چارچوب مورد بررسی قرار دادند که با استفاده از بلاک‌چین در آموزش مشارکتی طراحی شده‌اند و راهکارهایی برای طراحی سامانه‌های آموزشی مشارکتی ایمن‌تر ارائه داده‌اند[۱۱۰].

۱-۵-۱-۲-۴- امنیت گره

از نظر امنیت گره، بلاک‌چین به کنترل مجوز گره‌ها از طریق زنجیرهٔ اتحاد و حفظ امنیت داده‌ها با استفاده از زنجیرهٔ گره‌ها می‌پردازد. هر گره با انجام به‌روزرسانی پارامترها یا اصلاحات مدل به‌روز می‌شود و این به‌روزرسانی‌ها به‌صورت زنجیره‌ای و تغییرناپذیر ذخیره می‌شوند؛ همچنین برای اعتبارسنجی گره‌ها و اطمینان از نبود فعالیت‌های مخرب، می‌توان از سازوکار اجماع کمیته استفاده کرد؛ کمیته، که شامل گره‌های معتبر است، به گره‌های معتبر اجازه می‌دهد تا به‌روزرسانی‌ها را ارسال کرده و مدل جهانی را برای آموزش مؤثر به‌روز کنند. در مقابل، اگر به‌روزرسانی از گره‌ای مخرب باشد، آموزش مشارکتی به‌طور خودکار از آن به‌روزرسانی صرف‌نظر می‌کند تا از تأثیرات منفی بر مدل جهانی جلوگیری شود.

۲-۵-۱-۲-۴- امنیت مدل

در آموزش مشارکتی، داده‌ها به‌دلیل نبود تبادل مستقیم اطلاعات بین مشتری و سرور ایمن باقی می‌مانند؛ بااین‌حال، مدل جهانی که بر روی سرور مرکزی ساخته می‌شود، در معرض خطرات امنیتی قرار دارد؛ از جمله حملات سایبری که ممکن است توسط افراد غیرمجاز صورت گیرد. این خطر به‌دلیل تمرکز و دسترسی‌پذیری بالاتر مدل در سرور مرکزی بیشتر از مدل‌های ذخیره‌شده در سرورهای محلی است؛ بنابراین، حفظ

[DOI: 10.61186/jsdp.21.3.23]

امنیت و حراست از مدل‌های ساخته‌شده و آموزش‌دیده در هر دو سرور (مرکزی و محلی)، امری حیاتی است.

در زمینهٔ دستگاه‌های اینترنت اشیای صنعتی دستگاه‌های IIoT به‌گونه‌ای طراحی شده‌اند که به‌طور مستقل مدل را با استفاده از داده‌های محلی آموزش می‌دهند. پس از اتمام فرایند آموزش، هر دستگاه به‌طور مستقل، به‌روزرسانی‌های محلی خود را به گره لبه ارسال می‌کند. گره لبه، که به‌عنوان یک نقطهٔ تجمع عمل می‌کند، به‌روزرسانی‌های محلی را از تمامی دستگاه‌های متصل جمع‌آوری و به گرهی دیگر ارسال می‌کند که در آن به‌روزرسانی‌ها از تمام گره‌های لبه تجمیع می‌شود؛ این به‌روزرسانی‌ها سپس به بلوکی تبدیل می‌شوند که بر اساس قراردادهای هوشمند تأیید و به زنجیرهٔ بلاک‌چین پیوست می‌شود، که به‌طور طبیعی ضد دستکاری و ایمن است؛ در نهایت، سرور مرکزی تمام به‌روزرسانی‌های محلی را برای آموزش مدل جهانی دریافت و پس از فرایند آموزش، به‌روزرسانی‌های مدل جهانی را به تمامی گره‌های لبه ارسال می‌کند تا دستگاه‌های انتهایی متصل به این گره‌ها به‌روزرسانی شوند. این روش بهینه‌سازی و توزیع مدل در محیط‌های اینترنت اشیای صنعتی به حفظ امنیت و کارایی آموزش مشارکتی کمک می‌کند؛ در حالی‌که چالش‌های امنیتی مرتبط با هر دو سرور مرکزی و محلی به‌دقت مدیریت می‌شود.

این چارچوب به گونه‌ای طراحی شده است که برای برنامه‌های کاربردی دنیای واقعی قابل توسعه و با سناریوهای مختلف سازگار باشد. در پژوهش‌های اخیر، پژوهش‌گران با استفاده از تکنولوژی بلاک‌چین، این چارچوب را در حوزه‌های پردازش تصویر و شبکه‌های وسایل نقلیه به‌کار گرفته‌اند. رویکرد مورد استفاده در این پژوهش‌ها، آموزش مشارکتی در چارچوب اینترنت اشیا صنعتی بوده‌است. در چند مطالعهٔ مستقل، پژوهش‌گران چارچوبی مبتنی بر آموزش مشارکتی را برای صنایع مختلف از جمله بهداشت، شبکه‌های راه‌آهن و سازمان دفاعی طراحی و اجرا کرده‌اند[۱۱۱-۱۱۳]. این مطالعات نشان‌دهندهٔ تطبیق‌پذیری و قابلیت کاربرد وسیع این چارچوب در بخش‌های متنوع صنعتی است.

برای حفظ حریم خصوصی در یادگیری مشارکتی با استفاده از اینترنت اشیا صنعتی، از روش‌های متنوعی در دو سطح ارتباطات دستگاه به لبه و لبه به مدل مشترک استفاده می‌شود. این رویکرد کارایی و به‌روزرسانی مشترک را افزایش می‌دهد، با استانداردها و قوانین حریم خصوصی مطابقت دارد و از اطلاعات حساس در تبادلات مشارکتی در برابر سوءاستفاده محافظت می‌کند؛ با این روش می‌توان به بهینه‌سازی هم‌زمان عملکرد و حفظ امنیت داده‌ها پرداخت.

جدول (۴) (در بخش پیوست) به بررسی برنامه‌های کاربردی برای دستگاه‌های تلفن همراه در حوزهٔ اینترنت اشیا می‌پردازد؛ این برنامه‌ها از روش‌های پیشرفتهٔ یادگیری ماشین، به ویژه یادگیری مشارکتی و یادگیری عمیق برای ارائهٔ خدمات هوشمند و کارآمد به کاربران استفاده می‌کنند. مطالعات اخیر نکات مختلفی را مرتبط با این برنامه‌ها تجزیه و تحلیل کرده‌اند؛ از جمله توسعهٔ واژگان صفحه‌کلید بدون صدا، استفاده از استراتژی‌های میانگین انطباقی در جای متوسط مدل‌ها، پیش‌بینی کلمهٔ بعدی در صفحه‌کلید مجازی، بهبود کیفیت پیشنهادات جست‌وجوی صفحه‌کلید مجازی، پیش‌بینی ایموجی از متن تایپ‌شده و شناخت فعالیت‌های انسانی در این برنامه‌ها مورد بررسی قرار گرفته‌است. هر برنامهٔ کاربردی در این جدول با محدودیت‌ها و مزایای خاص خود معرفی شده‌است.

برنامه‌های کاربردی در دستگاه‌های تلفن همراه با بهره‌گیری از روش‌های پیشرفتهٔ یادگیری ماشین، به مزایای چشمگیری دست یافته‌اند؛ از جملهٔ این مزایا، گسترش واژگان صفحه‌کلید بدون صداست که به تنوع محتوا و بهبود کارایی کمک می‌کند[۸۰]؛ به‌علاوه، استفاده از استراتژی میانگین انطباقی با وزن در مدل‌های استاندارد، بهبود عملکرد و افزایش دقت را فراهم می‌کند[۱۱۴]؛ همچنین، این برنامه‌ها با بهره‌گیری از مدل‌های RNN در سرور و محیط‌های مشارکتی، بهبود قابل توجهی در فراخوانی اطلاعات ایجاد می‌کنند[۱۱۵]. آموزش با استفاده از تحدب تابع خطا و مدل‌های رگرسیون ترابری، فرایند یادگیری را ساده و کارآمد می‌سازد[۹۵]. دستیابی به عملکرد بهتر نسبت به یک مدل آموزش‌دیدهٔ سرور، نشان‌دهندهٔ بهره‌وری بالاتر این برنامه‌هاست[۱۱۶]. پتانسیل یکپارچه‌سازی یادگیری تقویتی عمیق و چارچوب یادگیری مشارکتی با سیستم لبهٔ تلفن همراه، بهبود یادگیری و هم‌گرایی در برنامه‌ها را ارائه می‌دهد[۱۱۷]؛ همچنین، پیشنهاد طرح استقرار سرویس آگاهی از حریم خصوصی نشان‌دهندهٔ توجه به امنیت و حریم خصوصی در برنامه‌هاست[۱۱۸]. استفاده از

[DOI: 10.61186/jsdp.21.3.23]

استراتژی‌های بهینه‌سازی گروهی به بهبود عملکرد این برنامه‌ها کمک می‌کند[۱۱۹]. شناسایی و ردکردن مشتری‌های اشتباه از دیگر مزایایی است که به بهبود تجربهٔ کاربری این برنامه‌ها کمک می‌کند[۱۲۰]. در نهایت، ادغام یادگیری امن مشارکتی با تجمیع داده‌های امن، تضمین‌کنندهٔ حفظ حریم خصوصی در این برنامه‌هاست[۱۲۱].

برنامه‌های کاربردی در دستگاه‌های تلفن همراه با وجود مزایای قابل توجه، ممکن است با محدودیت‌های متعددی روبه‌رو شوند؛ برای مثال، تکیه بر حالت احتمالی آموخته‌شده می‌تواند باعث کاهش قابلیت اطمینان و اعتماد به این برنامه‌ها شود[۸۰]. مقاومت ناکافی مدل در برابر نوفهٔ پس‌زمینه، می‌تواند باعث کاهش دقت عملکرد در مواجهه با محیط‌های پرسشی و پیچیده شود[۱۱۴].

هزینهٔ ارتباطی بالا، به‌عنوان یک محدودیت اساسی می‌تواند مانع استفادهٔ گسترده از برنامه‌ها شود[۱۱۵]. استفاده از تعداد زیادی پارامتر در آموزش مدل‌ها، موجب افزایش پیچیدگی و مشکلات در مدیریت و به‌روزرسانی آن‌ها می‌شود[۹۵]. در ارزیابی برنامه‌ها، مسائلی مانند تفاوت در حافظهٔ پنهان مشتریان، نبود قابلیت مقایسه در آزمایشات [۱۱۶] و نبود شناخت نحوهٔ توزیع بار محاسباتی در سناریوهای ناهمگن می‌تواند موانعی را برای بهره‌وری بهینه از منابع محاسباتی ایجاد کند[۱۱۷]. اگر تنها یک مدل تحرک اساسی را مدنظر قرار دهیم[۱۱۹] و از چندین ابر لبه استفاده نکنیم[۱۱۸]، ممکن است با محدودیت‌هایی روبه‌رو شویم که در برخورد با چالش‌ها و نیازهای متنوع برنامه‌ها، مشکلاتی را به‌وجود آورند؛ همچنین، دقت پایین‌تر نسبت به مدل‌های متمرکز [۱۲۰] و معماری پیچیده برای پیاده‌سازی برنامه‌ها، نیاز به دانش و مهارت بالا در توسعه و مدیریت دارد که ممکن است برای توسعه‌دهندگان و مدیران محدودیت ایجاد کند[۱۲۱].

پژوهش‌گران بر روی نقاط قوت و ضعف برنامه‌های کاربردی تمرکز کرده‌اند تا تجربهٔ کاربری را بهبود بخشند و توسعه و عملکرد آن‌ها را بهینه‌سازی کنند. با پیشرفت تکنولوژی‌های یادگیری ماشین، نوآوری‌های چشمگیری در برنامه‌های کاربردی اینترنت اشیا پدیدار خواهد شد و تجربیات جدیدی را برای کاربران در دنیای دیجیتال به ارمغان خواهد آورد. دستگاه‌های تلفن همراه به‌عنوان نقطه قوت این نوآوری‌ها عمل خواهند کرد.

جدول (۵) (در بخش پیوست) خلاصه‌ای از مطالعات اخیر در زمینهٔ یادگیری مشارکتی با تأکید بر امنیت در اینترنت اشیای صنعتی ارائه می‌دهد. سه بخش اصلی این جدول شامل یادگیری ماشین مشارکتی در اینترنت اشیا صنعتی، یادگیری عمیق مشارکتی در اینترنت اشیا صنعتی و بلاک‌چین مشارکتی در اینترنت اشیا صنعتی است. در هر بخش، جزئیات مرتبط با الگوریتم‌ها، کاربردها، روش‌ها و چالش‌های موجود در هر زمینه به‌دقت مورد بررسی قرار گرفته‌است:

یادگیری ماشین مشارکتی در اینترنت اشیا صنعتی: در این بخش، الگوریتم‌هایی نظیر FTM ، Primalchain Tensor Ridge Regression مورد بررسی قرارگرفته‌اند؛ این الگوریتم‌ها در کاربردهای مختلف از جمله پردازش زبان طبیعی و تشخیص گفتار یا تصویرپردازی بررسی شده‌اند.

یادگیری عمیق مشارکتی در اینترنت اشیا صنعتی: این بخش به بررسی الگوریتم‌ها و چارچوب‌های امنیتی در اینترنت اشیا صنعتی می‌پردازد. الگوریتم‌هایی همچونDeepPAR ، DeepDPA، Double Q-Deep Qnetwork وFedGRU مورد بررسی قرارگرفته‌اند. این الگوریتم‌ها در زمینه‌های گوناگون نظیر کارخانه‌های هوشمند یا شبکه‌های ترافیک مورد استفاده قرارمی‌گیرند.

بلاک‌چین مشارکتی در اینترنت اشیا صنعتی: این بخش به بررسی روندها و مطالعات اخیر در حوزهٔ بلاک‌چین‌های مشارکتی در اینترنت اشیا صنعتی می‌پردازد. این بلاک‌چین‌ها به ایجاد همکاری چندجانبه و افزایش امنیت داده‌های IIoT کمک می‌کنند.

مطالعهٔ مقالات اخیر بیانگر آن است که پژوهش‌ها در زمینهٔ یادگیری مشارکتی در اینترنت اشیای صنعتی (IIoT)، به‌سمت ارتقای عملکرد در زمینه‌های مختلف از جمله ذخیره‌سازی داده‌ها، مدیریت داده‌ها و بهینه‌سازی مدیریت منابع فناوری اطلاعات و ارتباطات گام برداشته‌است. این مقالات بر اهمیت بهره‌گیری از یادگیری مشارکتی در IIoT برای تقویت امنیت و حریم خصوصی داده‌ها، بهبود کارایی مدل‌های یادگیری ماشین در شرایط توزیع‌شده و بهینه‌سازی مصرف انرژی تأکید دارند؛ در این راستا، این پژوهش‌ها به نقد و مرور مفاهیم نوآورانه از قبیل به اشتراک‌گذاری داده و فرایندهای آموزش مدل در IIoT می‌پردازند و یادگیری مشارکتی را به‌عنوان یک رویکرد تخصصی و کارآمد برای

[DOI: 10.61186/jsdp.21.3.23]

بهینه‌سازی عملکرد و منابع در این حوزه ترسیم می‌کنند. جدول (۶) (در بخش پیوست) به اختصار به مقالات اخیر این حوزه می‌پردازد.

۶-۱-۲-۴-حفظ حریم خصوصی در یادگیری مشارکتی

یادگیری مشارکتی در حال حاضر سطح حریم خصوصی افراد را نسبت به یادگیری ماشین سنتی در یک مجموعه‌دادهٔ ثابت افزایش می‌دهد. این افزایش حریم خصوصی از طریق کاهش نیاز به انتقال کل داده‌ها به شخص ثالث و استفادهٔ مستقیم از آن برای آموزش مدل‌ها ایجاد می‌شود؛ به‌عبارت دیگر، در یادگیری مشارکتی، داده‌ها محلی نگهداری می‌شوند و تنها پارامترهای مدل به‌صورت امن به اشتراک گذاشته می‌شوند، که این امر از دسترسی مستقیم به اطلاعات شخصی حساس توسط شخص ثالث جلوگیری می‌کند[۶۱]؛ همچنین، استنتاج نیازی به ارسال اطلاعات حساس بیشتر به شخص ثالث ندارد؛ زیرا مدل جهانی از طریق دستگاه شخصی خود در دسترس افراد است[۲۰].

این بهبود در حریم خصوصی به افراد اجازه می‌دهد تا فقط پارامترهای مدل خود را با سرور به اشتراک بگذارند، بدون اینکه داده‌های کامل به سرور منتقل شود. این ویژگی مهم به افراد این امکان را می‌دهد که فعالانه در فرایند یادگیری مشارکت کنند؛ درحالی‌که حفظ حریم خصوصی خود را نیز تضمین می‌کنند.

با وجود پیشرفت‌ها در زمینهٔ حریم خصوصی در یادگیری مشارکتی، به‌روزرسانی‌های وزن یا شیب بارگذاری‌شده توسط افراد ممکن است اطلاعات مربوط به داده‌های کاربر را فاش کند؛ این امر به‌خصوص در مواردی که وزن‌های خاصی در ماتریس وزن به ویژگی‌ها یا مقادیر خاص داده‌های فرد حساس باشد، صدق می‌کند؛ برای مثال، این به‌روزرسانی‌ها ممکن است حاوی کلمات خاصی در پیش‌بینی زبان مدل باشند[۱۴۵]. این به‌روزرسانی‌ها برای هر مشتری که در یادگیری مشارکتی و همچنین سرور تجمیعی شرکت می‌کند در دسترس است. این مسئله نشان از چالش‌ها و نیاز به راه‌حل‌های بیشتر برای حفظ حریم خصوصی در این زمینه دارد.

جدول (۷) (در بخش پیوست) خلاصه‌ای از پژوهش‌های مهم در زمینهٔ یادگیری مشارکتی با تمرکز بر مکانیسم‌های افزایش حریم خصوصی را نشان می‌دهد؛ این پژوهش‌ها به‌دنبال راهکارهایی برای حفظ حریم خصوصی داده‌ها در هنگام آموزش مدل‌های یادگیری ماشینی به‌صورت مشارکتی هستند.

بر اساس بررسی پژوهش‌ها دو دستهٔ اصلی مکانیسم‌های حریم خصوصی در این زمینه وجود دارد: حریم خصوصی تفاضلی (DP)[1] و محاسبات ایمن چندحزبی (SMC)[2]. حریم خصوصی تفاضلی در کل برای محافظت از داده‌های محلی در برابر سرور استفاده می‌شود. این روش با اضافه‌کردن نوفه به داده‌ها، حریم خصوصی آن‌ها را حفظ می‌کند؛ به این ترتیب، حتی با دسترسی به مدل آموزش‌دیده، امکان استنتاج درست در مورد داده‌های خاصی وجود ندارد. در زمینه‌هایی که نیاز به حفظ حریم خصوصی داده‌ها در آموزش مدل‌ها وجود دارد، حریم خصوصی تفاضلی به‌خوبی عمل می‌کند.

محاسبات ایمن چندحزبی در کل برای محافظت از داده‌های محلی در برابر سایر دستگاه‌های مشارکتی استفاده می‌شود. این روش با انجام محاسبات به‌صورت رمزنگاری‌شده، حریم خصوصی داده‌ها را حفظ می‌کند؛ این روش به‌دلیل امکان انجام محاسبات رمزنگاری‌شده، در مواردی که چندین دستگاه می‌خواهند با یکدیگر همکاری کنند و همچنین حریم خصوصی داده‌ها باید حفظ شود، محاسبات ایمن چندحزبی اثربخش است.

پژوهش‌ها نشان از تنوع در رویکردهای حفظ حریم خصوصی در یادگیری مشارکتی دارد. این تنوع به‌دلیل چالش‌های مختلفی است که در این زمینه وجود دارد؛ از جملهٔ این رویکردها می‌توان به حفاظت از داده‌های محلی در برابر سرور، حفاظت از داده‌های محلی در برابر سایر دستگاه‌های مشارکتی، حفظ کارایی محاسباتی و حفظ دقت مدل‌های یادگیری ماشینی اشاره کرد.

انتخاب سازوکار مناسب برای حفظ حریم خصوصی در یادگیری مشارکتی به شرایط و نیازهای خاص هر پروژه بستگی دارد. جدول (۷) به تفصیل مکانیسم‌های مختلف حریم خصوصی، سهم عمدهٔ هر پژوهش و مرجع مربوطه را شرح می‌دهد.

۷-۱-۲-۴-یادگیری مشارکتی در انفورماتیک سلامت

در حال حاضر، با افزایش روزافزون جمعیت، فشار قابل توجهی بر کارکنان و پزشکان بیمارستان‌ها به‌ویژه در زمینهٔ ارائهٔ خدمات بهداشتی و درمانی وجود دارد؛ این فشار می‌تواند به کاهش کیفیت خدمات منجر شود. رفع این چالش نیازمند ارائهٔ راه‌حل‌های کارآمد و قابل اعتماد جدیدی از طریق بهره‌مندی از پیشرفت‌های علم‌وفناوری است؛ در این راستا، افزایش بهره‌وری و بهینه‌سازی فرایندهای بیمارستانی از طریق بهره‌گیری

[1] Differential Privacy (DP)
[2] Secure Multi-party Computation (SMC)

[DOI: 10.61186/jsdp.21.3.23]

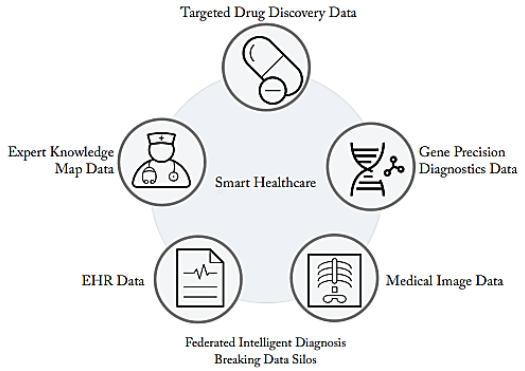
از فناوری‌های نوین می‌تواند نقش مؤثری در بهبود عملکرد نظام بهداشت و درمان و کاهش فشارهای وارده بر پرسنل ایفا کند؛ همچنین افزایش رضایت بیماران را به همراه خواهد داشت[۵۸].

در دههٔ اخیر، با پیشرفت سریع علوم رایانه و فناوری‌های سخت‌افزاری، حجم گسترده‌ای از اطلاعات در زمینه‌های مختلف از جمله مراقبت‌های بهداشتی در اختیار مراکز درمانی، بیماران، شرکت‌های بیمه و صنایع دارویی قرار گرفته‌است؛ این اطلاعات به‌عنوان منبعی ارزشمند و بی‌سابقه، فرصت‌های فراوانی را برای فناوری‌های علوم داده به ارمغان آورده‌است. این فناوری‌ها، با استفاده از تحلیل داده‌ها و استخراج بینش‌های قابل استفاده می‌توانند بهبود چشم‌گیری در کیفیت ارائهٔ خدمات در این حوزه‌ها ایجاد کنند[۸۴]. با پیشرفت فناوری‌های هوش مصنوعی برنامه‌های کاربردی بسیاری در زمینهٔ سلامت با هدف کاهش هزینه‌های نیروی کار، خطاهای انسانی و افزایش بهره‌وری توسعه یافته‌اند؛ یکی از کاربردهای مهم هوش مصنوعی در حوزهٔ سلامت، تشخیص بیماری‌ها در مراحل ابتدایی است. با استفاده از تکنولوژی‌های هوش مصنوعی، فرایند تشخیص بیماری‌ها بهبود یافته و نتایج مؤثری به‌دست آمده‌است؛ این تکنولوژی‌ها به ارائه‌دهندگان مراقبت‌های بهداشتی این امکان را می‌دهند تا با استفاده از داده‌های جمع‌آوری‌شده، بهبود کارایی و افزایش کیفیت مراقبت از بیماران را تجربه کنند[۴۱]. کاربردهای هوش مصنوعی در حوزهٔ سلامت شامل زمینه‌های متنوعی می‌شوند؛ تشخیص هوشمند بیماری‌ها، کشف داروهای هدفمند، بهره‌گیری از دانش خبره، تشخیص دقیق ژن‌ها، تحلیل تصاویر پزشکی و مدیریت پروندهٔ الکترونیک سلامت[1] از جملهٔ این زمینه‌های کاربردی هستند.

شکل (۱۱) نگاهی جامع به کاربردهای هوش مصنوعی در حوزهٔ سلامت ارائه می‌دهد که سبب بهبود فرایندهای تشخیص، پیشگیری و مدیریت بیماری‌ها می‌شود و برای ارائه‌دهندگان مراقبت‌های بهداشتی، ابزارهای قدرتمندی را برای ارتقای سطح خدمات بهداشتی فراهم می‌کنند. پنج منبع دادهٔ کلیدی در شکل (۱۱) شامل داده‌های کشف هدفمند دارو، داده‌های تشخیص دقیق ژنی، داده‌های تصاویر پزشکی، داده‌های سوابق پزشکی الکترونیک و داده‌های نقشهٔ دانش تخصصی هستند که هوش مصنوعی برای تشخیص‌های دقیق‌تر و مؤثرتر از آن‌ها بهره می‌برد.

[1] Electronic Health Record (EHR)

داده‌های کشف هدفمند دارو، مجموعه‌ای از اطلاعات مربوط به مولکول‌ها و ترکیبات شیمیایی‌اند که می‌توانند برای طراحی و توسعهٔ داروهای جدید مورد استفاده قرارگیرند. این داده‌ها شامل اطلاعاتی مانند ساختار مولکولی، خواص بیوشیمیایی و فعالیت‌های زیستی مولکول‌ها هستند.



(شکل-۱۱): کاربرد هوش مصنوعی در تشخیص هوشمند حوزهٔ سلامت [۴۱]

(Figure-11): Application of artificial intelligence in intelligent health diagnosis

داده‌های تشخیص دقیق ژنی، مجموعه‌ای از اطلاعات مربوط به توالی ژن‌ها و ارتباط آن‌ها با بیماری‌ها هستند که برای تشخیص دقیق‌تر بیماری‌ها و ارائهٔ درمان‌های شخصی‌سازی‌شده استفاده می‌شوند. داده‌های تصاویر پزشکی، مجموعه‌ای از تصاویر حاصل از روش‌های مختلف تصویربرداری مانند اشعهٔ ایکس، ام‌آرآی، سی‌تی‌اسکن و سونوگرافی هستند؛ این داده‌ها اطلاعات ارزشمندی در مورد ساختار و عملکرد بدن انسان ارائه می‌کنند و می‌توانند برای تشخیص بیماری‌ها، بررسی وضعیت بیماران و برنامه‌ریزی درمان‌های مناسب مورداستفاده قرارگیرند. داده‌های سوابق پزشکی الکترونیک شامل اطلاعات مربوط به تاریخچهٔ پزشکی، داروهای مصرفی و درمان‌های انجام‌شده برای بیماران هستند؛ این داده‌ها می‌توانند برای ارائهٔ مراقبت‌های شخصی‌سازی‌شده و پیش‌بینی خطر ابتلا به بیماری‌ها مورداستفاده قرارگیرند. داده‌های نقشهٔ دانش تخصصی، مجموعه‌ای از اطلاعات مربوط به تجربیات، دانش و تخصص پزشکان و متخصصان حوزهٔ سلامت در زمینه‌های مختلف پزشکی است؛ این داده‌ها شامل اطلاعاتی مانند علائم بیماری‌ها، روش‌های تشخیصی، درمان‌های مؤثر و عوارض جانبی داروها هستند که می‌توانند برای بهبود دقت تشخیص، ارائهٔ درمان‌های مؤثر و کاهش خطاهای پزشکی مورد استفاده قرارگیرند.

[DOI: 10.61186/jsdp.21.3.23]

هوش مصنوعی با تجزیه و تحلیل این داده‌ها و شناسایی الگوهای پیچیده می‌تواند به پزشکان در تشخیص دقیق‌تر و سریع‌تر بیماری‌ها و ارائهٔ درمان‌های مؤثرتر کمک کند؛ بااین‌حال، پذیرش فناوری‌های هوش مصنوعی در صنعت سلامت و مراقبت‌های بهداشتی همچنان در مراحل ابتدایی خود باقی مانده‌است. در هر سازمانی، جمع‌آوری داده‌ها امری حیاتی است؛ این داده‌ها را می‌توان برای پیش‌بینی روندهای فعلی و رویدادهای آینده مورد استفاده قرار داد. عوامل زیادی در کمبود سامانه‌های پزشکی هوشمند نقش دارند؛ یکی از موارد مهم، مشکل در جمع‌آوری حجم مناسب از داده‌ها با ویژگی‌های غنی است که می‌تواند علائم یک بیمار را توصیف جامع کند[۸۹].

یکی دیگر از کاربردهای هوش مصنوعی در حوزهٔ سلامت تحلیل تصاویر پزشکی است که امروزه با کمک بینایی ماشین و یادگیری ماشین پیشرفت قابل‌توجهی کرده‌است[۱۵۲]. موفقیت چشم‌گیر روش‌های یادگیری ماشین مدرن، به‌ویژه یادگیری عمیق را می‌توان به ساخت و انتشار پایگاه داده‌های عظیم تصاویر طبیعی مانند ImageNet[1] و MS COCO[2] نسبت داد؛ بااین‌حال، تحلیل تصاویر پزشکی برخلاف تحلیل تصاویر طبیعی، همچنان با چالش اندازهٔ نمونهٔ کوچک مواجه است[۱۵۳].

برطرف‌کردن این چالش نیازمند ایجاد سامانه‌های جمع‌آوری داده‌های هوشمند و کارآمد است. جمع‌آوری داده‌ها با ویژگی‌های غنی از طریق حسگرها، تجهیزات پزشکی پیشرفته و فناوری‌های جدید ممکن است یکی از راه‌حل‌های مؤثر برای افزایش دقت تشخیص و پیش‌بینی بیماری‌ها باشد؛ از طرفی در بخش مراقبت‌های بهداشتی، حجم زیادی از داده‌های حساس تولید می‌شود و مدیریت و ایمن‌سازی داده‌های خصوصی بسیار دشوار است[۱۵۴]. به‌طورمعمول، هر مرکز درمانی ممکن است داده‌های بسیاری از بیماران داشته باشد، اما این تعداد داده برای آموزش مدل‌های پیش‌بینی موردنظر کافی نباشد[۱۵۵]؛ برای مثال، آموزش یک آشکارساز تومور مبتنی بر هوش مصنوعی نیازمند پایگاه داده بزرگی است که طیف کاملی از آناتومی‌ها، آسیب‌شناسی‌ها و انواع داده‌های ورودی را دربرمی‌گیرد. به‌دست‌آوردن چنین داده‌هایی دشوار است؛ زیرا داده‌های بهداشتی بسیار حساس و استفاده از آن‌ها به‌شدت تحت‌نظارت است[۱۵۶].

با توجه به نقش محوری ساختاردهی بهینهٔ روش‌های جمع‌آوری، ذخیره‌سازی و پردازش داده‌ها در سازمان‌های پزشکی، به‌کارگیری فناوری‌های هوش مصنوعی در این‌حوزه، فرصتی بی‌نظیر برای ارتقای کیفیت خدمات پزشکی و تسهیل تصمیم‌گیری‌های پزشکان ایفا می‌کند؛ ازاین‌رو، تلاش در این زمینه از اهمیتی بسزا برخوردار است.

پرونده‌های الکترونیک سلامت به‌عنوان منبع مهمی از داده‌های مراقبت‌های بهداشتی شناخته می‌شوند که حجم عظیمی از داده‌های بیماران را برای تجزیه و تحلیل فراهم می‌کند[۱۵۷]. داده‌های پزشکی درکل به‌عنوان داده‌های متنی، تصویری، ویدئویی، صوتی و چهاربعدی طبقه‌بندی می‌شوند. تمام جنبه‌های داده‌های پزشکی، اعم از جمع‌آوری، ذخیره، اشتراک‌گذاری یا دریافت‌شده، در معرض خطرات امنیتی‌اند و امنیت‌داده‌ها در حال تبدیل‌شدن به یک نگرانی فزایندهٔ مهم برای کاربران است. با توجه به اهمیت امنیت داده‌های حساس در حوزهٔ سلامت، نیاز به توسعهٔ روش‌های نوآورانه برای مدیریت و ایمن‌سازی داده‌های حساس سلامت وجود دارد[۹۰].

یکی از چالش‌های مهم در حوزهٔ داده‌های سلامت، خصوصی و پراکنده‌بودن این داده‌هاست؛ برای نمونه، بیمارستان‌ها به‌دلیل داشتن پرونده‌های الکترونیک سلامت از جمعیت گسترده‌ای از بیماران، با مسئلهٔ پراکندگی داده‌ها مواجه‌اند؛ این پرونده‌ها شامل اطلاعات حساس با حریم خصوصی بالا هستند و به‌دلیل محدودیت‌ها در قوانین حفظ حریم خصوصی، اشتراک‌گذاری و ادغام این داده‌ها از بیمارستان‌های مختلف با چالش‌های قانونی و فنی مواجه می‌شود[۱۵۸].

در مواردی مانند سوابق پزشکی که داده‌ها به‌صورت محلی ذخیره و برچسب‌گذاری می‌شوند، حفظ حریم خصوصی یک چالش بزرگ است که باعث ممنوعیت اشتراک‌گذاری اطلاعات بین بیمارستان‌ها می‌شود[۱۵۹]. مقررات سخت‌گیرانه‌ای مانند قانون قابل حمل و پاسخ‌گویی بیمهٔ سلامت[3] برای تنظیم فرایند دسترسی و تجزیه و تحلیل داده‌های سلامت ایجاد شده‌است؛ حتی اگر ناشناس‌سازی داده‌ها بتواند تا حدودی این محدودیت‌ها را برطرف کند، پژوهش‌ها بیانگر آن است که حذف ابرداده‌ها مانند نام بیمار یا تاریخ تولد برای حفظ حریم خصوصی کافی نیست[۱۶۰]. محدودیت دسترسی به داده‌ها یک چالش بزرگ برای توسعهٔ رویکردهای تحلیلی داده‌ها، فناوری‌های نوین داده‌کاوی و یادگیری ماشین مانند

[1] Imagenet: A large-scale hierarchical image database
[2] Microsoft COCO: Common objects in context
[3] Health Insurance Portability and Accountability Act (HIPAA)

[DOI: 10.61186/jsdp.21.3.23]

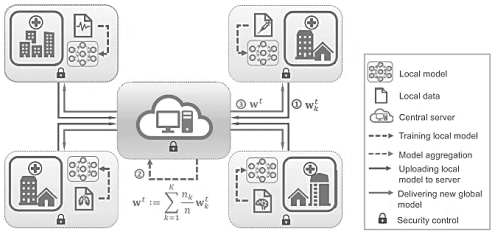
یادگیری عمیق [۱۶۱] است که به حجم زیادی از داده‌های متنوع با حجم بالا، برای آموزش نیاز دارند. از سوی دیگر، پرونده‌های الکترونیک سلامت حاوی سوگیری‌های نظام‌مند هستند که تعمیم‌پذیری نتایج را محدود می‌کند؛ این محدودیت‌ها از دلایل مختلفی از جمله تفاوت در دسترسی به اطلاعات یا تعداد کم نمونه‌های داده‌های آموزشی ناشی می‌شوند[۸۴].

درکل، داده‌های پزشکی دارای دو مشکل اساسی هستند: کمبود داده و برچسب‌گذاری ناکافی. این دو مشکل با استفاده از یادگیری انتقال مشارکتی قابل حل‌اند[۸۷]. برای برطرف‌کردن مشکل کمبود داده، مراکز پزشکی می‌توانند داده‌های خود را با رعایت مقررات حفاظت از حریم خصوصی به اشتراک بگذارند. این اقدام منجر به تولید مجموعه‌دادهٔ بزرگ می‌شود که آموزش مدل را بسیار بهتر از مدل‌های آموزش داده‌شده بر روی داده‌های یک مؤسسهٔ پزشکی واحد انجام می‌دهد.

استفاده از سازوکار یادگیری مشارکتی، که برای آموزش یک مدل جهانی مشترک، تمام داده‌های حساس را در مؤسسات محلی که داده‌ها به آن مجموعه تعلق دارند، حفظ می‌کند، می‌تواند به‌عنوان ابزاری مؤثر در ارتباط‌دادن منابع دادهٔ مراقبت‌های بهداشتی با حفظ حریم خصوصی آن‌ها در زمینهٔ مطالعات علوم‌داده بسیار مؤثر باشد؛ این رویکرد، با حفظ اطلاعات حساس در سطح محلی و هم‌زمان ایجاد یک مدل جهانی کارآمد، امکان انجام پژوهش‌های پیشرفته در حوزهٔ مراقبت‌های بهداشتی را با احترام به حریم خصوصی افراد و نهادها تسهیل می‌کند. یادگیری مشارکتی همهٔ مؤسسات مراقبت‌های بهداشتی را گرد هم می‌آورد و آن‌ها را قادر می‌سازد از حریم خصوصی خود اطمینان حاصل کنند و بدون افشای اطلاعات شخصی به یکدیگر متصل شوند[۸۹].

در یادگیری مشارکتی، عملکرد مدل‌های یادگیری ماشین با استفاده از مجموعه‌داده‌های پزشکی بزرگ و متنوع ارتقا قابل توجهی می‌یابد. با اشتراک‌گذاری داده‌ها به‌وسیلهٔ تعداد مناسبی از مؤسسات پزشکی در آینده از طریق یادگیری مشارکتی، هوش مصنوعی در حوزهٔ سلامت می‌تواند منافع بیشتری را برای بیماران به ارمغان بیاورد. این تبادل داده‌ها از طریق یک رویکرد مشارکتی، با حفظ حریم خصوصی و اطمینان از امنیت اطلاعات، به ارتقای خدمات بهداشتی و ارائه درمان‌های بهتر به افراد یاری خواهد رساند.

در حوزهٔ سلامت، یادگیری مشارکتی اغلب برای مطالعهٔ طیف وسیعی از وظایف، مانند هویت کاربر[1]، شناخت کاربر[2]، تشخیص[3]، شناسایی بستری‌شدن‌های احتمالی، تشخیص میزان مرگ‌ومیر، دوره‌های پذیرش در بخش مراقبت‌های ویژه و غیره استفاده می‌شود. الگوریتم‌های یادگیری ماشین به مجموعه‌داده‌های گسترده و جامع نیاز دارند و یادگیری مشارکتی دسترسی کنترل‌شده و غیرمستقیم را در عین محافظت از حریم خصوصی بیمار فراهم می‌کند. در شکل (۱۲) فرایند یادگیری مشارکتی در تجمیع داده‌های مراکز سلامت بیان‌شده‌است.



(شکل-۱۲): فرایند یادگیری مشارکتی در تجمیع داده‌های مراکز سلامت [۸۴]

(Figure-12): The process of federated learning in data aggregation of health centers

این چارچوب یک فرایند آموزش توزیع‌شده برای مدل‌های یادگیری ماشین در حوزهٔ سلامت را ارائه می‌دهد؛ در این فرایند، مراکز سلامت با استفاده از داده‌های محلی خود، مدل‌های یادگیری ماشین محلی را آموزش می‌دهند؛ سپس، به‌روزرسانی‌های این مدل‌ها دوره‌ای با یک سرور مرکزی به اشتراک گذاشته می‌شود. سرور مرکزی این به‌روزرسانی‌ها را جمع‌آوری و برای آموزش یک مدل جهانی ترکیب می‌کند؛ درنهایت، پارامترهای به‌روزرسانی‌شدهٔ مدل جهانی به تمام مراکز ارسال می‌شود تا از آن برای بهبود مدل‌های محلی خود استفاده کنند. این روش با حفظ حریم خصوصی بالا، بهره‌وری بیشتر در آموزش مدل‌ها به‌صورت محلی و افزایش دقت را ارائه می‌دهد.

امروزه کاربردهای یادگیری مشارکتی در حوزهٔ مراقبت‌های بهداشتی و سلامت مورد مطالعه و بررسی قرارگرفته‌اند. این کاربردها شامل مواردی همچون یادگیری شباهت بیمار [۱۶۲]، یادگیری بازنمایی بیمار، فنوتیپ‌سازی [۱۶۳, ۱۶۴] و مدل‌سازی پیش‌بینی می‌شوند[۱۶۵-۱۶۷]؛ این پژوهش‌ها نشان‌دهندهٔ تلاش‌های جدید و نوآورانه در جهت بهبود خدمات

[1] client identity
[2] client knowledge
[3] diagnostics

[DOI: 10.61186/jsdp.21.3.23]

بهداشتی و دقت در تشخیص، پیش‌بینی و مدیریت حوزهٔ سلامت با استفاده از یادگیری مشارکتی هستند.

پژوهش‌گران در مطالعهٔ [۱۶۲] یک پلتفرم حفظ حریم خصوصی را در یک محیط مشارکتی برای یادگیری شباهت بیماران در سراسر مؤسسات ارائه کردند. مدل آن‌ها امکان یافتن بیماران مشابه را از یک بیمارستان به بیمارستان دیگر، بدون اشتراک‌گذاشتن اطلاعات در سطح بیمار فراهم می‌کند؛ این رویکرد نه‌تنها اطمینان از حفظ حریم خصوصی بیماران را تضمین می‌کند بلکه به اشتراک‌گذاری داده‌ها را بین مؤسسات بهداشتی تسهیل می‌کند.

در پژوهش [۱۶۴] از مدل‌های فاکتورسازی تانسور برای تحلیل پرونده‌های سلامت الکترونیکی استفاده شده‌است؛ این مدل‌ها با استفاده از فاکتورسازی تانسور، داده‌های حاوی حجم زیادی از اطلاعات را به فنوتیپ‌های معنادار تبدیل می‌کنند. این فنوتیپ‌ها در محیط یادگیری مشارکتی برای تحلیل دقیق و کارآمد داده‌ها به‌کار می‌روند؛ این روش کارایی بالا و امکان تفسیر قابل توجهی در تحلیل داده‌های سلامت با حجم بالا را دارد و می‌تواند به‌طور قابل توجهی به بهبود فهم داده‌های سلامت و پشتیبانی از تصمیم‌گیری‌های پزشکان کمک کند.

در پژوهش مرجع [۱۶۳] یادگیری بازنمایی بیمار و بیماری چاقی مورد بررسی قرار گرفت؛ این پژوهش به بررسی نحوهٔ بازنمایی اطلاعات مربوط به بیماران و بیماری چاقی و ویژگی‌ها و الگوهای مرتبط با آن می‌پردازد؛ در این مطالعه از روش‌ها و روش‌های یادگیری ماشین برای بهبود نمایان‌سازی و بازنمایی داده‌ها به‌منظور تسهیل در تحلیل و درک بهتر بیماران و مسائل مرتبط با چاقی استفاده شده‌است.

در یادگیری مشارکتی، مدل‌سازی پیش‌بینی‌کننده نیز به‌وسیلهٔ دریافت اطلاعات از منابع مختلف صورت می‌گیرد که می‌تواند به پزشکان این امکان را بدهد تا اطلاعات بیشتری در مورد خطرات و فرایند درمان سریع‌تر بیماران دریافت کنند[۱۶۵, ۱۶۷, ۱۶۸]؛ برای مثال، پژوهش‌گران یک چارچوب حفظ حریم خصوصی را برای وظیفهٔ پیش‌بینی مرگ‌ومیر در بیمارستان در میان بیماران بستری در بخش مراقبت‌های ویژه[1] آزمایش کردند[۱۶۷].

برای افزایش کارایی یادگیری عمیق و همچنین حفظ حریم خصوصی در حوزهٔ سلامت، در یک پژوهش، یک چارچوب یادگیری مشارکتی معرفی شده‌است که به تسهیل آموزش مشترک مدل‌های یادگیری عمیق بدون نیاز به انتقال داده‌های حساس یا جزئیات مدل می‌پردازد؛ این رویکرد نوآورانه امکان یادگیری اطلاعات مفید از داده‌ها را بدون نیاز به اشتراک‌گذاشتن اطلاعات حساس فراهم می‌کند؛ در این پژوهش، تمرکز بر روی بررسی روابط ساختاری مغز در میان بیماری‌ها و گروه‌های بالینی قرار گرفته‌است و این چارچوب می‌تواند به تحلیل بهتر و درک عمیق‌تر از عوامل مؤثر در این روابط کمک کند[۱۶۹].

با هدف پیش‌بینی بستری‌شدن بیماران مبتلا به بیماری‌های قلبی با استفاده از داده‌های پروندهٔ الکترونیک سلامت از منابع داده‌ای مختلف، پژوهش دیگری صورت گرفت؛ در این مطالعه از طبقه‌بندی‌کنندهٔ ماشین بردار پشتیبان[2] برای تحلیل داده‌ها و از رویکرد یادگیری مشارکتی برای پیش‌بینی مقاومت بیماران در برابر برخی درمان‌ها و داروها و میزان بقای آن‌ها در مواجهه با بیماری‌های خاص استفاده شد[۱۶۵].

در پژوهشی دیگر، تحلیل پروندهٔ الکترونیکی سلامت برای پیش‌بینی زایمان زودرس مورد بررسی قرار گرفت؛ نتایج این پژوهش نشان دادند که مدل‌های تجمعی با درنظرگرفتن عدم‌قطعیت بهبود قابل توجهی در پیش‌بینی زایمان زودرس دارد و سهم مدل‌های با عدم‌قطعیت بالا در این مدل‌های تجمعی کاهش یافته‌است. این یافته‌ها نشان از اهمیت درنظرگرفتن عدم‌قطعیت در مدل‌های پیش‌بینی زایمان زودرس دارد؛ این رویکرد می‌تواند به بهبود مدیریت و پیشگیری از مشکلات مرتبط با زایمان زودرس در مراقبت‌های بهداشتی کمک کند[۱۶۸].

در این راستا، در پژوهشی دیگر به پیش‌بینی مدت زمان بستری بیماران و مرگ‌ومیر در ۳۱ بیمارستان در پایگاه‌دادهٔ پژوهش‌های مشترک eICU پرداخته شد[۱۷۰]؛ این پژوهش نشان می‌دهد که استفاده از مدل‌های یادگیری ماشین، به‌ویژه در یادگیری مشارکتی، می‌تواند به بهبود پیش‌بینی مدت‌زمان بستری بیماران و احتمال مرگ‌ومیر آن‌ها کمک کند؛ این رویکردها نه‌تنها می‌توانند دقت تشخیص را افزایش دهند؛ بلکه به پزشکان کمک می‌کنند تا سریع‌تر و با اطمینان بیشتر به تصمیم‌گیری‌های درمانی بپردازند.

در پژوهشی دیگر، یک شبکهٔ مشارکتی چندگانه[3] مبتنی بر شبکهٔ APOLLO با بهره‌گیری از سیستم مراقبت‌های بهداشتی به‌هم‌پیوسته طراحی و اجرا

[1] ICU

[2] SVM

[3] multi-FL network

[DOI: 10.61186/jsdp.21.3.23]

شده‌است؛ این شبکه با استفاده از اطلاعات دقیق جمع‌آوری‌شده از سیستم مراقبت‌های بهداشتی، داده‌های طولی سلامت و داده‌های پیامد را به‌دقت تجزیه و تحلیل می‌کند. این تحلیل اطلاعات به پزشکان کمک می‌کند تا وضعیت آیندهٔ بیماران را پیش‌بینی کنند؛ از طریق این شبکهٔ مشارکتی، شواهد تشخیص پزشکی از داده‌های دنیای واقعی به‌دقت تبدیل می‌شود و این ارتباط نوآورانه می‌تواند به پیشرفت در پیش‌بینی و درمان بیماران کمک کند[۱۷۱].

چکیده‌ای از پژوهش‌های یادگیری مشارکتی در حوزهٔ سلامت در جدول (۸) و جدول (۹) (در بخش پیوست) ذکر شده‌است. یادگیری مشابهت بیمار برای گروه‌بندی بیماران بر اساس شباهت علائم و نشانه‌های بیماری، فنوتیپ‌سازی برای شناسایی ویژگی‌های ژنتیکی و بالینی مرتبط با بیماری، پیش‌بینی مرگ‌ومیر به‌منظور تخمین احتمال مرگ بیمار، تشخیص بیماری از طریق داده‌های پزشکی و تجزیه و تحلیل داده‌های تصویربرداری از قبیل اسکن MRI و اشعهٔ ایکس از جمله کاربردهایی هستند که در جدول (۸) در زمینهٔ یادگیری ماشین و یادگیری مشارکتی در حوزهٔ سلامت مطرح شده‌اند.

این رویکردها امکان پیش‌بینی و تشخیص تغییرات در وضعیت بیماران را فراهم می‌کنند، که منجر به بهبود کیفیت مراقبت‌های بهداشتی و افزایش دقت در تصمیم‌گیری‌های پزشکان می‌شوند؛ این جدول همچنین نشان می‌دهد که با توجه به موضوع و هدف هر پروژه از روش‌های مختلف یادگیری ماشین در یادگیری مشارکتی در زمینهٔ مراقبت‌های بهداشتی و سلامت استفاده می‌شود. تعداد مشتری‌ها نشان‌دهندهٔ تعداد دستگاه‌هایی است که در مدل یادگیری مشارکتی شرکت کرده‌اند. این تعداد می‌تواند با توجه به رویکرد هر مطالعه، از چند دستگاه تا چندهزار دستگاه متغیر باشد.

جدول (۹)، برنامه‌های کاربردی مبتنی بر یادگیری مشارکتی با هدف مقابله با چالش‌ها و ارتقا کیفیت خدمات در حوزهٔ مراقبت‌های بهداشتی و سلامت را همراه با مزایا و محدودیت‌هایشان بررسی می‌کند؛ این برنامه‌ها به‌عنوان ابزاری قدرتمند در پیش‌بینی بستری‌شدن بیماران، تجزیه و تحلیل تصاویر MRI برای تشخیص بیماری‌ها، پردازش یادداشت‌های بالینی، طبقه‌بندی EEG، پیش‌بینی مرگ‌ومیر بیماران، تجزیه و تحلیل فنوتیپ‌ها و تطبیق مشابهت بیماران استفاده می‌شوند و دارای رویکردها و الگوریتم‌های خاص خود در تحلیل داده‌ها هستند. بررسی جامع این برنامه‌ها نشان می‌دهد که یادگیری مشارکتی به‌عنوان یک رویکرد نوین در حوزهٔ سلامت، می‌تواند نقش به‌سزایی در پیشرفت و بهبود عملکرد این حوزه ایفا کند.

۵-چشم‌اندازهای آینده

رشد سریع هوش مصنوعی در عصر حاضر، فرایند هوشمندسازی دیجیتال را در صنایع مختلف تسریع بخشیده و این امر ضمن به ارمغان‌آوردن مزایای متعدد، چالش‌هایی را نیز به‌همراه داشته‌است. یکی از این چالش‌ها، معضل تکه‌تکه‌شدن داده‌ها[1] و جزیره‌ای‌شدن داده‌ها[2] است[۱۸۵, ۱۸۶]. این چالش مانع به اشتراک‌گذاری داده‌ها بین حوزه‌های مختلف می‌شود و امکان بهره‌برداری کامل از ارزش بالقوهٔ داده‌ها را محدود می‌کند. ظهور یادگیری مشارکتی تا حدودی مسائل بالا را کاهش داده و به کانون توجه بسیاری از پژوهش‌گران تبدیل شده‌است؛ با وجود این، توسعهٔ یادگیری مشارکتی با چالش‌های متعددی روبه‌روست و هیچ استراتژی واحدی نمی‌تواند به‌طور جامع این موانع را در کاربرد عملی فناوری یادگیری مشارکتی حل کند؛ اگرچه پژوهش‌گران در مورد تمام جنبه‌های یادگیری مشارکتی به‌عنوان یک تکنیک یادگیری ماشین جدید با حفظ حریم خصوصی مطالعاتی انجام داده‌اند، اما همچنان برخی جنبه‌ها نیازمند توجه بیشتر پژوهش‌گران برای مطالعه و کاوش عمیق‌ترند.

۵-۱-ارتقای امنیت یادگیری مشارکتی با استفاده از الگوریتم‌های رمزنگاری کارآمدتر و روش‌های دفاعی تهاجمی

با پیشرفت روزافزون فناوری اطلاعات و پیچیده‌ترشدن روش‌های هک، حفاظت از داده‌ها و حفظ حریم خصوصی کاربران به چالشی فزاینده تبدیل شده‌است[۱۸۷]. ظهور انواع جدید حملات سایبری مانند DOS، DDoS و بدافزار، خطر افشای اطلاعات خصوصی کاربران را به‌طور قابل‌توجهی افزایش می‌دهد و اشتراک‌گذاری داده‌ها در یادگیری مشارکتی را به امری مخاطره‌آمیز تبدیل می‌کند[۱۸۸]؛ این چالش‌ها، ضرورت ارتقای امنیت یادگیری مشارکتی را برای تسهیل اشتراک‌گذاری امن داده‌ها و مشارکت فعالانه‌تر کاربران

[1] data fragmentation
[2] data island

[DOI: 10.61186/jsdp.21.3.23]

در این فرایند مشارکتی آشکار می‌کند. اجرای روش‌های یادگیری مشارکتی در کنار سیاست‌ها و فرایندهای مناسب حفظ حریم خصوصی و ارتقای امنیت یادگیری مشارکتی با استفاده از روش‌های رمزنگاری قوی‌تر و سازوکارهای پیشرفتهٔ تشخیص حمله ضروری است[۱۸۹]؛ در این راستا، می‌توان از روش‌های مختلفی مانند حریم خصوصی تفاضلی و رمزنگاری هوموفیک برای محافظت از داده‌ها در برابر دسترسی‌های غیرمجاز استفاده کرد؛ همچنین برای تضمین امنیت‌داده‌ها و ارتقای کارایی رمزنگاری، استفاده از رمزنگاری مبتنی بر سخت‌افزار نیز باید مورد توجه قرارگیرد. برخی پژوهش‌گران در حال بررسی ادغام فناوری‌های نوظهور امنیتی مانند بلاک‌چین با یادگیری مشارکتی برای تضمین امنیت یادگیری بین دامنه‌ای در یادگیری مشارکتی هستند.

با افزایش مقیاس یادگیری مشارکتی، تنوع و تعداد حملات بالقوه افزایش قابل توجهی می‌یابد و هنوز مشخص نیست که مشارکت گستردهٔ مشتری در یادگیری مشارکتی می‌تواند امنیت پایدار را در بلندمدت حفظ کند. از آنجا که مشتری‌ها در یادگیری مشارکتی پارامترها را آپلود می‌کنند، شناسایی مستقیم مشتری‌های مخرب برای سرور چالش‌برانگیز است؛ بنابراین، استفاده از اطلاعات تکمیلی از منابع خارجی علاوه بر اطلاعات آماری موجود در مدل‌های یادگیری مشتری ضروری است. این اطلاعات می‌تواند به توسعه‌دهندگان یادگیری مشارکتی در طراحی روش‌های دفاعی کارآمدتر و شناسایی دقیق‌تر حملات و نفوذهای پیچیده کمک کند. با وجود پیشرفت‌هایی در زمینهٔ امنیت یادگیری مشارکتی، همچنان چالش‌های متعددی باقی است. پژوهش‌های بیشتر برای توسعهٔ روش‌های امن و کارآمدتر برای یادگیری مشارکتی ضروری است تا این فناوری بتواند کامل پتانسیل خود را نشان‌دهد.

۵-۲-پژوهش‌ها بر روی الگوریتم‌های کارآمدتر یادگیری مشارکتی

با افزایش حجم داده‌ها و پیچیدگی مدل‌های یادگیری ماشین، تقاضا برای افزایش توان محاسباتی و پهنای باند ارتباطی بین دستگاه‌ها در حال افزایش است. در الگوریتم‌های سنتی یادگیری مشارکتی، تمرکز اصلی بر روی دستیابی به هم‌گرایی مدل جهانی بوده‌است. این امر مستلزم تبادل مکرر مدل بین دستگاه‌ها و سرور مرکزی است که منجر به افزایش ترافیک شبکه و هزینه‌های ارتباطی می‌شود[۱۹۰]. محدودیت‌های منابع ارتباطی مانند پهنای باند شبکه، هزینه‌های ارتباطی و توزیع ناعادلانهٔ منافع آموزش، چالش‌های دیگری را برای یادگیری مشارکتی ایجاد می‌کند؛ همچنین یافتن تعادل بین کارایی و دقت در مدل‌های یادگیری مشارکتی نیز چالش‌برانگیز است. از روش‌های مختلف مانند نمونه‌گیری تصادفی، فشرده‌سازی داده‌ها و یادگیری تقویتی عمیق می‌توان برای افزایش کارایی مدل‌ها بدون افت دقت آن‌ها استفاده کرد.

نبود توافق دربارهٔ اندازه و کیفیت داده‌ها نیز یکی از چالش‌های اساسی است که برای انجام پژوهش‌های کارآمد در این حوزه باید مورد توجه قرارگیرد. اندازه و کیفیت داده‌ها می‌تواند بر کیفیت و دقت مدل‌های یادگیری مشارکتی تأثیر به‌سزایی داشته باشد؛ لذا، استفاده از روش‌های بهبود کیفیت‌داده و توسعهٔ فرایندهای استاندارد برای اندازه‌گیری و ارزیابی دقیق داده‌ها، دارای اهمیت بسیاری است.

سازوکار سنتی یادگیری مشارکتی در زمینهٔ توزیع عادلانهٔ منافع مرتبط با آموزش مدل ناکارآمد است؛ زیرا تمام شرکت‌کنندگان مدل یکسانی را دریافت می‌کنند. این امر نیاز به ایجاد انگیزه برای شرکت‌کنندگان را نادیده می‌گیرد و مانع از توسعهٔ پایدار سیستم یادگیری مشارکتی می‌شود. این ملاحظات به‌تدریج منجر به طراحی الگوریتم‌های یادگیری مشارکتی کارآمدتر و جامع‌تر در پاسخ به چالش‌های دنیای واقعی شده است. در پیاده‌سازی یادگیری مشارکتی، اهداف بهینه‌سازی و روش‌های آموزشی باید با توجه به محدودیت‌های منابع تنظیم شوند؛ همچنین، مطالعات بیشتر در زمینهٔ ادغام الگوریتم‌های یادگیری مشارکتی با روش‌های آموزشی و سازوکارهای جمع‌آوری داده‌ها برای بهینه‌سازی چارچوب یادگیری مشارکتی و ارتقای کارایی، کاهش هزینه‌ها و توزیع عادلانهٔ منافع آموزش مدل ضروری است.

۵-۳-اهمیت و چالش‌های انتخاب مشتری مناسب در یادگیری مشارکتی در مقیاس بزرگ

پیاده‌سازی یادگیری مشارکتی در مقیاس بزرگ چالش‌برانگیز است و نیاز به زیرساخت‌های مناسب برای تبادل‌داده‌ها و مدل‌ها بین عوامل مختلف دارد؛ در این راستا، انتخاب مشتری مناسب نقشی حیاتی در ارتقای عملکرد مدل جهانی ایفا می‌کند. کیفیت و اعتبار داده‌های مشتریان، منابع آموزشی در دسترس و مصرف انرژی، از

[DOI: 10.61186/jsdp.21.3.23]

جمله عواملی هستند که بر عملکرد کلی مدل تأثیر قابل توجهی می‌گذارند[۱۹۱]. ماهیت سیار و پویای محیط شبکه و موقعیت مکانی مشتریان در یادگیری مشارکتی، که اغلب از دستگاه‌های هوشمند استفاده می‌کنند، چالش‌هایی را در زمینهٔ پایداری بازدهی آموزش این سیستم ایجاد می‌کند.

با گسترش کاربردهای یادگیری مشارکتی در مقیاس بزرگ، شاهد افزایش تصاعدی تعداد مشتریان سیار شرکت‌کننده در این فرایند هستیم. انتخاب مشتری مناسب نقشی اساسی در ارتقای عملکرد مدل‌های یادگیری مشارکتی در مقیاس بزرگ ایفا می‌کند؛ بااین‌حال، ماهیت پویای یادگیری مشارکتی، انتخاب مشتری را به یک مسئلهٔ زمان‌بندی پویا تبدیل می‌کند که در هر دور ارتباط باید انجام شود[۱۹۲]. این امر ضرورت توسعهٔ روشی کارآمد برای انتخاب مشتریان باکیفیت [۱۹۳، ۱۹۴] و عملکرد پایدار [۱۹۵] در محیط پیچیدهٔ یادگیری مشارکتی را دو چندان می‌کند. انتخاب مشتری مناسب ضمن درنظرگرفتن کارایی استراتژی زمان‌بندی، به برقراری تعادل بهتر بین معیارهای انتخاب مانند کیفیت‌داده، مصرف انرژی و انگیزهٔ مشتریان کمک می‌کند؛ بنابراین، طراحی یک طرح انتخاب پویای مشتری کارآمد که به‌طور پویا مشتریان باکیفیت را از میان تعداد زیادی از مشتریان برای بهینه‌سازی مدل جهانی و ارتقای استحکام یادگیری مشارکتی انتخاب کند، به موضوع چالش‌برانگیز و مورد توجه بسیاری از پژوهش‌گران تبدیل شده‌است.

۵-۴-پژوهش بر روی روش‌های جدید ترکیب مدل در یادگیری مشارکتی چندوجهی[1]

با توجه به تنوع و ناهمگنی داده‌های دستگاه‌های سازمانی در حوزه‌های مختلف، مشتریان در یادگیری مشارکتی می‌توانند اشکال مختلفی از داده‌ها را از جمله تصاویر، صدا، متن و غیره ارائه دهند که به این داده‌ها، داده‌های چندوجهی گفته می‌شود. تنوع داده‌ها ایجاب می‌کند که مشتریان برای انجام وظایف شخصی‌سازی‌شده، مدل‌های محلی متفاوتی را آموزش دهند. ادغام مستقیم مدل‌های چندوجهی مختلف به‌وسیلهٔ سرور در فرایند یادگیری مشارکتی به‌دلیل ناهمگنی داده‌ها دشوار است.

بر این اساس در یادگیری مشارکتی چندوجهی، استخراج دانش از داده‌های چندوجهی، ادغام مدل‌های محلی متنوع و ارتقای عملکرد کلی مدل‌های یادگیری مشارکتی، از چالش‌های کلیدی و حوزه‌های پژوهشی فعال محسوب می‌شود.

۵-۵-گسترش پژوهش در زمینهٔ کاربرد یادگیری مشارکتی در حوزه‌های مختلف

رشد و توسعهٔ یادگیری مشارکتی در سه مرحله خلاصه می‌شود: حفظ حریم خصوصی سنتی، مدل یادگیری مشارکتی بر پایهٔ حفظ حریم خصوصی و مدل یادگیری مشارکتی امن با تمرکز بر حفظ حریم خصوصی. الگوریتم‌های یادگیری ماشینی متعددی که مورد استفادهٔ گسترده قرار می‌گیرند، می‌توانند از روش یادگیری مشارکتی برای آموزش مدل‌ها بهره‌مند شوند؛ این روش از منابع داده‌ای ساختاریافته، متنی، تصویری و انواع دیگر داده‌ها پشتیبانی می‌کند و در دسته‌بندی نمونه‌ها، برنامه‌ریزی مسیر [۱۹۶]، پیش‌بینی رگرسیونی، تشخیص تصویر [۱۹۷، ۱۹۸]، تجزیه و تحلیل ژن، پردازش زبان طبیعی و سایر وظایف به‌کار گرفته شود.

در سال‌های اخیر، یادگیری مشارکتی در حوزه‌های مراقبت‌های بهداشتی و سلامت، امور مالی، اینترنت اشیا و خدمات شهری که نیازمند الزامات سخت‌گیرانه‌ای برای حفظ حریم خصوصی‌اند، نقش مهمی ایفا کرده‌است. با توجه به ویژگی‌های رویکرد یادگیری توزیع‌شده در یادگیری مشارکتی، این روش در کاهش فشار ذخیره‌سازی و محاسباتی روی سرور مرکزی، تنظیم ساختار توزیع‌داده و بهینه‌سازی حالت آموزش فدرال نیز نقشی برجسته دارد.

علاوه‌بر ترویج همکاری بین مناطق و حوزه‌های مختلف و پیشبرد بیشتر توسعهٔ تجاری، پژوهش‌گران باید به کاربرد یادگیری مشارکتی در آموزش و پرورش، دولت الکترونیک، هواشناسی، زغال‌سنگ [۱۹۹]، توزیع برق [۲۰۰] و سایر حوزه‌ها نیز توجه کنند؛ برای مثال، در زمینهٔ آموزش و پرورش با توجه به انباشت حجم عظیمی از داده‌ها در پژوهش‌های سلامت جسمی و روانی دانش‌آموزان، می‌توان یک پلتفرم اشتراک‌گذاری اطلاعات دانش‌آموزی چندمنبعی ایجاد کرد و با تضمین حریم خصوصی منبع داده، ارزش اشتراک داده را محقق کرد. در این چارچوب، یادگیری مشارکتی به راه حلی ارزشمند تبدیل می‌شود؛ همچنین در زمینهٔ دولت الکترونیک در فرایند کار با داده‌های دولتی، بسیاری از ادارات دولتی به‌دلیل فقدان طرح تأیید حق مالکیت

[1] Multi-modal Federated Learning

[DOI: 10.61186/jsdp.21.3.23]

دارایی داده‌های معتبر، از به اشتراک‌گذاری داده‌های شخصی خودداری می‌کنند. در چنین شرایطی، یادگیری مشارکتی را می‌توان با اجزای توسعهٔ کلان‌داده ادغام کرد تا جزیره‌ای‌بودن داده‌های ادارات دولتی را حل کرد و به اشتراک‌گذاری ایمن و بین دپارتمانی داده‌های دولتی و اجتماعی دست یافت و خطر افشای داده را به‌طور مؤثر کاهش داد.

در حال حاضر، یادگیری مشارکتی چشم‌انداز کاربردی امیدوارکننده‌ای دارد؛ بااین‌حال، به‌کارگیری این فناوری در حوزه‌های بیشتر، همچنان عرصه‌ای به‌طورکامل ناشناخته است. برای بهره‌مندی از یادگیری مشارکتی در تمام جنبه‌های زندگی روزمرهٔ مردم و کاهش خطر افشای اطلاعات شخصی در عصر کلان‌داده، نیاز به کاوش و توسعهٔ بیشتر این فناوری وجود دارد[۲۰۱].

در سال‌های اخیر، حجم مقالات منتشرشده در حوزهٔ یادگیری مشارکتی افزایش تصاعدی یافته، که نشان‌دهندهٔ توجه روزافزون به اهمیت حفظ حریم خصوصی است. یادگیری مشارکتی به‌عنوان رویکردی برای حفظ امنیت در یادگیری ماشین سنتی، می‌تواند بهره‌وری از کلان‌داده را به‌طور کامل به ارمغان آورد و مسئلهٔ حفظ حریم خصوصی را مرتفع سازد؛ بااین‌حال، با توجه به نیازهای کاربردی گوناگون در محیط‌های واقعی پیچیده و محدودیت‌های موجود در یادگیری مشارکتی، بهینه‌سازی پویای فرایند یادگیری در یادگیری مشارکتی با درنظرگرفتن اهداف و محدودیت‌ها ضروری است. رویکرد یادگیری مشارکتی می‌تواند راه حلی عملی برای دیگر حوزه‌های پژوهشی، نه صرفاً حوزهٔ یادگیری ماشین ارائه دهد.

۶- جمع‌بندی و نتیجه‌گیری

یادگیری مشارکتی، به‌عنوان رویکردی نوین در هوش مصنوعی توزیع‌شده، یکی از راه حل‌های مهم و در حال توسعه برای حفظ حریم خصوصی است؛ در این رویکرد، چندین عامل با یکدیگر همکاری می‌کنند تا بدون نیاز به اشتراک‌گذاری مستقیم داده‌ها، مدل‌های یادگیری ماشین را آموزش دهند. پژوهش‌گران در زمینهٔ یادگیری مشارکتی از درک عمیق مبانی نظری و ساختاری این فناوری تا توسعهٔ روش‌ها و استراتژی‌های نوآورانه برای غلبه بر چالش‌های پیش‌رو، پژوهش‌های گسترده‌ای را در شاخه‌های مختلف یادگیری مشارکتی انجام داده‌اند و دستاوردهای قابل توجهی را در هر یک از این حوزه‌ها کسب کرده‌اند؛ این تلاش‌ها منجر به درک عمیق‌تر یادگیری مشارکتی توسط پژوهش‌گران شده است و آن‌ها را قادر می‌سازد تا به‌دنبال ادغام کامل رویکرد یادگیری مشارکتی با طیف وسیعی از کاربردها باشند.

این مقاله ضمن معرفی مفاهیم اساسی یادگیری مشارکتی و مروری بر کاربردهای آن در زمینه‌های مختلف، با بررسی دستاوردهای اخیر پژوهشی در حوزهٔ یادگیری مشارکتی گامی مهم در جهت معرفی نظام‌مند مفهوم این فناوری، چالش‌های پیش‌روی توسعهٔ آن و جهت‌گیری‌های پژوهشی برای ادغام یادگیری مشارکتی باکاربردهای مختلف برداشته‌است. برپایهٔ این بررسی، تفکری عمیق و تحلیلی در مورد مسیر پیش‌روی توسعهٔ یادگیری مشارکتی و موانعی که باید برطرف شوند، ارائه شده‌است. انتظار می‌رود این پژوهش به پژوهش‌گران حوزهٔ یادگیری مشارکتی در درک روند توسعه و وضعیت فعلی پژوهش‌های در این زمینه یاری رساند و زمینه‌ای مساعد برای پیشرفت این فناوری فراهم کند. تحلیل جامع مبانی، کاربردها و چالش‌های یادگیری مشارکتی در این مقاله نشان می‌دهد که این رویکرد به‌عنوان یکی از مهم‌ترین و کاربردی‌ترین حوزه‌های نوین هوش مصنوعی، پتانسیل لازم برای حل چالش‌های مختلف در حوزه‌های گوناگون را داراست و پیش‌بینی می‌شود که پژوهش‌های در حوزهٔ یادگیری مشارکتی برای حداقل یک دهه دیگر ادامه یابد؛ زیرا هنوز موانع اساسی متعددی وجود دارد که باید برطرف شوند. مطالعات نشان می‌دهد که تمرکز پژوهش‌های آتی در این حوزه بر روی سازوکارهای حفظ حریم خصوصی و امنیت داده‌ها، الگوهای همکاری، توزیع عادلانهٔ منافع بین ذی‌نفعان در آموزش و روش‌های شخصی‌سازی یادگیری مشارکتی خواهد بود تا زمینهٔ به‌کارگیری گسترده‌تر این فناوری در حوزه‌های مختلف فراهم شود.

[DOI: 10.61186/jsdp.21.3.23]

(جدول-۳): منابع بررسی‌شده در این پژوهش

(Table-2): Sources reviewed in this study

ردیف	عنوان مقاله/کتاب	محتوا	زمینه	نویسندگان	سال انتشار
۱	Fusion of Federated Learning and Industrial Internet of Things: A Survey [۵۸]	بررسی ادغام اینترنت اشیا صنعتی (IIoT) و یادگیری مشارکتی جهت حفظ حریم خصوصی داده‌ها و بهره‌گیری از توانمندی‌های یادگیری ماشین، یادگیری عمیق و تکنیک‌های بلاک‌چین برای یادگیری مشارکتی در IIoT امن. تجزیه و تحلیل روش‌های مقابله با چالش‌های داده‌های ناهمگن و حجیم. ارائهٔ برنامه‌های کاربردی IIoT با یادگیری مشارکتی در حوزه‌های سلامت و صنعت خودرو برای ارتقای امنیت‌داده‌ها و افزایش کارایی سیستم‌ها.	یادگیری مشارکتی و اینترنت اشیا	Parimala M, et al	۲۰۲۱
۲	Applications of Federated Learning in Smart Cities: Recent Advances, Taxonomy, and Open Challenges [۱۲]	بررسی پیشرفت‌های فعلی یادگیری مشارکتی به‌عنوان ابزاری قدرتمند و چندحوزه‌ای در زمینه‌هایی مانند اینترنت اشیا، شهر هوشمند، حمل‌ونقل، ارتباطات، امور مالی و پزشکی.	یادگیری مشارکتی و شهر هوشمند	Zhaohua Zheng et al	۲۰۲۱
۳	Achieving Security and Privacy in Federated Learning Systems: Survey, Research Challenges and Future Directions [۱]	بررسی حملات امنیتی و چالش‌های حفظ حریم خصوصی در یادگیری مشارکتی و ارائهٔ راهکارهایی برای مقابله با این مشکل و دستیابی به امنیت و حریم خصوصی.	امنیت و حفظ حریم خصوصی در یادگیری مشارکتی	Alberto Blanco-Justiciaa et al	۲۰۲۰
۴	A Survey of Federated Learning for Edge Computing: Research Problems and Solutions [۵۹]	ارائهٔ یک رویکرد جدید مبتنی بر یادگیری مشارکتی در برنامه‌های محاسبات لبه، ابزارهای توسعه، کارایی ارتباطات، امنیت و حریم خصوصی.	یادگیری مشارکتی برای محاسبهٔ لبه	Qi Xia et al	۲۰۲۱
۵	A review of applications in federated learning [4]	بررسی جامع کاربردهای رایج یادگیری مشارکتی در مهندسی صنایع و علوم رایانه و زمینه‌های کاربردی.	کاربردهای یادگیری مشارکتی	Li Li bet al	۲۰۲۰
۶	A Systematic Literature Review on Federated Machine Learning: From A Software Engineering Perspective [۶۰]	یک بررسی سازمان‌یافته دربارهٔ مفهوم یادگیری مشارکتی، چالش‌های پژوهش و راه‌حل‌ها از دیدگاه مهندسی نرم‌افزار.	مفهوم یادگیری مشارکتی	SIN KIT LO, et al	۲۰۲۰
۷	A Review of Privacy-preserving Federated Learning for the Internet-of-Things [۶۱]	بررسی حفظ حریم خصوصی در یادگیری مشارکتی و برنامه‌های کاربردی اینترنت اشیا.	یادگیری مشارکتی و اینترنت اشیا	Christopher Briggs et al	۲۰۲۰
۸	A Systematic Literature Review on Federated Learning: From A Model Quality Perspective [۶۲]	بررسی و تحلیل سیستماتیک رویکردهای بهبود کیفیت مدل‌های یادگیری مشارکتی.	مفهوم یادگیری مشارکتی	Yi Liu et al	۲۰۲۰
۹	Threats to Federated Learning: A Survey [۶۳]	بررسی حمله‌های مسمومیت (Poisoning) و استنباط (inference) و چالش‌های مختلف حفظ حریم خصوصی در یادگیری مشارکتی	چالش‌های یادگیری مشارکتی	Lingjuan Lyu1 et al	۲۰۲۰
۱۰	Federated Learning in Mobile Edge Networks: A Comprehensive Survey [۶۴]	بررسی تلفیق یادگیری مشارکتی و محاسبات لبه‌ای، بحث در مورد چالش‌های اجرای یادگیری مشارکتی در بهینه‌سازی شبکهٔ لبه.	شبکه‌های یادگیری مشارکتی و لبهٔ تلفن همراه	Wei Yang et al	۲۰۲۰
۱۱	Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications [۶۵]	بررسی سخت‌افزارها، نرم‌افزارها، سیستم‌عامل‌ها و پروتکل‌های یادگیری مشارکتی همراه با بحث در مورد مراقبت‌های بهداشتی مبتنی بر یادگیری مشارکتی.	مفهوم یادگیری مشارکتی	Mohammed Aledhari, et al	۲۰۲۰
۱۲	Federated Machine Learning: Concept and Applications [۳]	بررسی مفهوم یادگیری مشارکتی با مقدمه‌ای کامل در تعریف مفاهیم، معماری‌ها و کاربردهای آن.	مفهوم یادگیری مشارکتی	QIANG YANG et al	۲۰۱۹
۱۳	A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection [۶۶]	بررسی اجزای سیستم یادگیری مشارکتی، مانند توزیع داده‌ها، مدل یادگیری ماشین، مکانیزم حفظ حریم خصوصی و معماری ارتباطات.	مفهوم یادگیری مشارکتی	Qinbin Li1et al	۲۰۲۱

[DOI: 10.61186/jsdp.21.3.23]

ردیف	عنوان مقاله/کتاب	محتوا	زمینه	نویسندگان	سال انتشار
۱۴	A Survey on Security and Privacy of Federated Learning [۶۷]	بررسی کاربردهای یادگیری مشارکتی در زمینه‌های مختلف از جمله مهندسی صنایع و علوم رایانه.	کاربردهای یادگیری مشارکتی	Viraaji Mothukuria et al	۲۰۲۱
۱۵	Federated Learning: Challenges, Methods, and Future Directions [۹]	بررسی ویژگی‌ها، چالش‌ها و چشم‌اندازهای یادگیری مشارکتی.	چالش‌های یادگیری مشارکتی	Tian Li et al	۲۰۲۰
۱۶	From federated learning to federated neural architecture search: a survey [۶۸]	بررسی مفاهیم یادگیری مشارکتی و رویکردهای جست‌وجوی معماری عصبی بر اساس یادگیری تقویتی، الگوریتم‌های تکاملی و مبتنی بر شیب توصیفی این معماری عصبی متحد، به‌صورت آنلاین و آفلاین، در طبقه‌بندی پیاده‌سازی می‌شود و رویکردهای جست‌وجوی تک و چندهدفه نیز مورد بررسی قرار می‌گیرد.	مفهوم یادگیری مشارکتی	Hangyu Zhu et al	۲۰۲۱
۱۷	Survey of Personalization Techniques for Federated Learning [۶۹]	بررسی ضرورت شخصی‌سازی و تکنیک‌های شخصی‌سازی مدل‌های جهانی در یادگیری مشارکتی برای بهبود کارکرد مدل.	شخصی‌سازی در یادگیری مشارکتی	Viraj Kulkarni et al	۲۰۲۰
۱۸	Towards Utilizing Unlabeled Data in Federated Learning: A Survey and Prospective [۷۰]	بررسی و شناسایی نیاز به بهره‌برداری از داده‌های بدون برچسب در یادگیری مشارکتی.	داده‌های بدون برچسب در یادگیری مشارکتی	Yilun Jin1 et al	۲۰۲۰
۱۹	(Book) Federated Learning Synthesis Lectures on Artificial Intelligence and Machine Learning [۴۱]	بررسی چگونگی ساخت مدل پیش‌بینی مشترک با حفظ حریم خصوصی داده‌ها در یادگیری مشارکتی و بررسی انواع راه‌حل‌های حفظ حریم خصوصی داده‌ها.	مفهوم یادگیری مشارکتی	Qiang Yang et al	۲۰۱۹
۲۰	Federated Learning for Internet of Things: A Comprehensive Survey [۷۱]	نقش یادگیری مشارکتی در خدمات مختلف اینترنت اشیا، شامل: به اشتراک‌گذاری داده‌های اینترنت اشیا، تخلیه و ذخیره‌سازی داده‌ها، شناسایی حمله، بومی‌سازی، و حریم خصوصی و امنیت اینترنت اشیا.	یادگیری مشارکتی و اینترنت اشیا	Dinh C. et al	۲۰۲۱
۲۱	Federated Learning for Vehicular Internet of Things: Recent Advances and Open Issues [۷۲]	بررسی پیشرفت یادگیری مشارکتی و کاربرد آن در شبکه‌های وسایل نقلیه.	شبکه‌های یادگیری مشارکتی و وسایل نقلیه	Zhaoyang Du, et al	۲۰۲۰
۲۲	Federated Learning: Opportunities and Challenges [۷۳]	بررسی حفظ حریم خصوصی داده‌های محلی، فرصت‌ها و چالش‌های یادگیری مشارکتی.	چالش‌های یادگیری مشارکتی	Priyanka Mary Mammen	۲۰۲۱
۲۳	From Distributed Machine Learning to Federated Learning: A Survey [۷۴]	بررسی راهکارهای یادگیری توزیع‌شده، ارتباط داده‌ها و امنیت سیستم‌های یادگیری مشارکتی.	داده‌ها و منابع محاسباتی در یادگیری مشارکتی	Ji Liuz, Jizhou Huangz et al	۲۰۲۱
۲۴	Review Federated Learning in Smart City Sensing: Challenges and Opportunities [۷۵]	مروری بر پتانسیل یادگیری مشارکتی در شهرهای هوشمند اینترنت اشیای و چالش‌های آن.	یادگیری مشارکتی و شهر هوشمند	Ji Chu Jiang, et al	۲۰۲۰
۲۵	Emerging Trends in Federated Learning: From Model Fusion to Federated X Learning [۷۶]	بررسی یادگیری مشارکتی با سایر الگوهای یادگیری، یادگیری مشارکتی x، یادگیری چندوظیفه‌ای، فراگیری، یادگیری انتقال، یادگیری بدون نظارت و یادگیری تقویتی.	روندهای نوظهور در یادگیری مشارکتی	Shaoxiong Ji1, et al	۲۰۲۱ latest version ۲۰۲۱
۲۶	(Book) Federated Learning Privacy and Incentive [۷۷]	بررسی تکنیک‌های مربوط به حفظ حریم خصوصی داده‌ها و کاربردهای یادگیری مشارکتی.	یادگیری مشارکتی و حریم خصوصی داده‌ها	Randy Goebel, et al	۲۰۲۰
۲۷	communication-efficient and distributed learning over wireless networks: Principles and applications [۷۸]	بررسی در مورد معماری‌ها، الگوریتم‌ها و روش‌های پردازش داده‌ها در شبکه‌های بی‌سیم مبتنی بر یادگیری مشارکتی.	مفهوم یادگیری مشارکتی	Park J, Samarakoon S, et al	۲۰۲۰
۲۸	Preserving data privacy via federated learning: Challenges and solutions [۷۹]	مروری کوتاه بر چالش‌ها و حملات حریم خصوصی داده‌ها در سیستم‌های یادگیری مشارکتی، همراه با راه‌حل‌های احتمالی برای محافظت از حریم خصوصی داده‌ها در طرح‌های یادگیری مشارکتی.	یادگیری مشارکتی و حریم خصوصی داده‌ها	Li Z, et al	۲۰۲۰

[DOI: 10.61186/jsdp.21.3.23]

(جدول-۴): برنامهٔ کاربردی برای اینترنت اشیا، خانه‌های هوشمند و دستگاه‌های تلفن همراه

(Table 4): Application for the Internet of Things, smart homes and mobile devices

زمینه	محدودیت	مزایا	مطالعات	زمینهٔ کاربرد	مرجع
برنامه‌های کاربردی در دستگاه‌های تلفن همراه	به‌طورکامل به حالت احتمالی آموخته‌شده تکیه می‌کند.	گسترش واژگان صفحه کلید بدون صدا باعث بهبود کارایی و تنوع محتوا می‌شود.	یادگیری کلمات خارج از واژگان.	صفحه‌کلید تلفن هوشمند.	Chen et al., 2019 [۸۰]
	مدل در مقابل نوفهٔ پس‌زمینه مقاومت ندارد.	استفاده از یک استراتژی میانگین انطباقی با وزن در مدل استاندارد.	یادگیری آشکارساز کلمات تعبیه‌شده.	دستیار صوتی تلفن هوشمند.	Leroy et al., 2019 [۱۱۴]
	هزینهٔ ارتباطی بالایی دارد.	استفاده از مدل RNN در سرور و محیط‌های مشارکتی با بهبود فراخوانی.	پیش‌بینی کلمهٔ بعدی در صفحه‌کلید مجازی.	صفحه‌کلید تلفن هوشمند.	Hard et al.2019 [۱۱۵]
	غیرمعمول است که مدل‌ها با تعداد زیادی پارامتر آموزش داده شوند.	آموزش راحت با استفاده از تحدب تابع خطا و مدل رگرسیون لجستیک.	بهبود کیفیت پیشنهادات جست‌وجوی صفحه‌کلید مجازی.	صفحه‌کلید تلفن هوشمند.	Yang, Andrew, et al, 2018[۹۵]
	محتوای حافظهٔ پنهان مشتری متفاوت است و معیارها را نمی‌توان در آزمایشات مقایسه کرد.	دستیابی به عملکرد بهتر از یک مدل آموزش‌دیدهٔ سرور.	پیش‌بینی ایموجی از متن تایپ‌شده روی صفحه‌کلید.	صفحه‌کلید تلفن هوشمند.	Ramaswamy et al. 2019 [۱۱۶]
	نحوهٔ توزیع بار محاسباتی عظیم در سناریوهای ناهمگن کشف نشده‌است.	بحث دربارهٔ پتانسیل یکپارچه‌سازی یادگیری تقویتی عمیق و یادگیری مشارکتی با سیستم لبهٔ تلفن همراه.	بهینه‌سازیMEC، حافظهٔ پنهان و ارتباطات	محاسبات لبهٔ تلفن همراه.	Wang, X. et al. 2019 [۱۱۷]
	برای چندین ابر لبه قابل استفاده نیست.	پیشنهاد طرح استقرار سرویس آگاهی از حریم خصوصی (PSP) برای پاسخ‌گویی به خواسته‌های خدمات کاربران.	قراردادن خدمات آگاهانهٔ حفظ حریم خصوصی برای محاسبات لبهٔ تلفن همراه.	محاسبات لبهٔ تلفن همراه. رایانش لبه‌ای.	Qian et al., 2019 [۱۱۸]
	فقط مدل تحرک اساسی را برای سادگی درنظرمی‌گیرد.	کاهش تنزل عملکرد با استفاده از استراتژی بهینه‌سازی گروه.	حفظ حریم خصوصی در پیش‌بینی تحرک انسانی.	حس‌گرهای حرکتی دستگاه‌های تلفن همراه.	Feng et al. 2020 [۱۱۹]
	تولید مدل‌هایی با دقت کمی بدتر در مقایسه با مدل‌های متمرکز.	شناسایی و ردکردن مشتری‌های اشتباه.	شناخت فعالیت‌های انسانی.	حس‌گرهای حرکتی دستگاه‌های هوشمند.	Sozinov et al., 2018[۱۲۰]
	نسبتاً معماری پیچیده‌ای برای پیاده‌سازی دارد.	ترکیب یادگیری امن مشارکتی با تجمیع داده‌های امن.	طراحی خانه‌های هوشمند مبتنی بر یادگیری امن مشارکتی.	خانهٔ هوشمند IOT[1]	Aïvodji et al., 2019[۱۲۱]
	با مکانیسم نقشه‌برداری برای استقرار متنوع انعطاف‌پذیر نیست.	شناسایی مؤثر خطرات فیزیکی.	یادگیری الگوهای رفتاری کاربران.	خانهٔ هوشمندIOT	Yu et al., 2020 [۱۲۲]
	نیاز به کار بیشتر در مورد توجیه هم‌گرایی فرایند هم‌جوشی است.	افزایش بهره‌وری یادگیری تقلیدی از ربات‌های محلی در سیستم‌های رباتیک ابر.	ربات یادگیری تقلید.	شبکهٔ ربات	Liu et al., 2020 [۵۳]

[1] Internet of things (IOT)

[DOI: 10.61186/jsdp.21.3.23]

(جدول-۵): بررسی اجمالی مطالعات اخیر در مورد FL با امنیت IIOT.

(Table-5): An overview of recent studies on FL with IIOT security.

چارچوب	الگوریتم	کاربرد	تکنیک	چالش‌های محدودیت
FML in IIoT [۱۰۰, ۱۰۱, ۱۲۳-۱۲۴]	FTM[1]	کارخانه‌های هوشمند	FTM با رمزگذاری هومومورفیک که از تحول خطی استفاده می‌کند.	چالش برای حفظ تعادل بین یادگیری ماشین و امنیت‌داده‌ها. نیاز به سرور متمرکز برای استخراج مشارکتی.
	Primalchain	پردازش زبان طبیعی و تشخیص گفتار	حریم خصوصی تفاضلی یا افتراقی[2]	تأخیر در مقیاس بزرگ یادگیری ماشین بیشتر است. کارایی را می‌توان بهبود بخشید.
	Tensor Ridge Regression	پردازش تصویر	تجزیهٔ عامل موازی	مجموعه‌داده‌های دارای بُعد بالا منجر به آموزش بیش‌ازحد، پیچیدگی محاسباتی بالا و نیاز به حافظهٔ بزرگ می‌شود.
	STA	بینایی کامپیوتر و تشخیص الگو	تکنیک هم‌ترازی Tensor	روش‌های یادگیری تنک برای تشخیص تانسور موردبررسی قرارنمی‌گیرند و برای فضای دارای بعد بالا کارآمد نیستند.
	CPSS	اینترنت اشیا بی‌سیم	حفظ حریم خصوصی معیار مبتنی بر تجزیه	از آنجاکه از داده‌های رمزگذاری‌شده استفاده می‌کند، هزینهٔ بسیار بالایی دارد.
FDL in IIoT [۵۶, ۱۲۶-۱۲۸]	DeepPAR DeepDPA	کارخانه‌های هوشمند	رمزگذاری مجدد پروکسی گروه مدیریت کلید پویا	نقص در مکانیسم امنیتی در دستگاه لبه.
	Double Q-Deep Qnetwork	شبکه‌های تلفن همراه	فرایند تصمیم‌گیری مارکوف در حافظهٔ پنهان سازمانی غیرمتمرکز	زیان غیرمتمرکز را به حداکثر می‌رساند.
	FedGRU	شبکهٔ ترافیک	جمع پارامترها الگوریتم میانگین مشارکتی پروتکل اعلامیهٔ مشترک	با استفاده از شبکهٔ کانولوشن گراف می‌توان وابستگی زمانی را بهتر به‌دست آورد.
	ASTW FedAVG	پردازش تصویر	استراتژی ناهم‌زمان جمع وزنی	فقط سرور در توسعهٔ مدل محلی نقش دارد. هزینهٔ ارتباطات را می‌توان کاهش داد.
Federated Blockchain [۱۰۹, ۱۱۱-۱۱۳, ۱۲۹-۱۳۱]	Federated Collaboration framework	داده‌های حس‌گر پوشیدنی	بلاک‌چین مرکز دادهٔ خصوصی و عمومی	چالش‌های مقیاس بزرگ همکاری چندجانبه و امن داده‌های اینترنت اشیا دارد.
	BlockFL	شبکهٔ ارتباط بی‌سیم	در دستگاه یادگیری ماشین سازوکار اجماع هوشمند	امکان هک مدارک کار به‌وسیلهٔ ماینرهای مخرب دارد.
	FL-Block	پردازش تصویر	حریم خصوصی غیرمتمرکز حملهٔ مسمومیت	مبادلات بین حفظ حریم خصوصی و کارایی باید بهینه شود.
	BFL	شبکهٔ وسایل نقلیه	رویکرد تجدید پاداش VML	افزایش تأخیر کلی در انتخاب به‌روزرسانی‌های بلوک.
	CrowdSFL	صنعت بهداشت	الگوریتم رمزگذاری منبع انبوه	نیاز به تعریف مکانیسم توزیع پاداش. مدل را می‌توان بهینه کرد.
	SVM and Deep network	شبکهٔ راه‌آهن	SVM بر اساس عملکرد هستهٔ مخلوط و مدل چندکلاسه	دقت و کارایی پیش‌بینی می‌تواند به حداکثر برسد.
	IoBT	امنیت اجتماعی از طریق سازمان دفاعی	مدل چندلایه دفاع به رهبری نبرد	مشارکت گره محلی در روند آموزش می‌تواند بر اساس سهم آن‌ها پاداش یابد.

[1] Federated Tensor Mining (FTM)

[2] Differential Privacy (DP)

[DOI: 10.61186/jsdp.21.3.23]

(جدول-۶): خلاصه مقاله‌های اخیر یادگیری مشارکتی در IIOT برای ذخیره‌سازی داده‌ها[1] - مدیریت داده‌ها [2]- مدیریت منابع[3]

(Table-6): Summary of Recent FL Research Articles in IIOT for Data Storage - Data Management - Resource Management

چارچوب	زمینهٔ پژوهش	تکنیک‌های مورد استفاده	مشارکت‌ها	اثبات مفهوم
ذخیره سازی داده‌ها [۴۲، ۱۳۲-۱۳۸]	ذخیره‌سازی اطلاعات امن. جمع‌آوری داده‌های پویا. کاهش ازدحام. کاهش مصرف انرژی.	راه حل مبتنی بر Middleware در شبکه‌های SDN[4] برای افزایش بهره‌وری و امکانات شبکه. تعامل ابهام برای تفکیک اطلاعات نادرست یا نامشخص، محاسبات ابری، تأخیر سیاست آگاهی.	درخت ویژگی بازیابی طراحی شده است. کاهش فضای ذخیره‌سازی. الگوریتم تکاملی چند هدفه ارائه شده است.	تراکم گاز در کارخانه خدمات و نگهداری مشتری.
	ذخیره‌سازی اطلاعات مؤثر. جمع‌آوری داده‌های حجیم. فراهم‌کردن مدیریت هوشمندانه.	راه حل مبتنی بر SOA [5] سرور پایگاه داده توزیع‌شده. مدل تجمیع داده‌ها.	معماری خدمات FFBF[6] و یک چارچوب IDMS[7] پیشنهاد شده است.	بخش تولید. مراقبت‌های بهداشتی. دستگاه‌های پوشیدنی.
	جمع‌آوری داده‌ها از منابع مختلف، تجمیع و تجزیه و تحلیل داده‌ها.	مدل مرکز رویداد	پیشنهاد یک مدل تجمع داده و همبستگی.	بخش نگهداری. خطوط تولید به‌هم پیوسته.
	رسیدگی به خرابی دستگاه ایجاد رابط برای تبادل اطلاعات و داده‌ها.	راه حل مبتنی بر معماری SDN, CPS[8], DRL[9]	پیشنهاد DRL مبتنی بر بلاک‌چین و CCPSA[10] میزان استفاده از تجهیزات افزایش می‌یابد.	برنامه‌های صنعتی پیچیده. وسایل نقلیهٔ هدایت‌شدهٔ خودکار. ربات‌های صنعتی.
مدیریت داده‌ها [۱۰۹، ۱۱۰، ۱۳۹-۱۴۴]	کاهش حجم دادهٔ بارگذاری‌شده. ارائهٔ اطلاعات به گره‌های لبهٔ تلفن همراه.	یادگیری تقویتی عمیق برای بهینه‌سازی. یادگیری مشارکتی برای ارائهٔ اطلاعات.	ارائهٔ یک چارچوب "In-Edge AI" برای بهبود استقرار. یادگیری Q عمیق برای بهبود محاسبات در لبه‌ها.	اثرات Xender
	ارائهٔ مکانیسم ادغام دانش. ارائهٔ الگویی برای یادگیری انتقال.	یادگیری مشارکتی همراه با یادگیری تقلیدی.	پیشنهاد یک روش یادگیری انتقال با استفاده از یادگیری تقلید مشارکتی (FIL)[11].	اتومبیل‌های خودران
	تأمین امنیت بالاتر در حالی که چندین طرف سعی در همکاری دارند.	یادگیری عمیق و یادگیری مشارکتی همراه با بلاک‌چین.	ارائهٔ یک چارچوب همکاری داده با استفاده از FDL[12]. پیشنهاد مکانیسم امن مبتنی بر بلاک‌چین برای محاسبه.	یک بلاک‌چین خصوصی مبتنی بر پروتکل Libra. داده‌های خام جمع‌آوری‌شده از دستگاه پوشیدنی.
	به اشتراک گذاشتن داده‌ها. در چندین طرف بدون هیچ‌گونه ریزش.	یادگیری مشارکتی و بلاک‌چین.	یادگیری مشارکتی خصوصی افتراقی پیشنهاد شده است.	مجموعه داده‌های رویترز.
	بهینه‌سازی ساختار مدل. به حداقل رساندن هزینه محاسبات. به حداقل رساندن خطاهای آزمون مدل جهانی.	یادگیری مشارکتی و الگوریتم تکاملی چند هدفه.	الگوریتم میانگین مشارکتی پیشنهاد شده است. نسخهٔ اصلاح‌شدهٔ الگوریتم SET پیشنهاد شده است.	مجموعه داده‌های مستقل هم‌توزیع و غیرمستقل هم‌توزیع.
	ایجاد حریم خصوصی بهتر در مدل‌های مشترک.	یادگیری مشارکتی و محاسبات چندجانبه (MPC).	ارائه MPC[13] دو فاز فعال یادگیری مشارکتی پیشنهاد الگوریتم انتخاب کمیته	واحدهای تولیدی تشخیص عیب در ماشین‌های الکتریکی.
	جلوگیری از بهره‌برداری از داده‌های خصوصی در برنامه‌های حساس.	یادگیری مشارکتی همراه با یادگیری افزوده.	پیشنهاد حریم خصوصی افزایش یافته یادگیری مشارکتی برای هوش مصنوعی صنعتی. استفاده از تجزیه و تحلیل تجمع و پیشنهاد الگوریتم تجمع مدل.	مجموعه داده‌های MNIST. بهداشت و درمان و خلبان اتوماتیک.
	ارائهٔ اطلاعات به شبکهٔ لبه. جلوگیری از حملات مخرب.	ارتباطات گسترده، بلاک‌چین همراه با یادگیری تقویتی عمیق.	طرح تصویب اعتبار تراکنش متمایز [14]ارائه می‌شود. یادگیری تقویتی عمیق. برای برنامه‌ریزی بهینه‌شدهٔ منابع.	پنج ایستگاه پایه [15] هر کدام دارای سرور محاسباتی و سرور ذخیره‌سازی هستند.

[1] Data Storage
[2] Data Management
[3] Resource Management
[4] Software-Defined Network (SDN)
[5] Service-Oriented Architecture
[6] Fuzzy Folded BF (FFBF)
[7] Integrated Database Management System
[8] Cyber-Physical Systems (CPS)
[9] Deep Reinforcement Learning (DRL)
[10] Cyber Physical System Architecture (CCPSA)
[11] Federated Imitation Learning (FIL)
[12] Federated Deep Learning (FDL)
[13] Multi-party Computation (MPC)
[14] Differentiated transaction
[15] Base station (BS)

[DOI: 10.61186/jsdp.21.3.23]

چارچوب	زمینهٔ پژوهش	تکنیک‌های مورد استفاده	مشارکت‌ها	اثبات مفهوم
	بهینه‌سازی بیش از حد پارامترها در مدل یادگیری ماشین.	بهینه‌سازی ازدحام ذرات PSO[1] همراه با یادگیری مشارکتی.	چارچوب بهینه‌سازی ازدحام ذرات برای تنظیم پارامتر پیشنهاد شده است و تعداد لایه‌های پنهان و سلول‌های عصبی بهینه شده است.	ترافیک شهر هوشمند با مجموعه داده‌های City Pulse EU FP7
مدیریت منابع [۱۲۱-۱۳۵]	بهینه‌سازی قدرت انتقال. استفادهٔ مجدد از منابع بی‌سیم.	یادگیری مشارکتی سلسله مراتبی.	حالت بسته برای ارزیابی هم‌گرایی. بهینه‌سازی قدرت انتقال. به حداقل رساندن تابع زیان.	سناریوی BS شبکهٔ سلولی ناهمگن متشکل از MBS[2] و SBS[3]
	فعال‌کردن بارگیری وظایف و امور مهم در لبه‌ها.	یادگیری عمیق مبتنی بر یادگیری مشارکتی.	کاهش هزینه به‌دلیل تأخیر، محاسبه و مصرف انرژی.	شبکه‌های ناهمگن در محاسبات لبه‌ای
	بهینه‌سازی منابع در اینترنت اشیا شناختی.	یادگیری مشارکتی پراکنده.	برنامه‌ریزی خطی برای بهینه‌سازی هزینهٔ کلی.	صنعت هوشمند
	ارزیابی مدل یادگیری ماشین. ایجاد فرایند ساخت‌یافته.	یادگیری مشارکتی صنعتی (IFL)[4]	مدل قابل تطبیق با شرایط متنوع. پیشنهاد یادگیری مشارکتی صنعتی.	چارچوب هم‌زمان یادگیری مشارکتی متمرکز
	کاهش ارتباطات غیرقابل اعتماد.	یادگیری مشارکتی مبتنی بر بلاک‌چین.	متعادل‌بودن دقت یادگیری.	شبکه‌های بی‌سیم دوقلو دیجیتال(DTWN)[5]
	تخصیص پویا منابع.	یادگیری تقویتی متمرکز عمیق(DFRL)[6]	یادگیری Q عمیق چندعاملی (MAQL)[7] برای برش پویا پیشنهاد شده است.	اینترنت اشیا چند صنعتی
	انجام طبقه‌بندی تصویر در دامنهٔ اکتشاف.	یادگیری مشارکتی توزیع‌شده.	مرکز همجوشی زمینی (GFC[8]) مستقر شده است. هزینهٔ ارتباطات کاهش می‌یابد.	وسایل نقلیهٔ هوایی بدون سرنشین(UAVs)[9]

(جدول-۷): خلاصه ای ازپژوهش‌های مهم در یادگیری مشارکتی با تمرکز بر مکانیسم‌های افزایش حریم خصوصی

(Table-7): A summary of important study in federation learning research focusing on privacy enhancement mechanisms

جزئیات حریم خصوصی	مکانیزم حریم خصوصی	سهم عمده	مرجع
Batch-level DP, Ɛ-DP مکانیسم لاپلاس	DP[10]	شرح روش نزولی شیب انتخابی توزیع‌شده برای کاهش ارتباطات و استفاده از حریم خصوصی دیفرانسیل برای محافظت از به‌روزرسانی‌های پارامتر مدل	[۲۰]
Batch-level DP ،(Ɛ-δ)-DP (مکانیسم گاوسی)	DP	شرح روش حسابداری کارآمد برای جمع‌آوری ضررهای حریم خصوصی هنگام آموزش DNN با حریم خصوصی افتراقی	[۱۴۶]
پروتکل تجمیع امن فقط در صورتی‌که تعداد کافی به‌روزرسانی ارسال کند، شیب متوسط مشتری را ارزیابی می‌کند.	SMC[11]	روش جدید برای ارائهٔ محاسبات ایمن چندحزبی که به‌طور خاص برای یادگیری مشارکتی تنظیم شده‌است	[۱۵]
سطح کاربر DP ،(Ɛ-δ)-DP (مکانیسم گاوسی)	DP	روش ارائهٔ حریم خصوصی دیفرانسیل در سطح کاربر برای یادگیری مشارکتی تنها با ضرر کمی در ابزار مدل	[۱۴۷]
سطح کاربر DP ،(Ɛ-δ)-DP (مکانیسم گاوسی)	DP	روش ارائهٔ حریم خصوصی افتراقی در سطح کاربر برای یادگیری مشارکتی بدون نادیده‌گرفتن ابزار مدل	[۱۴۵]
حمله در برابر رکورد/سطح دسته‌ای DP آزمایش شده‌است. (با استفاده از [۲۰] اجرا شده‌است).	DP	نمایش روش حمله به مدل جهانی با استفاده از یک شبکهٔ خصمانهٔ تولیدکننده، حتی در برابر DP در سطح رکورد/دسته‌ای نیز مؤثر است.	[۱۴۸]
به‌روزرسانی‌های شیب با استفاده از رمزنگاری هوموروفیک رمزگذاری می‌شوند سرور جمع گرادیان متوسطی را برای تمام کارگران به‌دست می‌آورد، اما فقط پس از جمع‌شدن تعداد مشخصی از به‌روزرسانی‌ها می‌تواند این نتیجه را رمزگشایی کند.	HE12,SMC	روشی برای رمزنگاری به‌روزرسانی‌های کاربر در حین آموزش توزیع‌شده، قابل رمزگشایی فقط هنگامی‌که بسیاری از مشتری‌ها در هدف یادگیری توزیع‌شده شرکت کرده باشند.	[۱۴۹]
به‌صورت اختیاری از پروتکل تجمیع امن در [۱۵۰] استفاده می‌کند.	SMC	شرح سیستم یادگیری مشارکتی آمادهٔ تولید در مقیاس کامل (تمرکز روی دستگاه‌های تلفن همراه)	[۱۵۱]

[1] Particle Swarm Optimization (PSO)
[2] Macro Base Station (MBS)
[3] Small Cell Base Station (SBS)
[4] Industrial Federated Learning (IFL)
[5] Digital Twin Wireless Networks (DTWN)
[6] Deep Federated Reinforcement Learning (DFRL)
[7] Multi-Agent Deep Q-learning (MAQL)
[8] Ground Fusion Centre (GFC)
[9] Unmanned Aerial Vehicles (UAVs)
[10] Differential privacy (DP)
[11] Secure multi-party computation (SMC)
[12] Homomorphic encryption (HE)

(جدول-۸): خلاصه‌ای از کارهای اخیر در زمینهٔ یادگیری مشارکتی برای مراقبت‌های بهداشتی و سلامت

(Table-8): A summary of recent works in federated learning for the health care

زمینهٔ کاربرد	متد یادگیری ماشین مورداستفاده	تعداد مشتری‌ها	داده‌های پژوهش
یادگیری مشابهت بیمار[1] [۱۶۲]	Hashing	۳	MIMIC-III[۱۷۲]
یادگیری مشابهت بیمار[۱۷۳]	Hashing	۲۰	MIMIC-III
فنوتیپ‌سازی [۱۶۴]	TF[2]	۱-۵	MIMIC-III, UCSD[۱۴۹]
فنوتیپ‌سازی[3] [۱۶۳]	NLP	۱۰	MIMIC-III
یادگیری ویژگی[4] [۱۶۹]	PCA	۱۰-۱۰۰	ADNI, UK Biobank, PPMI, MIRIAD
پیش‌بینی مرگ‌ومیر [۱۶۶]	Autoencoder	۵-۵۰	eICU Collaborative Research Database[۱۵۰]
پیش‌بینی مرگ‌ومیر [۱۷۴]	LR, NN	۳۱	eICU Collaborative Research Database
پیش‌بینی مرگ‌ومیر [۱۶۷]	LR, MLP[5]	۲	MIMIC-III
پیش‌بینی مرگ‌ومیر در کرونا [۱۷۵]	LRR, MLP, LASSO	۵	Mount Sinai COVID-19 Dataset
پیش‌بینی بستری بیماران [۱۶۵]	SVM	۵و۱۰	Boston Medical Center
پیش‌بینی زایمان زودرس [۱۶۸]	RNN	۵۰	Cerner Health Facts
تشخیص فعالیت فیزیکی[۱۷۶]	CNN	۵	UCI Smartphone٤
پیش‌بینی عوارض جانبی دارو [۱۷۷, ۱۷۸]	SVM, MLP, LR	۱۰	LCED[6], MIMIC
تشخیص آریتمی [۱۷۹]	NN	۱۶،۳۲،۶۴	PhysioNet Dataset[۱۸۰]
پیش‌بینی بیماری [۱۸۱]	NN	۵،۱۰	Pima Indians Diabetes Dataset [۱۸۲], Cleveland Heart Disease Database [۱۸۱]
تجزیه و تحلیل داده‌های تصویربرداری [۸۴]	VAE[7]	۴	MNIST, Brain Imaging Data

(جدول-۹): خلاصه‌ای از برنامه‌های کاربردی یادگیری مشارکتی در مراقبت‌های بهداشتی و سلامت

(Table-9): A summary of the Federated learning applications in health care

زمینه	محدودیت	مزایا	مطالعات	زمینهٔ کاربرد	مرجع
برنامه‌های کاربردی در مراقبت‌های بهداشتی	برای هم‌گرایی به تکرارهای بیشتری نیاز است.	طبقه‌بندی عملکرد با استفاده از تعداد نسبتاً کمی از ویژگی‌ها.	الگوریتم تقسیم دو خوشه‌ای اولیه[1].	پیش‌بینی بستری‌شدن بیماران.	Brisimi et al., 2018 [۱۶۵]
	تنها در مجموعه‌دادهٔ محدود آزمایش شده‌است.	برخورد مؤثر با تنوع ویژگی‌های ابعاد بالا.	ارائهٔ چارچوب تجزیه و تحلیل مشارکتی سازگار با خطوط لولهٔ استاندارد ENIGMA.	تجزیه و تحلیل تصویربرداری تشدید مغناطیسی (MRI[2]).	Silva et al.2019 [۱۶۹]
	برای موارد کوچک مشکوک مناسب نیست	افزایش دقت یا افزودن مرحلهٔ پیش‌پردازش.	روش NLP مشارکتی دو مرحله‌ای.	پردازش یادداشت‌های بالینی.	Liu et al., 2019 [۱۶۳]
	فقط روی سه مجموعه‌دادهٔ مختلف کار شده‌است.	نخستین طبقه‌بندی الکتروانسفالوگرافی(EEG[3]) بر روی داده‌های EEG ناهمگن.	طراحی یک چارچوب یادگیری مشارکتی افقی ناهمگن سلسله مراتبی.	طبقه‌بندی EEG.	Gao et al.2019 [۴۳]
	پارامترهای مدل جامعه منجر به سربار اضافی ارتباطات خواهد شد.	نسبت به مدل یادگیری مشارکتی پایه، در دوره‌های ارتباطی کمتری به دقت پیش‌بینی‌کنندهٔ بالاتری هم‌گرا شده‌است.	معرفی یادگیری مشارکتی مبتنی بر جامعه و ارزیابی آن در سوابق پزشکی الکترونیک [4]غیرمستقل هم‌توزیع icu	پیش‌بینی مرگ‌ومیر و زمان بستری در بیمارستان.	Li, Cheng, Liu, Wang, & Chen, 2019 [۱۸۳]
	دست‌کم‌گرفتن هزینهٔ حریم خصوصی.	یادگیری مشارکتی را به روش متمایز خصوصی انجام می‌دهد.	ایجاد اثربخشی یادگیری مشارکتی بر یادگیری متمرکز و محلی	پیش‌بینی بالینی.	Pfohl et al., 2019 [۱۷۰]
	آموزش داده‌های مستقل هم‌توزیع از داده‌های غیرمستقل هم‌توزیع بهتر است.	با معرفی فناوری به اشتراک‌گذاری داده‌ها، موارد غیرمستقل هم‌توزیع را کاهش می‌دهد.	روش تقویت سازگار.	پیش‌بینی مرگ‌ومیر در استفاده از موادمخدر.	Huang, Yin et al., 2019 [۱۸۴]
	فقط با داده‌های کوچک دقیق است. پیچیدگی محاسباتی.	اطلاعات خلاصه داده‌های بیمار را فاش نمی‌کند.	فاکتوربندی تانسور مشارکتی برای حفظ حریم خصوصی برای حفظ فنوتیپ‌های محاسباتی.	تجزیه و تحلیل فنوتیپ‌های محاسباتی.	Kim et al., 2017 [۱۶۴]
	پیچیدگی محاسباتی	اجتناب از حملات امنیتی مهندسی معکوس	FPH[5]	تطبیق مشابهت بیمار.	Lee et al., 2018 [۱۶۲]

[1] Patient similarity learning
[2] Tensor Factorization
[3] Phenotyping
[4] Representation Learning
[5] Multi-layer perceptron
[6] Limited MarketScan Explorys Claims-EMR Data
[7] variational autoencoder

[DOI: 10.61186/jsdp.21.3.23]

7-Reference ۷-منابع

[1] Blanco-Justicia A, Domingo-Ferrer J et al. “Achieving security and privacy in federated learning systems: Survey, research challenges and future directions,” Engineering Applications of Artificial Intelligence, Vol. 106, pp. 1-14, 104468, November 2021.

[2] McMahan B, Moore E, Ramage D, Hampson S, y Arcas BA. “Communication-efficient learning of deep networks from decentralized data.” InArtificial intelligence and statistics, Vol. 54, pp. 1273-1282, April 2017.

[3] Yang Q, Liu Y, Chen T, Tong Y. “Federated machine learning: Concept and applications." ACM Transactions on Intelligent Systems and Technology (TIST), Vol. 10, pp. 1-19, January 2019.

[4] Li L, Fan Y, Tse M, Lin KY. “A review of applications in federated learning.” Computers & Industrial Engineering, Vol. 149, November 2020.

[5] Konečný J, McMahan HB, Ramage D, Richtárik P. “Federated optimization: Distributed machine learning for on-device intelligence.” arXiv preprint arXiv:1610.02527. October 2016.

[6] Dayarathna M, Bandara S, Jayamaha N, Herath M, Madhushan A, Jayasena S, Suzumura T. “An x10-based distributed streaming graph database engine.” In2017 IEEE 24th International Conference on High Performance Computing (HiPC), pp. 243-252, December 2017.

[7] Srinivas J, Reddy KV, Qyser AM. “Cloud computing basics.” International journal of advanced research in computer and communication engineering. Vol. 1, pp. 343-347, July 2012.

[8] Liu J, Huang J, Zhou Y, Li X, Ji S, Xiong H, Dou D. “From distributed machine learning to federated learning: A survey.” Knowledge and Information Systems, Vol. 64, pp. 885-917, April 2022.

[9] Li T, Sahu AK, Talwalkar A, Smith V. “Federated learning: Challenges, methods, and future directions.” IEEE signal processing magazine, Vol. 37, pp. 50-60, May 2020.

[10] Yang A, Ma Z, Zhang C, Han Y, Hu Z, Zhang W, Huang X, Wu Y. “Review on application progress of federated learning model and security hazard protection.” Digital Communications and Networks, Vol. 9, pp. 146-158, February 2023.

[11] Wang G. “Interpret federated learning with shapley values.” arXiv preprint arXiv:1905.04519. May 2019.

[12] Zheng Z, Zhou Y, Sun Y, Wang Z, Liu B, Li K. “Applications of federated learning in smart cities: recent advances, taxonomy, and open challenges.” Connection Science, Vol. 34, pp. 1-28, December 2022.

[13] Kairouz P, McMahan HB, Avent B, Bellet A, Bennis M, Bhagoji AN, Bonawitz K, Charles Z, Cormode G, Cummings R, D’Oliveira RG. “Advances and open problems in federated learning.” Foundations and trends® in machine learning, Vol. 14, pp. 1-210, June 2021.

[14] Smith V, Chiang CK, Sanjabi M, Talwalkar AS. “Federated multi-task learning.” Advances in neural information processing systems (NIPS), Vol. 30, December 2017.

[15] Bonawitz K, Ivanov V, Kreuter B, Marcedone A, McMahan HB, Patel S, et al., editors. “Practical secure aggregation for privacy-preserving machine learning.” proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1175-1191, November 2017.

[16] Chen Y, Luo F, Li T, Xiang T, Liu Z, Li J. “A training-integrity privacy-preserving federated learning scheme with trusted execution environment.” Information Sciences, Vol. 522, pp. 69-79, June 2020.

[17] Sarikaya Y, Ercetin O. “Motivating workers in federated learning: A stackelberg game perspective.” IEEE Networking Letters, Vol. 2, pp.23-27, October 2019.

[18] Khan LU, Pandey SR, Tran NH, Saad W, Han Z, Nguyen MN, et al. “Federated learning for edge networks: Resource optimization and incentive mechanism.” IEEE Communications Magazine, Vol. 58, pp. 88-93. October 2020.

[19] Pandey SR, Tran NH, Bennis M, Tun YK, Manzoor A, Hong CS. “A crowdsourcing framework for on-device federated learning.” IEEE Transactions on Wireless Communications, Vol. 19, pp. 3241-3256, February 2020.

[20] Shokri R, Shmatikov V. “Privacy-preserving deep learning.” InProceedings of the 22nd ACM SIGSAC conference on computer and communications security, pp. 1310-1321, October 2015.

[21] Konečný J, McMahan HB, Yu FX, Richtárik P, Suresh AT, Bacon D. “Federated learning: Strategies for improving communication efficiency.” arXiv preprint arXiv:161005492. October 2017.

[22] Konečný J, McMahan HB, Ramage D, Richtárik P. “Federated optimization: Distributed machine learning for on-device intelligence.” arXiv preprint arXiv:1610.02527. October 2016.

[23] Khalooei M, Homayounpour M M, Amirmazlaghani M. “A survey on vulnerability of deep neural networks to adversarial examples and defense approaches to deal with them.” Signal and Data Processing, Vol. 20 Issue 2 pp. 113-144, DOI: 10.61186/jsdp.20.2.113, September 2023.

[24] Mohammadi S, Khalatbary A, Babagoli M. “Propose a meta-heuristic model of intrusion

[DOI: 10.61186/jsdp.21.3.23]

detection using feature selection based on improved gray wolf optimization and random forest." Signal and Data Processing, Vol. 20 Issue 1, pp.133-144, DOI: 10.61186/jsdp.20.1.133, June 2023.

[25] McMahan, H.B., Ramage, D. "Federated learning: Collaborative machine learning without centralized training data." Google AI Blog , April 2017, https://ai.googleblog.com/2017/04/federated-learning-collaborative.html.

[26] Cai H, Venkatasubramanian KK. "Detecting data manipulation attacks on physiological sensor measurements in wearable medical systems." EURASIP Journal on Information Security, Vol. 2018, pp. 1-21. September2018.

[27] Blanchard P, El Mhamdi EM, Guerraoui R, Stainer J. "Machine learning with adversaries: Byzantine tolerant gradient descent." Advances in neural information processing systems, Vol. 30, 2017.

[28] Chen Y, Su L, Xu J. "Distributed statistical machine learning in adversarial settings: Byzantine gradient descent." InAbstracts of the 2018 ACM International Conference on Measurement and Modeling of Computer Systems, Vol. 46, pp. 96, June 2018.

[29] Yin D, Chen Y, Kannan R, Bartlett P. "Byzantine-robust distributed learning: Towards optimal statistical rates." Proceedings of the 35th International conference on machine learning, Vol. 80, pp. 5650-5659, July 2018.

[30] Guerraoui R, Rouault S. "The hidden vulnerability of distributed learning in byzantium". Proceedings of the 35th International Conference on Machine Learning, Vol. 80, pp. 3521-3530, July 2018.

[31] Xie C, Koyejo S, Gupta I. Zeno: "Distributed stochastic gradient descent with suspicion-based fault-tolerance." Proceedings of the 36th International Conference on Machine Learning , Vol. 97, pp. 6893-6901, May 2019.

[32] Li T, Sahu AK, Zaheer M, Sanjabi M, Talwalkar A, Smith V. "Federated optimization in heterogeneous networks." Proceedings of Machine learning and systems, Vol. 2, pp. 429-450, March 2020.

[33] Muñoz-González L, Co KT, Lupu EC. "Byzantine-robust federated machine learning through adaptive model averaging." arXiv preprint arXiv:1909.05125, September 2019.

[34] Tahanian E, Amouei M, Fateh H, Rezvani M. A "game-theoretic approach for robust federated learning." International Journal of Engineering, Vol. 34 Issue 4, pp.832-842, April 2021.

[35] Rezaei M, Rezvani M, Zahedi M. "Automatic Configuration of Federated Learning Client in Graph Classification using Genetic Algorithms." Journal of AI and Data Mining, Vol. 12 Issue 1, pp. 115-126, January 2024.

[36] Dong X, Yu Z, Cao W, Shi Y, Ma Q. "A survey on ensemble learning." Frontiers of Computer Science. Vol. 14, pp. 241-258, April 2020 .

[37] Jiang D, Shan C, Zhang Z. "Federated learning algorithm based on knowledge distillation." In2020 International conference on artificial intelligence and computer engineering (ICAICE). pp. 163-167 October 2020.

[38] Zhou ZH. Ensemble methods: foundations and algorithms. CRC press; June 2012.

[39] Verbraeken J, Wolting M, Katzy J, Kloppenburg J, Verbelen T, Rellermeyer JS. "A survey on distributed machine learning." Acm computing surveys (csur), Vol. 53 Issue 2 pp. 1-33, March 2020.

[40] Dehghani M, Yazdanparast Z. "From distributed machine to distributed deep learning: a comprehensive survey." Journal of Big Data. Vol. 10, pp. 158, October 2023.

[41] Yang Q, Liu Y, Cheng Y, Kang Y, Chen T, Yu H. "Federated learning: synthesis lectures on artificial intelligence and machine learning." Vol.13, pp.1-207, December 2019. https://doi.org/10.1007/978-3-031-01585-4

[42] Borylo P, Lason A, Rzasa J, Szymanski A, Jajszczyk A. "Energy-aware fog and cloud interplay supported by wide area software defined networking." In 2016 IEEE International Conference on Communications (ICC), pp. 1-7, May 2016.

[43] Gao D, Ju C, Wei X, Liu Y, Chen T, Yang Q. "Hhhfl: Hierarchical heterogeneous horizontal federated learning for electroencephalography." arXiv preprint arXiv:1909.05784, September 2019.

[44] .Ju C, Gao D, Mane R, Tan B, Liu Y, Guan C. "Federated transfer learning for EEG signal classification." In2020 42nd annual international conference of the IEEE engineering in medicine & biology society (EMBC), pp. 3040-3045 , July 2020.

[45] Hu K, Liu R, Yu H. "Horizontal Federated Learning For Brain-Computer Interface." In Proceedings of the 5th Distributed Artificial Intelligence Conference (DAI'23), December 2023.

[46] Zhang Z, Li P, Al Hammadi AY, Guo F, Damiani E, Yeun CY. "Reputation-based federated learning defense to mitigate threats in EEG signal classification." In2024 16th International Conference on Computer and Automation Engineering (ICCAE), pp. 173-180, March 2024.

[47] Landau O, Puzis R, Nissim N. "Mind your mind: EEG-based brain-computer interfaces and their security in cyber space." ACM Computing Surveys (CSUR), Vol. 35, pp. 1-38, February 2020.

[48] Lee S, Lacy ME, Jankowich M, Correa A, Wu WC. "Association between obesity phenotypes of insulin resistance and risk of type 2 diabetes in African Americans: the Jackson heart study." Journal of clinical &

[DOI: 10.61186/jsdp.21.3.23]

translational endocrinology. Vol. 19, pp. 100210, March 2020.
[49] Gascón A, Schoppmann P, Balle B, Raykova M, Doerner J, Zahur S, et al. “Privacy-Preserving Distributed Linear Regression on High-Dimensional Data.” Proc Priv Enhancing Technol, pp. 345-364, June 2017.
[50] Nock R, Hardy S, Henecka W, Ivey-Law H, Patrini G, Smith G, Thorne B. “Entity resolution and federated learning get a federated resolution.” arXiv preprint arXiv:1803.04035, March 2018.
[51] Cheng K, Fan T, Jin Y, Liu Y, Chen T, Papadopoulos D, Yang Q. “Secureboost: A lossless federated learning framework.“ IEEE intelligent systems, Vol. 36 Issue 6, pp. 87-98, May 2021.
[52] Pan SJ, Ni X, Sun JT, Yang Q, Chen Z. “Cross-domain sentiment classification via spectral feature alignment.” InProceedings of the 19th international conference on World wide web, pp. 751-760, April 2010.
[53] Liu Y, Kang Y, Xing C, Chen T, Yang Q. “A secure federated transfer learning framework.” IEEE Intelligent Systems, Vol. 35, pp. 70-82, August 2020 .
[54] Sharma S, Xing C, Liu Y, Kang Y, editors. “Secure and efficient federated transfer learning.” 2019 IEEE International Conference on Big Data (Big Data), pp. 2569-2576, December 2019.
[55] Chen Y, Ning Y, Slawski M, Rangwala H. “Asynchronous online federated learning for edge devices with non-iid data.” In 2020 IEEE International Conference on Big Data (Big Data), pp. 15-24, December 2020.
[56] Chen Y, Sun X, Jin Y. “Communication-efficient federated deep learning with layerwise asynchronous model update and temporally weighted aggregation.” IEEE transactions on neural networks and learning systems, Vol. 31 Issue 10, pp. 4229-4238, December 2019.
[57] Kitchenham B. Procedures for performing systematic reviews. Keele, UK, Keele University, pp. 1-26, July 2004.
[58] Pham QV, Dev K, Maddikunta PK, Gadekallu TR, Huynh-The T. “Fusion of federated learning and industrial internet of things: a survey.” arXiv preprint arXiv:2101.00798, January 2021.
[59] Xia Q, Ye W, Tao Z, Wu J, Li Q. A “survey of federated learning for edge computing: Research problems and solutions.” High-Confidence Computing, Vol. 1 Issue 1, June 2021.
[60] Lo SK, Lu Q, Wang C, Paik HY, Zhu L. “A systematic literature review on federated machine learning: From a software engineering perspective.” ACM Computing Surveys (CSUR), Vol. 54 Issue 5, pp. 1-39, May 2021.
[61] Briggs C, Fan Z, Andras P. “A review of privacy-preserving federated learning for the Internet-of-Things.” Federated Learning Systems: Towards Next-Generation AI, Vol. 965, pp. 21-50, June 2021.
[62] Liu Y, Zhang L, Ge N, Li G. “A systematic literature review on federated learning: From a model quality perspective.” arXiv preprint arXiv:2012.01973, December 2020.
[63] Lyu L, Yu H, Yang Q. “Threats to federated learning: A survey.” arXiv preprint arXiv:2003.02133. March 2020.
[64] Lim WYB, Luong NC, Hoang DT, Jiao Y, Liang Y-C, Yang Q, et al. “Federated learning in mobile edge networks: A comprehensive survey.” IEEE Communications Surveys & Tutorials, Vol. 22 Issue 3, pp. 2031-2063, April 2020.
[65] Aledhari M, Razzak R, Parizi RM, Saeed F. “Federated learning: A survey on enabling technologies, protocols, and applications.” IEEE Access, Vol. 8, pp. 140699-140725, July 2020.
[66] Li Q, Wen Z, Wu Z, Hu S, Wang N, Li Y, Liu X, He B. “A survey on federated learning systems: Vision, hype and reality for data privacy and protection.” IEEE Transactions on Knowledge and Data Engineering, Vol. 35 Issue 4, pp. 3347-3366, November 2021.
[67] Mothukuri V, Parizi RM, Pouriyeh S, Huang Y, Dehghantanha A, Srivastava G. “A survey on security and privacy of federated learning.” Future Generation Computer Systems, Vol. 115, pp. 619-640 February 2021.
[68] Zhu H, Zhang H, Jin Y. “From federated learning to federated neural architecture search: a survey.” Complex & Intelligent Systems, Vol. 7, pp. 639-657, April 2021.
[69] Kulkarni V, Kulkarni M, Pant A. “Survey of personalization techniques for federated learning.” 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), March 2020.
[70] Jin Y, Wei X, Liu Y, Yang Q. “Towards utilizing unlabeled data in federated learning: A survey and prospective.” arXiv preprint arXiv:2002.11545, February 2020.
[71] Nguyen DC, Ding M, Pathirana PN, Seneviratne A, Li J, Poor HV. “Federated learning for internet of things: A comprehensive survey.” IEEE Communications Surveys & Tutorials, Vol. 23 Issue 3, pp.1622-1658, April 2021.
[72] Du Z, Wu C, Yoshinaga T, Yau KL, Ji Y, Li J. “Federated learning for vehicular internet of things: Recent advances and open issues.” IEEE Open Journal of the Computer Society, Vol. 1, pp. 45-61, May 2020.
[73] Mammen PM. “Federated learning: Opportunities and challenges.” arXiv preprint arXiv:2101.05428, January 2021.
[74] Liu J, Huang J, Zhou Y, Li X, Ji S, Xiong H, Dou D. “From distributed machine learning to federated learning: A survey.” Knowledge and Information Systems. Vol. 64, pp. 885-917, April 2022 .

[DOI: 10.61186/jsdp.21.3.23]

Surveys & Tutorials, pp.1342-1397, Vol. 23 Issue 2, February 2021.
[87] Banabilah S, Aloqaily M, Alsayed E, Malik N, Jararweh Y. "Federated learning review: Fundamentals, enabling technologies, and future applications." Information processing & management, Vol. 59 Issue 6, November 2022.
[88] Liu J, Huang J, Zhou Y, Li X, Ji S, Xiong H, Dou D. "From distributed machine learning to federated learning: A survey." Knowledge and Information Systems. Vol. 64, pp. 885-917, April 2022.
[89] Dasaradharami Reddy K, Gadekallu TR. "A comprehensive survey on federated learning techniques for healthcare informatics." Computational Intelligence and Neuroscience. Vol. 2023 Issue 1, March 2023.
[90] Li H, Li C, Wang J, Yang A, Ma Z, Zhang Z, Hua D. "Review on security of federated learning and its application in healthcare." Future Generation Computer Systems, Vol. 144, pp. 271-290, July 2023.
[91] Joung J. "Machine learning-based antenna selection in wireless communications." IEEE Communications Letters, Vol. 20 Issue 11, pp. 2241-2244, July 2016.
[92] Li H, Ota K, Dong M. "Learning IoT in edge: Deep learning for the Internet of Things with edge computing." IEEE network, Vol. 32 Issue 1, pp.96-101, January 2018.
[93] Luong NC, Hoang DT, Gong S, Niyato D, Wang P, Liang YC, Kim DI. "Applications of deep reinforcement learning in communications and networking: A survey." IEEE communications surveys & tutorials, Vol. 21 Issue 4, May 2019.
[94] Pham QV, Fang F, Ha VN, Piran MJ, Le M, Le LB, Hwang WJ, Ding Z. "A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art." IEEE access. pp.116974-117017, Vol. 8, June 2020.
[95] Yang T, Andrew G, Eichner H, Sun H, Li W, Kong N, Ramage D, Beaufays F. "Applied federated learning: Improving google keyboard query suggestions." arXiv preprint arXiv:1812.02903. December 2018.
[96] Sheller MJ, Edwards B, Reina GA, Martin J, Pati S, Kotrotsou A, Milchenko M, Xu W, Marcus D, Colen RR, Bakas S. "Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data." Scientific reports, Vol. 10, pp. 12598, July 2020 .
[97] Li L, Ota K, Dong M. "Deep learning for smart industry: Efficient manufacture inspection system with fog computing." IEEE Transactions on Industrial Informatics, Vol. 14 Issue 10, pp. 4665-4673, June 2018.
[98] Da Xu L, He W, Li S. "Internet of things in industries: A survey." IEEE Transactions on industrial informatics, Vol. 10 Issue 4, pp. 2233-2243, January 2014.
[75] Jiang JC, Kantarci B, Oktug S, Soyata T. "Federated learning in smart city sensing: Challenges and opportunities." Sensors, Vol. 20 Issue 21, October 2020.
[76] Ji S, Tan Y, Saravirta T, Yang Z, Liu Y, Vasankari L, Pan S, Long G, Walid A. "Emerging Trends in Federated Learning: From Model Fusion to Federated X Learning." arXiv preprint arXiv:2102.12920, February 2021. latest version: Ji S, Tan Y, Saravirta T, Yang Z, Liu Y, Vasankari L, Pan S, Long G, Walid A. "Emerging trends in federated learning: From model fusion to federated x learning." International Journal of Machine Learning and Cybernetics, Vol. 15, pp. 3769–3790, March 2024.
[77] Yang Q, Fan L, Yu H, editors. "Federated learning: Privacy and incentive." Springer Nature, Vol. 12500, November 2020.
[78] Park J, Samarakoon S, Elgabli A, Kim J, Bennis M, Kim SL, Debbah M. "Communication-efficient and distributed learning over wireless networks: Principles and applications." arXiv preprint arXiv:2008.02608, August 2020.
[79] Li Z, Sharma V, Mohanty SP. "Preserving data privacy via federated learning: Challenges and solutions." IEEE Consumer Electronics Magazine, Vol. 9 Issue 3, pp.8-16, May 2020.
[80] Zhao Z, Feng C, Yang HH, Luo X. "Federated-learning-enabled intelligent fog radio access networks: Fundamental theory, key techniques, and future trends." IEEE wireless communications, Vol. 27 Issue 2, pp.22-28, April 2020.
[81] Niknam S, Dhillon HS, Reed JH. "Federated learning for wireless communications: Motivation, opportunities, and challenges." IEEE Communications Magazine, Vol. 58 Issue 6, pp.46-51, June 2020.
[82] Liu Y, Yuan X, Xiong Z, Kang J, Wang X, Niyato D. "Federated learning for 6G communications: Challenges, methods, and future directions." China Communications, Vol. 17 Issue 9, pp.105-118, September 2020.
[83] Briggs C, Fan Z, Andras P. "A review of privacy preserving federated learning for private IoT analytics." arXiv preprint arXiv:2004.11794, April 2020.
[84] Xu J, Glicksberg BS, Su C, Walker P, Bian J, Wang F. "Federated learning for healthcare informatics." Journal of healthcare informatics research, Vol. 5, pp.1-19, March 2021.
[85] Brik B, Ksentini A, Bouaziz M. "Federated learning for UAVs-enabled wireless networks: Use cases, challenges, and open problems." IEEE Access, Vol. 8, pp. 53841-53849, March 2020.
[86] Wahab OA, Mourad A, Otrok H, Taleb T. "Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems." IEEE Communications

[DOI: 10.61186/jsdp.21.3.23]

IoT." IEEE Transactions on Industrial Informatics. Vol. 16 Issue 6, pp. 4177-4186, September 2019.
[111] Li Z, Liu J, Hao J, Wang H, Xian M. "CrowdSFL: A secure crowd computing framework based on blockchain and federated learning." Electronics. Vol. 9 Issue 5, May 2020.
[112] Hua G, Zhu L, Wu J, Shen C, Zhou L, Lin Q. "Blockchain-based federated learning for intelligent control in heavy haul railway." IEEE Access, Vol. 8, pp. 176830-176839, September 2020.
[113] Sharma PK, Park JH, Cho K. Blockchain and "federated learning-based distributed computing defence framework for sustainable society." Sustainable Cities and Society, Vol. 59, pp. 102220, August 2020.
[114] Leroy D, Coucke A, Lavril T, Gisselbrecht T, Dureau J. "Federated learning for keyword spotting." InICASSP 2019-2019 IEEE international conference on acoustics, speech and signal processing (ICASSP), pp. 6341-6345, May 2019.
[115] Hard A, Rao K, Mathews R, Ramaswamy S, Beaufays F, Augenstein S, Eichner H, Kiddon C, Ramage D. "Federated learning for mobile keyboard prediction." arXiv preprint arXiv:1811.03604, November 2018.
[116] Ramaswamy S, Mathews R, Rao K, Beaufays F. "Federated learning for emoji prediction in a mobile keyboard." arXiv preprint arXiv:1906.04329, June 2019.
[117] Wang X, Han Y, Wang C, Zhao Q, Chen X, Chen M. "In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning." in IEEE Network, Vol. 33 Issue 5, pp. 156-165, July 2019.
[118] Qian Y, Hu L, Chen J, Guan X, Hassan MM, Alelaiwi A. "Privacy-aware service placement for mobile edge computing via federated learning." Information Sciences, Vol. 505, pp. 562-570, December 2019.
[119] Feng J, Rong C, Sun F, Guo D, Li Y. "PMF: A privacy-preserving human mobility prediction framework via federated learning." Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, Vol. 4, pp. 1-21, March 2020.
[120] Sozinov K, Vlassov V, Girdzijauskas S. "Human activity recognition using federated learning." In2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCo m), pp. 1103-1111, December 2018.
[121] Aïvodji UM, Gambs S, Martin A. "IOTFLA: A secured and privacy-preserving smart home architecture implementing federated learning." In 2019 IEEE security and
[99] Huang J, Kong L, Chen G, Wu MY, Liu X, Zeng P. "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism." IEEE Transactions on Industrial Informatics, Vol. 15 Issue 6, pp. 3680-3689, March 2019.
[100] Kong L, Liu XY, Sheng H, Zeng P, Chen G. "Federated tensor mining for secure industrial internet of things." IEEE Transactions on Industrial Informatics, Vol. 16 Issue 3, pp. 2144-2153, August 2019.
[101] Arachchige PC, Bertok P, Khalil I, Liu D, Camtepe S, Atiquzzaman M. "A trustworthy privacy preserving framework for machine learning in industrial IoT systems." IEEE Transactions on Industrial Informatics, Vol. 16 Issue 9, pp. 6092-6102, February 2020.
[102] Kuang L, Yang LT, Feng J, Dong M. "Secure tensor decomposition using fully homomorphic encryption scheme." IEEE Transactions on Cloud Computing, Vol. 6 Issue 3, pp.868-878, December 2015.
[103] Raja G, Manaswini Y, Vivekanandan GD, Sampath H, Dev K, Bashir AK. "AI-powered blockchain-a decentralized secure multiparty computation protocol for IoV." In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 865-870, July 2020.
[104] Huynh-The T, Hua CH, Pham QV, Kim DS. "MCNet: An efficient CNN architecture for robust automatic modulation classification." IEEE Communications Letters, Vol. 24 Issue 4, pp. 811-815, January 2020.
[105] Deepa N, Pham QV, Nguyen DC, Bhattacharya S, Prabadevi B, Gadekallu TR, Maddikunta PK, Fang F, Pathirana PN. "A survey on blockchain for big data: Approaches, opportunities, and future directions." Future Generation Computer Systems,Vol. 131, pp. 209-226, June 2022.
[106] Hakak S, Khan WZ, Gilkar GA, Assiri B, Alazab M, Bhattacharya S, Reddy GT. "Recent advances in blockchain technology: A survey on applications and challenges." International Journal of Ad Hoc and Ubiquitous Computing, Vol. 38, pp. 82-100, November 2021.
[107] Wang YE, Wei GY, Brooks D. "Benchmarking TPU, GPU, and CPU platforms for deep learning." arXiv preprint arXiv:1907.10701, July 2019.
[108] Cho HD, Engineer PD, Chung K, Kim T. "Benefits of the big." LITTLE Architecture, EETimes, February 2012.
[109] Yin B, Yin H, Wu Y, Jiang Z. "FDC: A secure federated deep learning mechanism for data collaborations in the Internet of Things." IEEE Internet of Things Journal, Vol. 7 Issue 7, pp. 6348-6359, January 2020.
[110] Lu Y, Huang X, Dai Y, Maharjan S, Zhang Y. "Blockchain and federated learning for privacy-preserved data sharing in industrial

[DOI: 10.61186/jsdp.21.3.23]

interplay." IEEE communications magazine, Vol. 56 Issue 2, pp. 44-51, February 2018.
[134] Singh A, Garg S, Kaur K, Batra S, Kumar N, Choo KK. "Fuzzy-folded bloom filter-as-a-service for big data storage in the cloud." IEEE Transactions on Industrial Informatics, Vol. 15 Issue 4, pp. 2338-2348, June 2018.
[135] Saqlain M, Piao M, Shim Y, Lee JY. "Framework of an IoT-based industrial data management for smart manufacturing." Journal of Sensor and Actuator Networks, Vol. 8 Issue 2, April 2019.
[136] Anton SD, Fraunholz D, Zemitis J, Pohl F, Schotten HD. "Highly scalable and flexible model for effective aggregation of context-based data in generic IIoT scenarios." arXiv preprint arXiv:1906.03064, May 2019.
[137] Wan J, Tang S, Shu Z, Li D, Wang S, Imran M, Vasilakos AV. "Software-defined industrial internet of things in the context of industry 4.0." IEEE Sensors Journal, Vol. 16 Issue 20, pp.7373-7380, May 2016.
[138] Liu CH, Lin Q, Wen S. "Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning." IEEE Transactions on Industrial Informatics, Vol. 15 Issue 6, pp. 3516-3526, December 2018.
[139] Liu B, Wang L, Liu M, Xu CZ. "Federated imitation learning: A novel framework for cloud robotic systems with heterogeneous sensor data." IEEE Robotics and Automation Letters, Vol. 5 Issue 2, pp. 3509-3516, February 2020.
[140] Zhu H, Jin Y. "Multi-objective evolutionary federated learning." IEEE transactions on neural networks and learning systems, Vol. 31 Issue 4, pp. 1310-1322, June 2019.
[141] Kanagavelu R, Li Z, Samsudin J, Yang Y, Yang F, Goh RS, Cheah M, Wiwatphonthana P, Akkarajitsakul K, Wang S. "Two-phase multi-party computation enabled privacy-preserving federated learning." In2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID), pp. 410-419, May 2020.
[142] Hao M, Li H, Luo X, Xu G, Yang H, Liu S. "Efficient and privacy-enhanced federated learning for industrial artificial intelligence." IEEE Transactions on Industrial Informatics, Vol. 16 Issue 10, pp. 6532-6542, October 2019.
[143] Zhang K, Zhu Y, Maharjan S, Zhang Y. "Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of Things." IEEE network, Vol. 33 Issue 5, pp. 12-19, October 2019.
[144] Qolomany B, Ahmad K, Al-Fuqaha A, Qadir J. "Particle swarm optimized federated learning for industrial IoT and smart city services." InGLOBECOM 2020-2020 IEEE privacy workshops (SPW), pp. 175-180, May 2019.
[122] Yu T, Li T, Sun Y, Nanda S, Smith V, Sekar V, Seshan S. "Learning context-aware policies from multiple smart homes via federated multi-task learning." In2020 IEEE/ACM Fifth international conference on internet-of-things design and implementation (IoTDI), pp. 104-115, April 2020.
[123] Guo W, Kotsia I, Patras I. "Tensor learning for regression." IEEE Transactions on Image Processing, Vol. 21 Issue 2, pp. 816-827, August 2011.
[124] Lai Z, Wong WK, Xu Y, Zhao C, Sun M. "Sparse alignment for robust tensor learning." IEEE transactions on neural networks and learning systems, Vol. 25 Issue 10, pp.1779-1792 January 2014.
[125] Feng J, Yang LT, Liu X, Zhang R. "Privacy-preserving tensor analysis and processing models for wireless internet of things." IEEE Wireless Communications, Vol. 25 Issue 6, pp. 98-103, December 2018.
[126] Zhang X, Chen X, Liu JK, Xiang Y. "DeepPAR and DeepDPA: privacy preserving and asynchronous deep learning for industrial IoT." IEEE Transactions on Industrial Informatics, Vol. 16 Issue 3, pp. 2081-2090, September 2019.
[127] Wang X, Wang C, Li X, Leung VC, Taleb T. "Federated deep reinforcement learning for Internet of Things with decentralized cooperative edge caching." IEEE Internet of Things Journal, Vol. 7 Issue 10, pp. 9441-9455, April 2020.
[128] Liu Y, James JQ, Kang J, Niyato D, Zhang S. "Privacy-preserving traffic flow prediction: A federated learning approach." IEEE Internet of Things Journal, Vol. 7 Issue 8, pp. 7751-7763, April 2020.
[129] Kim H, Park J, Bennis M, Kim SL. "Blockchained on-device federated learning." IEEE Communications Letters, Vol. 24 Issue 6, pp. 1279-1283, June 2019.
[130] Qu Y, Gao L, Luan TH, Xiang Y, Yu S, Li B, Zheng G. "Decentralized privacy using blockchain-enabled federated learning in fog computing." IEEE Internet of Things Journal, Vol. 7 Issue 6, pp. 5171-5183, March 2020.
[131] Pokhrel SR, Choi J. "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges." IEEE Transactions on Communications, Vol. 68 Issue 8, pp. 4734-4746, April 2020.
[132] Fu JS, Liu Y, Chao HC, Bhargava BK, Zhang ZJ. "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing." IEEE Transactions on Industrial Informatics, Vol. 14 Issue 10, pp. 4519-4528, January 2018.
[133] Kaur K, Garg S, Aujla GS, Kumar N, Rodrigues JJ, Guizani M. "Edge computing in the industrial internet of things environment: Software-defined-networks-based edge-cloud

[DOI: 10.61186/jsdp.21.3.23]

Global Communications Conference, pp. 1-6, December 2020.
[145] McMahan HB, Ramage D, Talwar K, Zhang L. "Learning differentially private recurrent language models." arXiv preprint arXiv:1710.06963, October 2017.
[146] Abadi M, Chu A, Goodfellow I, McMahan HB, Mironov I, Talwar K, Zhang L. "Deep learning with differential privacy." In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pp. 308-318, October 2016.
[147] G Geyer RC, Klein T, Nabi M. "Differentially private federated learning: A client level perspective." arXiv preprint arXiv:1712.07557. December 2017.
[148] Hitaj B, Ateniese G, Perez-Cruz F. "Deep models under the GAN: information leakage from collaborative deep learning." In Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, pp. 603-618, October 2017.
[149] Zhang X, Ji S, Wang H, Wang T. "Private, yet practical, multiparty deep learning." In 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), pp. 1442-1452, June 2017.
[150] Wang S, Tuor T, Salonidis T, Leung KK, Makaya C, He T, Chan K. "Adaptive federated learning in resource constrained edge computing systems." IEEE journal on selected areas in communications, Vol. 37 Issue 6, pp. 1205-1221, March 2019.
[151] Bonawitz K, Eichner H, Grieskamp W, Huba D, Ingerman A, Ivanov V, Kiddon C, Konečnỳ J, Mazzocchi S, McMahan HB. "Towards federated learning at scale: System design." arXiv preprint arXiv:1902.01046. 2019.
[152] Barragán-Montero A, Javaid U, Valdés G, Nguyen D, Desbordes P, Macq B, Willems S, Vandewinckele L, Holmström M, Löfman F, Michiels S. "Artificial intelligence and machine learning for medical imaging: A technology review." Physica Medica. Vol. 83, pp. 242-256, March 2021.
[153] Guan H, Yap PT, Bozoki A, Liu M. "Federated learning for medical image analysis: A survey." Pattern Recognition, Vol. 151, March 2024.
[154] Agrawal S, Chowdhuri A, Sarkar S, Selvanambi R, Gadekallu TR. "Temporal weighted averaging for asynchronous federated intrusion detection systems." Computational Intelligence and Neuroscience, Vol. 2021 Issue 1, December 2021.
[155] Szegedi G, Kiss P, Horváth T. "Evolutionary Federated Learning on EEG-data." In ITAT, pp. 71-78, September 2019.
[156] Van Panhuis WG, Paul P, Emerson C, Grefenstette J, Wilder R, Herbst AJ, Heymann D, Burke DS. "A systematic review of barriers to data sharing in public health." BMC public health, Vol. 14, pp. 1-9, December 2014.
[157] Glicksberg BS, Johnson KW, Dudley JT. "The next generation of precision medicine: observational studies, electronic health records, biobanks and continuous monitoring." Human molecular genetics, Vol. 27 Issue R1, pp. R56-R62, May 2018.
[158] Gostin LO. "National health information privacy: regulations under the Health Insurance Portability and Accountability Act." Jama, Vol. 285, pp. 3015-3021, June 2001.
[159] Miotto R, Wang F, Wang S, Jiang X, Dudley JT. "Deep learning for healthcare: review, opportunities and challenges." Briefings in bioinformatics, Vol. 19 Issue 6, pp.1236-1246, November 2018.
[160] Rieke N, Hancox J, Li W, Milletari F, Roth HR, Albarqouni S, Bakas S, Galtier MN, Landman BA, Maier-Hein K, Ourselin S. "The future of digital health with federated learning." NPJ digital medicine, Vol. 3, pp. 1-7, September 2020.
[161] LeCun Y, Bengio Y, Hinton G. "Deep learning." Nature, Vol. 521, pp. 436-444, May 2015.
[162] Lee J, Sun J, Wang F, Wang S, Jun CH, Jiang X. "Privacy-preserving patient similarity learning in a federated environment: development and analysis." JMIR medical informatics, Vol. 6, April 2018.
[163] Liu D, Dligach D, Miller T. "Two-stage federated phenotyping and patient representation learning." In Proceedings of the conference. Association for Computational Linguistics, Meeting, Vol. 2019, pp. 283-291, August 2019.
[164] Kim Y, Sun J, Yu H, Jiang X. "Federated tensor factorization for computational phenotyping." In Proceedings of the 23rd ACM SIGKDD International conference on knowledge discovery and data mining, pp. 887-895, August 2017.
[165] Brisimi TS, Chen R, Mela T, Olshevsky A, Paschalidis IC, Shi W. "Federated learning of predictive models from federated electronic health records." International journal of medical informatics, Vol. 112, pp. 59-67, April 2018.
[166] Huang L, Shea AL, Qian H, Masurkar A, Deng H, Liu D. "Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records." Journal of biomedical informatics, Vol. 99, November 2019.
[167] Sharma P, Shamout FE, Clifton DA. "Preserving patient privacy while training a predictive model of in-hospital mortality." arXiv preprint arXiv:1912.00354, December 2019.
[168] Boughorbel S, Jarray F, Venugopal N, Moosa S, Elhadi H, Makhlouf M. "Federated uncertainty-aware learning for distributed hospital ehr data." arXiv preprint arXiv:1910.12191, October 2019.

[DOI: 10.61186/jsdp.21.3.23]

challenge 2015: reducing false arrhythmia alarms in the ICU." In 2015 Computing in Cardiology Conference (CinC), pp. 273-276, September 2015.

[181] Detrano R, Janosi A, Steinbrunn W, Pfisterer M, Schmid JJ, Sandhu S, Guppy KH, Lee S, Froelicher V. "International application of a new probability algorithm for the diagnosis of coronary artery disease." The American journal of cardiology, Vol. 64 Issue 5, pp.304-310, August 1989.

[182] Smith JW, Everhart JE, Dickson WC, Knowler WC, Johannes RS. "Using the ADAP learning algorithm to forecast the onset of diabetes mellitus." InProceedings of the annual symposium on computer application in medical care, American Medical Informatics Association, pp. 261-265, November 1988.

[183] Li S, Cheng Y, Liu Y, Wang W, Chen T. "Abnormal client behavior detection in federated learning." arXiv preprint arXiv:1910.09933. October 2019.

[184] Huang L, Yin Y, Fu Z, Zhang S, Deng H, Liu D. "LoAdaBoost: Loss-based AdaBoost federated machine learning with reduced computational complexity on IID and non-IID intensive care data." Plos one, Vol. 15, April 2020.

[185] Fallahpour A, Barri K, Wong KY, Jiao P, Alavi AH. "An integrated data mining approach to predict electrical energy consumption." International Journal of Bio-Inspired Computation, Vol. 17, pp. 142-153, April 2021.

[186] Cai X, Cao Y, Ren Y, Cui Z, Zhang W. "Multi-objective evolutionary 3D face reconstruction based on improved encoder–decoder network." Information Sciences, Vol. 581, pp. 233-248, December 2021.

[187] Zhang Z, Cao Y, Cui Z, Zhang W, Chen J. "A many-objective optimization based intelligent intrusion detection algorithm for enhancing security of vehicular networks in 6G." IEEE Transactions on Vehicular Technology, Vol. 70 Issue 6, pp. 5234-5243, February 2021.

[188] Ko I, Chambers D, Barrett E. "Recurrent autonomous autoencoder for intelligent DDoS attack mitigation within the ISP domain." International journal of machine learning and cybernetics, Vol. 12, pp. 3145-3167, November 2021.

[189] Al-Hazaimeh OM, Al-Jamal MF, Alomari AK, Bawaneh MJ, Tahat N. "Image encryption using anti-synchronisation and Bogdanov transformation map." International Journal of Computing Science and Mathematics, Vol. 15, pp.43-59, April 2022.

[190] Qin Z, Li GY, Ye H. "Federated learning and wireless communications." IEEE Wireless Communications, Vol. 28 Issue 5, pp. 134-140, September 2021.

[191] Yang M, Qian H, Wang X, Zhou Y, Zhu H. "Client selection for federated learning

[169] Silva S, Gutman BA, Romero E, Thompson PM, Altmann A, Lorenzi M. "Federated learning in distributed medical databases: Meta-analysis of large-scale subcortical brain data." In 2019 IEEE 16th international symposium on biomedical imaging (ISBI 2019), pp. 270-274, April 2019.

[170] Pfohl SR, Dai AM, Heller K. "Federated and differentially private learning for electronic health records." arXiv preprint arXiv:1911.05861. November 2019.

[171] Lee JS, Darcy KM, Hu H, Casablanca Y, Conrads TP, Dalgard CL, Freymann JB, Hanlon SE, Huang GD, Kvecher L, Maxwell GL. "From discovery to practice and survivorship: building a national real-world data learning healthcare framework for military and veteran cancer patients." Clinical Pharmacology & Therapeutics, Vol. 106, pp. 52-57, July 2019.

[172] Johnson AE, Pollard TJ, Shen L, Lehman LW, Feng M, Ghassemi M, Moody B, Szolovits P, Anthony Celi L, Mark RG. "MIMIC-III, a freely accessible critical care database." Scientific data, Vol. 3, pp. 1-9, May 2016.

[173] Xu J, Xu Z, Walker P, Wang F. "Federated patient hashing." InProceedings of the AAAI Conference on Artificial Intelligence, Vol. 34, pp. 6486-6493, April 2020.

[174] Pollard TJ, Johnson AE, Raffa JD, Celi LA, Mark RG, Badawi O. "The eICU Collaborative Research Database, a freely available multi-center database for critical care research." Scientific data, Vol. 5, pp. 1-13, September 2018.

[175] Vaid A, Jaladanki SK, Xu J, Teng S, Kumar A, Lee S, Somani S, Paranjpe I, De Freitas JK, Wanyan T, Johnson KW. "Federated learning of electronic health records improves mortality prediction in patients hospitalized with COVID-19." MedRxiv. August 2020.

[176] Chen Y, Qin X, Wang J, Yu C, Gao W. "Fedhealth: A federated transfer learning framework for wearable healthcare." IEEE Intelligent Systems, Vol. 35 Issue 4, pp. 83-93, April 2020.

[177] Choudhury O, Gkoulalas-Divanis A, Salonidis T, Sylla I, Park Y, Hsu G, Das A. "Differential privacy-enabled federated learning for sensitive health data." arXiv preprint arXiv:1910.02578. October 2019.

[178] Choudhury O, Park Y, Salonidis T, Gkoulalas-Divanis A, Sylla I. "Predicting adverse drug reactions on distributed health data using federated learning." In AMIA Annual symposium proceedings, Vol. 2019, pp. 313-322, 2019(Published online March 2020).

[179] Yuan B, Ge S, Xing W. "A federated learning framework for healthcare iot devices." arXiv preprint arXiv:2005.05083, May 2020.

[180] Clifford GD, Silva I, Moody B, Li Q, Kella D, Shahin A, Kooistra T, Perry D, Mark RG. "The PhysioNet/computing in cardiology

[DOI: 10.61186/jsdp.21.3.23]

with label noise." IEEE Transactions on Vehicular Technology, Vol. 71 Issue 2, pp. 2193-2197, December 2021.
[192] Peng W, Lin J, Ma X. "A bi-objective optimisation approach for the critical chain project scheduling problem." International Journal of Computing Science and Mathematics, Vol. 13, pp. 311-330, September 2021.
[193] Wang L, Pan Z, Wang J. "A review of reinforcement learning based intelligent optimization for manufacturing scheduling." Complex System Modeling and Simulation, Vol. 1 Issue 4, pp. 257-270, December 2021.
[194] Wu X, Cao Z, Wu S. "Real-time hybrid flow shop scheduling approach in smart manufacturing environment." Complex System Modeling and Simulation, Vol. 1 Issue 4, pp. 335-350, December 2021.
[195] Cai X, Wang P, Cui Z, Zhang W, Chen J. "Weight convergence analysis of DV-hop localization algorithm with GA." Soft Computing, Vol. 24, pp. 18249-18258, December 2020.
[196] Bai H, Fan T, Niu Y, Cui Z. "Multi-UAV cooperative trajectory planning based on many-objective evolutionary algorithm." Complex System Modeling and Simulation, Vol. 2 Issue 2, pp. 130-141, June 2022.
[197] Lv D. "Scale parameter recognition of blurred moving image based on edge combination algorithm." International Journal of Computing Science and Mathematics, Vol. 15, pp. 168-182, June 2022.
[198] Swain D, Bijawe SS, Akolkar PP, Shinde A, Mahajani MV. "Diabetic retinopathy using image processing and deep learning." International Journal of Computing Science and Mathematics, Vol. 14, pp.397-409, 2021.
[199] Cai X, Zhang J, Ning Z, Cui Z, Chen J. "A many-objective multistage optimization-based fuzzy decision-making model for coal production prediction." IEEE Transactions on Fuzzy Systems, Vol. 29 Issue 12, pp.3665-3675, June 2021.
[200] Chen S, Zhang J, Bai Y, Xu P, Gao T, Jiang H, Gao W, Li X. "Blockchain Enabled Intelligence of Federated Systems (BELIEFS): An attack-tolerant trustable distributed intelligence paradigm." Energy Reports, Vol. 7, pp. 8900-8911, November 2021.
[201] Cui Z, Zhang J, Wu D, Cai X, Wang H, Zhang W, Chen J. "Hybrid many-objective particle swarm optimization algorithm for green coal production problem." Information Sciences, Vol. 518, pp. 256-271, May 2020.

هاله فاتح مدرک کارشناسی ارشد خود را از دانشگاه صنعتی خواجه نصیرالدین طوسی در سال ۱۳۹۹ دریافت کرد. ایشان در حال حاضر دانشجوی مقطع دکترای دانشکدهٔ مهندسی کامپیوتر دانشگاه صنعتی شاهرود است.
نشانی رایانامهٔ ایشان عبارت‌است از:
h.fateh@shahroodut.ac.ir

محسن رضوانی مدرک دکترای خود را از دانشگاه **UNSW** استرالیا در گرایش شبکه و امنیت در سال ۱۳۹۴ دریافت و مدرک کارشناسی ارشد خود را در گرایش مهندسی نرم‌افزار از دانشگاه صنعتی شریف و مدرک کارشناسی خود را در همین گرایش از دانشگاه صنعتی امیرکبیر دریافت کرده‌است. ایشان در حال حاضر دانشیار دانشکدهٔ مهندسی کامپیوتر دانشگاه صنعتی شاهرود است.
نشانی رایانامهٔ ایشان عبارت‌است از:
mrezvani@shahroodut.ac.ir

اسماعیل طحانیان مدرک کارشناسی و کارشناسی ارشد خود را از دانشگاه صنعتی خواجه نصیرالدین طوسی به ترتیب در سال‌های ۱۳۸۶و ۱۳۸۸ و مدرک دکترا را از دانشگاه شاهد تهران در سال ۱۳۹۵ دریافت کرد. ایشان در حال حاضر استادیار دانشکدهٔ مهندسی کامپیوتر دانشگاه صنعتی شاهرود است.
نشانی رایانامهٔ ایشان عبارت‌است از:
e.tahanian@shahroodut.ac.ir

[DOI: 10.61186/jsdp.21.3.23]