یادگیری شخصی برای برنامه‌های کاربردی IoT هوشمند: یک چارچوب مبتنی بر لبه ابر

مقدمه

اینترنت اشیا) (IoTبه طور گسترده‌ای در جنبه‌های مختلف زندگی مدرن نفوذ کرده‌است و بسیاری از سرویس‌ها و برنامه‌های IoT هوشمند در حال ظهور هستند. اخیرا، یادگیری متحد برای آموزش یک مدل به اشتراک گذاشته شده جهانی با بهره‌برداری از مقدار زیادی از نمونه‌های داده ایجاد شده توسط کاربر بر روی دستگاه‌های IoT در حالی که از نشت داده‌ها جلوگیری می‌کند، پیشنهاد شده‌است. با این حال، ناهمگونی دستگاه، آماری و مدل ذاتی در محیط‌های IoT پیچیده، چالش‌های بزرگی را برای یادگیری متحد سنتی ایجاد می‌کند، که استقرار مستقیم آن را نامناسب می‌سازد. در این مقاله، ما از یک چارچوب یادگیری متحد شخصی در یک معماری لبه ابر برای برنامه‌های IoT هوشمند دفاع می‌کنیم .

تعریف مسئله و هدف اصلی مقاله

در این مقاله، ما از یک چارچوب یادگیری متحد شخصی در یک معماری لبه ابر برای برنامه‌های IoTهوشمند دفاع می‌کنیم .برای مقابله با مسائل ناهمگونی در محیط‌هایIoT ، ما روش‌های یادگیری شخصی سازی شده در حال ظهور را بررسی می‌کنیم که قادر به کاهش اثرات منفی ناشی از ناهمگونی در جنبه‌های مختلف هستند .

گسترش دستگاه‌های هوشمند، شبکه‌های موبایل و فن‌آوری محاسبات، عصر جدیدی از اینترنت اشیا) (IoTرا به راه انداخته‌است، که آماده است تا پیشرفت‌های قابل‌توجهی در تمام جنبه‌های زندگی مدرن ما، از جمله سیستم بهداشت و درمان هوشمند، زیرساخت‌های حمل و نقل هوشمند و غیره ایجاد کند . با اتصال مقادیر زیادی از دستگاه‌های هوشمند به یکدیگر درIoT ، ما قادر به دسترسی به داده‌های عظیم کاربر برای به دست آوردن بینش، آموزش مدل‌های یادگیری ماشین وظیفه مشخص و به طور قانونی ارائه خدمات و محصولات هوشمند با کیفیت بالا هستیم .برای

دستیابی به مزایای داده‌های IoT ، رویکرد غالب جمع‌آوری داده‌های پراکنده کاربر به یک ابر مرکزی برای مدلسازی و سپس انتقال مدل آموزش‌دیده به دستگاه‌های کاربر برای استنتاج وظایف است .

تحت افزایش قوانین سخت گیرانه حفاظت از حریم خصوصی داده‌ها مانند مقررات عمومی حفاظت از داده) (GDPR[۳]، حرکت داده‌ها با مشکلات بی‌سابقه‌ای مواجه خواهد شد .یک جایگزین، آموزش و به روز رسانی مدل در هر دستگاه IoT با داده‌های محلی آن، جدا از سایر دستگاه‌ها است .با این حال، یک مانع کلیدی این رویکرد در تقاضای بالای منابع برای استقرار و آموزش مدل‌ها در دستگاه‌های IoT با منابع محاسباتی، انرژی و حافظه محدود نهفته‌است .

ضرورت تحقیق

از آنجایی که داده‌های حساس به کاربر برای آپلود به ابر راه دور مورد نیاز است، ممکن است حریم خصوصی زیادی را تحمیل کند .

تحت افزایش قوانین سخت گیرانه حفاظت از حریم خصوصی داده‌ها مانند مقررات عمومی حفاظت از داده حرکت داده‌ها با مشکلات بی‌سابقه‌ای مواجه خواهد شد .یک جایگزین، آموزش و به روز رسانی مدل در هر دستگاه IoT با داده‌های محلی آن، جدا از سایر دستگاه‌ها است .با این حال، یک مانع کلیدی این رویکرد در تقاضای بالای منابع برای استقرار و آموزش مدل‌ها در دستگاه‌های IoT با منابع محاسباتی، انرژی و حافظه محدود نهفته‌است .علاوه بر این، نمونه‌های ناکافی داده و انتقال داده‌های محلی منجر به یک مدل بدتر خواهد شد .

یک راه‌حل پیچیده برای مقابله با آموزش داده توزیع‌شده یادگیری متحد است که قادر به آموزش مشارکتی یک مدل مشترک با کیفیت بالا با جمع‌آوری و میانگین گیری به روز رسانی های محاسبه‌شده محلی آپلود شده توسط دستگاه‌های IoT است

شاخه حل جاری

چالش‌های اصلی یادگیری در IOTرا آموزش می‌دهند. در این بخش، ما ابتدا چالش‌های اصلی و اثرات منفی بالقوه را هنگام استفاده از یادگیری متحد سنتی در محیط‌های IoT شرح می‌دهیم .

DEVICE HETEROGENEITY

معمولا تعداد زیادی از دستگاه‌های IoT وجود دارند که از نظر سخت‌افزار (پردازنده، حافظه)، شرایط شبکه(WiFi ، G۴ ، G۳)و توان (سطح باتری)در کاربردهای IoT متفاوت هستند، که منجر به ظرفیت‌های محاسباتی، ذخیره‌سازی و ارتباطی متنوعی می‌شوند . بنابراین، چالش‌های عدم تجانس دستگاه در یادگیری متحد، مانند هزینه ارتباطی بالا، موانع و تلورانس خطا ایجاد می‌شود .در تنظیمات متحد، هزینه‌های ارتباطی محدودیت‌های اصلی با توجه به این واقعیت هستند که دستگاه‌های IoT اغلب آفلاین یا بر روی اتصالات آهسته یا گران‌قیمت هستند .

در فرآیند یادگیری متحد که یک به روز رسانی همزمان را انجام می‌دهد، دستگاه‌های با ظرفیت محاسباتی محدود می‌توانند سرگردان شوند زیرا آن‌ها زمان بیشتری برای گزارش به روز رسانی های مدل خود نسبت به دستگاه‌های دیگر در همان دور صرف می‌کنند .

STATISTICAL HETEROGENEITY

یک کار نظارت شده با ویژگی‌های x و برچسب y را در نظر بگیرید، توزیع داده‌های محلی کاربر i می‌تواند به صورت زیر نمایش داده شود .($P_i(x, y)$)

همان طور,As $Pi\,(x, y) = Pi\,(y|x)Pi\,(x) = Pi\,(x|y)Pi\,(y)$ داده‌های کاربر می‌توانند در بسیاری از اشکال غیر IID باشند، مانند انحراف توزیع ویژگی، انحراف توزیع برچسب و تغییر مفهوم.

به عنوان مثال، در کاربردهای مراقبت‌های بهداشتی، توزیع داده‌های فعالیت کاربران تا حد زیادی با توجه به ویژگی‌های فیزیکی متنوع کاربران و عادات رفتاری (انحراف توزیع ویژگی)متفاوت است .علاوه بر این، تعداد نمونه‌های داده در میان دستگاه‌ها ممکن است به طور قابل‌توجهی متفاوت باشد . این نوع ناهمگونی آماری در محیط‌های IoT پیچیده فراگیر است .برای پرداختن به این چالش عدم تجانس، رویکرد یادگیری متحد متعارف، کنترل متحد (فدوآوگ)، نشان داده می‌شود که قادر به کار با داده‌های خاص غیر IID است .با این حال، فدینگ آوگ ممکن است منجر به عملکرد به شدت تخریب‌شده در هنگام مواجهه با توزیع داده‌های بسیار نامتوازن شود .به طور خاص، از یک سو، داده‌های غیر IID منجر به اختلاف وزن بین فرآیند یادگیری متحد و فرآیند آموزش متمرکز سنتی خواهد شد، که نشان می‌دهد که فدوگ در نهایت یک مدل بدتر از روش‌های متمرکز به دست خواهد آورد و در نتیجه منجر به عملکرد ضعیف خواهد شد.

MODEL HETEROGENEITY

در چارچوب یادگیری متحد اصلی، دستگاه‌های شرکت‌کننده باید بر روی یک معماری خاص از مدل آموزشی به توافق برسند به طوری که مدل جهانی را بتوان به طور موثر با جمع‌آوری وزن‌های مدل جمع‌آوری‌شده از مدل‌های محلی به دست آورد .در چارچوب یادگیری متحد اصلی، دستگاه‌های شرکت‌کننده باید بر روی یک معماری خاص از مدل آموزشی به توافق برسند به طوری که مدل جهانی را بتوان به طور موثر با جمع‌آوری وزن‌های مدل جمع‌آوری‌شده از مدل‌های محلی به دست آورد .در نتیجه، معماری‌های مدل از مدل‌های محلی مختلف اشکال مختلفی را نشان می‌دهند، که انجام تجمع ساده توسط یادگیری متحد سنتی را غیر ممکن می‌سازد. در نتیجه، معماری‌های مدل از مدل‌های

محلی مختلف اشکال مختلفی را نشان می‌دهند، که انجام تجمع ساده توسط یادگیری متحد سنتی را غیر ممکن می‌سازد. در نتیجه، معماری‌های مدل از مدل‌های محلی مختلف اشکال مختلفی را نشان می‌دهند، که انجام تجمع ساده توسط یادگیری متحد سنتی را غیر ممکن می‌سازد

CLOUD-EDGE FRAMEWORK FOR PERSONALIZED FEDERATED LEARNING

همانطور که در بخش ۲ توضیح داده شد، عدم تجانس دستگاه، عدم تجانس آماری و عدم تجانس مدل در برنامه‌های کاربردی IoT وجود دارد، که چالش‌های بزرگی برای یادگیری متحد سنتی ایجاد می‌کند .یک راه‌حل موثر برای پرداختن به این مسائل ناهمگونی می‌تواند به شخصی سازی ختم شود .با ابداع و استفاده از روش‌های یادگیری متحد پیشرفته‌تر، هدف ما این است که انعطاف‌پذیری زیادی ایجاد کنیم به طوری که دستگاه‌های فردی بتوانند مدل‌های شخصی خود را ایجاد کنند تا نیازهای منبع و کاربرد خود را برآورده کنند و در عین حال از مزیت یادگیری متحد برای به اشتراک گذاری دانش جمعی لذت ببرند .در این مقاله، ما از یک چارچوب یادگیری متحد شخصی برای برنامه‌های کاربردی IoT هوشمند برای مقابله با چالش‌های ناهمگونی به شیوه‌ای جامع دفاع می‌کنیم .

همان طور که در شکل۱ نشان‌داده شده‌است .چارچوب PerFit پیشنهادی ما یک معماری لبه ابر را اتخاذ می‌کند، که توان محاسباتی لبه مورد نیاز را در نزدیکی دستگاه‌های IoT به ارمغان می‌آورد .

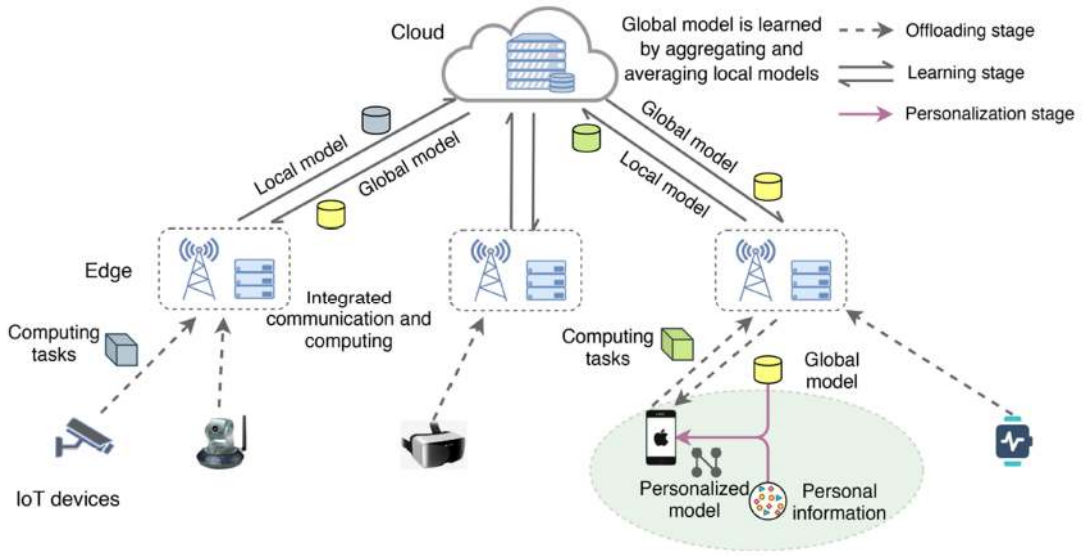


FIGURE 1. The personalized federated learning framework for intelligent IoT applications, which supports flexible selection of personalized federated learning approaches.

به طور خاص، فرآیند یادگیری مشارکتی در PerFit اساسا شامل سه مرحله زیر است که در شکل نشان‌داده شده‌است

۱. مرحله تهاجم: هنگامی که لبه قابل‌اعتماد است (به عنوان مثال، دروازه لبه در خانه)، کاربر دستگاه IoT می‌تواند کل مدل یادگیری و نمونه‌های داده خود را برای محاسبات سریع به لبه تخلیه کند . در غیر این صورت، کاربر دستگاه با نگه داشتن لایه‌های ورودی و نمونه‌های داده آن به صورت محلی بر روی دستگاه خود و تخلیه لایه‌های مدل باقی مانده به لبه برای محاسبات مشترک لبه - دستگاه، پارتیشن بندی مدل را انجام خواهد داد .

مرحله یادگیری: دستگاه و لبه به طور مشترک مدل محلی را براساس نمونه‌های داده‌های شخصی محاسبه می‌کنند و سپس اطلاعات مدل محلی را به سرور ابری ارسال می‌کنند . سرور ابری اطلاعات مدل محلی ارائه‌شده توسط لبه‌های شرکت‌کننده را جمع‌آوری می‌کند و آن‌ها را در یک مدل جهانی برای بازگرداندن به لبه‌ها میانگین گیری می‌کند . سرور ابری اطلاعات مدل محلی

ارائه‌شده توسط لبه‌های شرکت‌کننده را جمع‌آوری می‌کند و آن‌ها را در یک مدل جهانی برای بازگرداندن به لبه‌ها میانگین گیری می‌کند .

مرحله شخصی سازی: برای در نظر گرفتن ویژگی‌ها و الزامات شخصی خاص، هر دستگاه یک مدل شخصی را براساس اطلاعات مدل جهانی و اطلاعات شخصی خودش (به عنوان مثال، داده‌های محلی)آموزش می‌دهد .عملیات یادگیری خاص در این مرحله به مکانیزم یادگیری متحد شخصی اتخاذ شده بستگی دارد که در بخش بعدی توضیح داده خواهد شد .چارچوب PerFit پیشنهادی از محاسبات لبه برای تقویت قابلیت محاسبات دستگاه‌های منفرد از طریق محول سازی محاسبات برای کاهش اثر سرگردان استفاده می‌کند .

چارچوب PerFit پیشنهادی از محاسبات لبه برای تقویت قابلیت محاسبات دستگاه‌های منفرد از طریق محول سازی محاسبات برای کاهش اثر سرگردان استفاده می‌کند .اگر ما تراکم مدل محلی را در سرور لبه انجام دهیم، همچنین به کاهش سربار ارتباطی با اجتناب از دستگاه‌های عظیم برای ارتباط مستقیم با سرور ابری بر روی پهنای باند شبکه ستون فقرات گران‌قیمت کمک می‌کند [۱۵] .علاوه بر این، با انجام شخصی سازی، می‌توانیم مدل‌های شخصی سبک‌وزن را در برخی از دستگاه‌های محدود کننده منابع (به عنوان مثال، با اصلاح مدل یا یادگیری انتقال)گسترش دهید . این امر به کاهش عدم تجانس دستگاه در منابع ارتباطی و محاسباتی کمک می‌کند .همچنین، ناهمگونی آماری و ناهمگونی مدل می‌تواند به خوبی پشتیبانی شود، زیرا ما می‌توانیم مدل‌ها و مکانیزم‌های شخصی سازی شده را برای دستگاه‌های فردی مختلف متناسب با ویژگی‌های داده‌های محلی آن‌ها، نیازمندی‌های برنامه کاربردی و محیط‌های استقرار استفاده کنیم. این امر به کاهش عدم تجانس دستگاه در منابع ارتباطی و محاسباتی کمک می‌کند . همچنین، ناهمگونی آماری و ناهمگونی مدل می‌تواند به خوبی پشتیبانی شود، زیرا ما می‌توانیم مدل‌ها و مکانیزم‌های شخصی سازی شده را برای دستگاه‌های فردی مختلف متناسب با

ویژگی‌های داده‌های محلی آن‌ها، نیازمندی‌های برنامه کاربردی و محیط‌های استقرار استفاده کنیم.

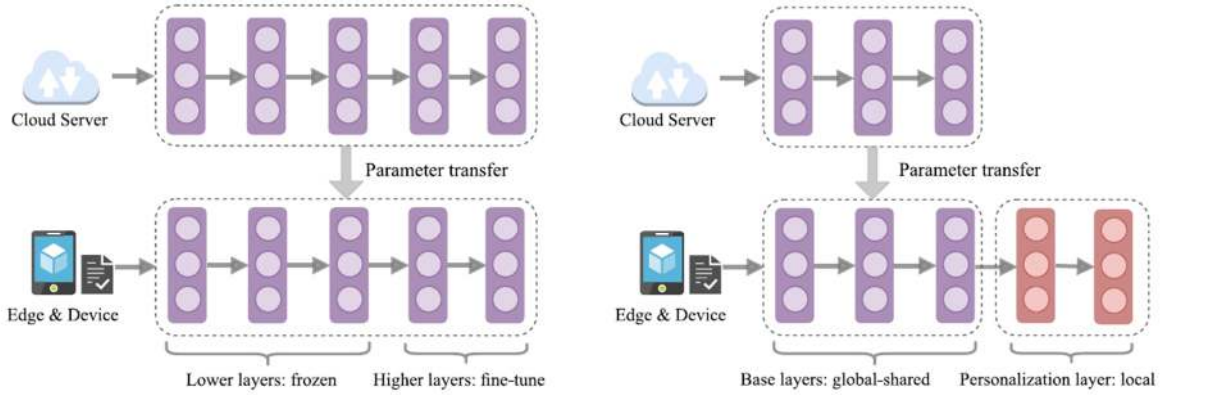
چندین مکانیزم یادگیری متحد شخصی شده کلیدی را بررسی و تشریح می‌کنیم که می‌توانند با چارچوب PerFit برای برنامه‌های IoT هوشمند ترکیب شوند.

این طرح‌های یادگیری متحد شخصی را می توان طبقه‌بندی کرد .

با یادگیری انتقال متحد، فرایادگیری متحد، یادگیری چند وظیفه‌ای متحد و تقطیر متحد، که به شرح زیر توضیح داده خواهد شد .

FEDERATED TRANSFER LEARNING

در تنظیمات یادگیری متحد، دامنه‌ها اغلب متفاوت اما مرتبط هستند، که انتقال دانش را ممکن می‌سازد .ایده اصلی یادگیری انتقال متحد، انتقال مدل مشترک جهانی به دستگاه‌های IoT توزیع شده‌برای شخصی سازی بیشتر به منظور کاهش ناهمگونی آماری) توزیع‌های داده غیر(IID ذاتی در یادگیری متحد است .با توجه به معماری شبکه‌های عصبی عمیق و اضافه‌بار ارتباطات، دو رویکرد اصلی برای شخصی سازی از طریق یادگیری انتقال متحد وجود دارد . بر این اساس، هر دستگاه قادر به ساخت مدل شخصی با اصلاح مدل جهانی با داده‌های محلی خود می‌باشد .برای کاهش سربار آموزشی، به جای بازآموزی کل مدل، تنها پارامترهای مدل لایه‌های مشخص به خوبی تنظیم خواهند شد .همانطور که در شکل ۲ مشخص است.



(a) The whole trained global model in the cloud server is transferred to the device for personalization with its local data.

(b) The device model is combined with the part of model transferred from cloud server and the personalization layers owned by users locally.

FEDERATED META LEARNING

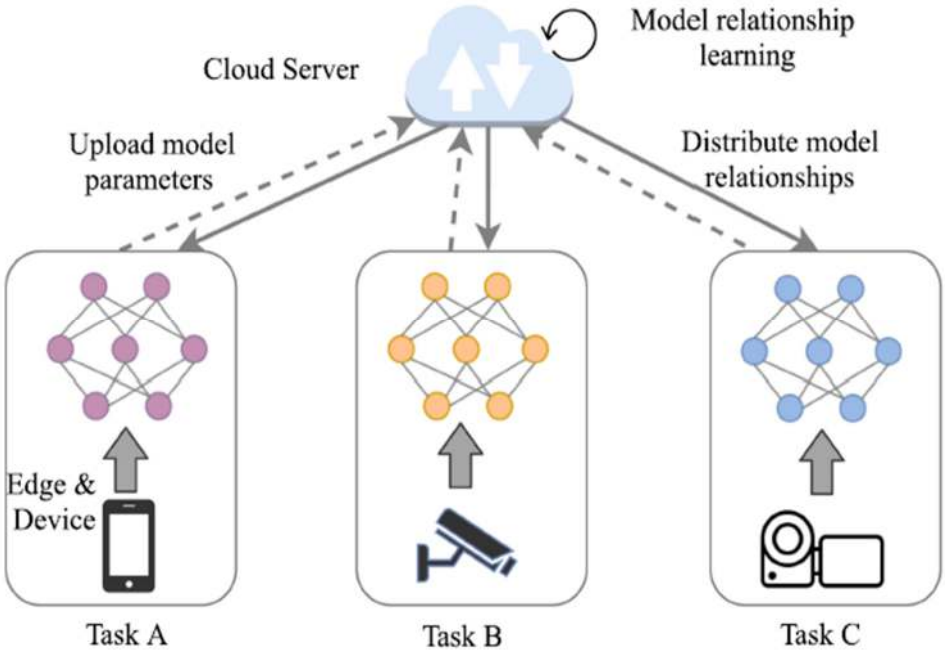
یادگیری متحد در محیط‌های IoT به طور کلی با ناهمگونی آماری مانند عدم IID و توزیع داده‌های نامتعادل مواجه است، که تضمین یک عملکرد با کیفیت بالا برای هر دستگاه IoT شرکت‌کننده را به چالش می‌کشد .برای مقابله با این مشکل، برخی از محققان بر روی بهبود الگوریتم FADAVG با اعمال نفوذ در قدرت شخصی سازی فرایادگیری تمرکز می‌کنند .در فرایادگیری، مدل توسط یک فرا یادگیرنده آموزش‌دیده است که قادر به یادگیری تعداد زیادی از کاره‌ای مشابه است و هدف مدل آموزش‌دیده این است که به سرعت با یک کار مشابه جدید از مقدار کمی از داده‌های جدید سازگار شود. در فرایادگیری، مدل توسط یک فرا یادگیرنده آموزش‌دیده است که قادر به یادگیری تعداد زیادی از کاره‌ای مشابه است و هدف مدل آموزش‌دیده این است که به سرعت با یک کار مشابه جدید از مقدار کمی از داده‌های جدید سازگار شود

FEDERATED MULTI-TASK LEARNING

به طور کلی، هدف یادگیری انتقال متحد و فرایادگیری متحد، یادگیری یک مدل مشترک از وظایف مشابه یا مشابه در میان دستگاه‌های IoT با شخصی سازی با تنظیم دقیق است .در راستای یک خط متفاوت، هدف یادگیری چند وظیفه متحد شده، یادگیری وظایف متمایز برای دستگاه‌های مختلف به طور همزمان است و تلاش می‌کند تا روابط مدل میان آن‌ها را بدون خطر

حریم خصوصی به دست آورد . از طریق روابط مدل، مدل هر دستگاه ممکن است قادر به دستیابی به اطلاعات دستگاه دیگر باشد .علاوه بر این، مدل یاد شده برای هر دستگاه همیشه شخصی سازی شده‌است .

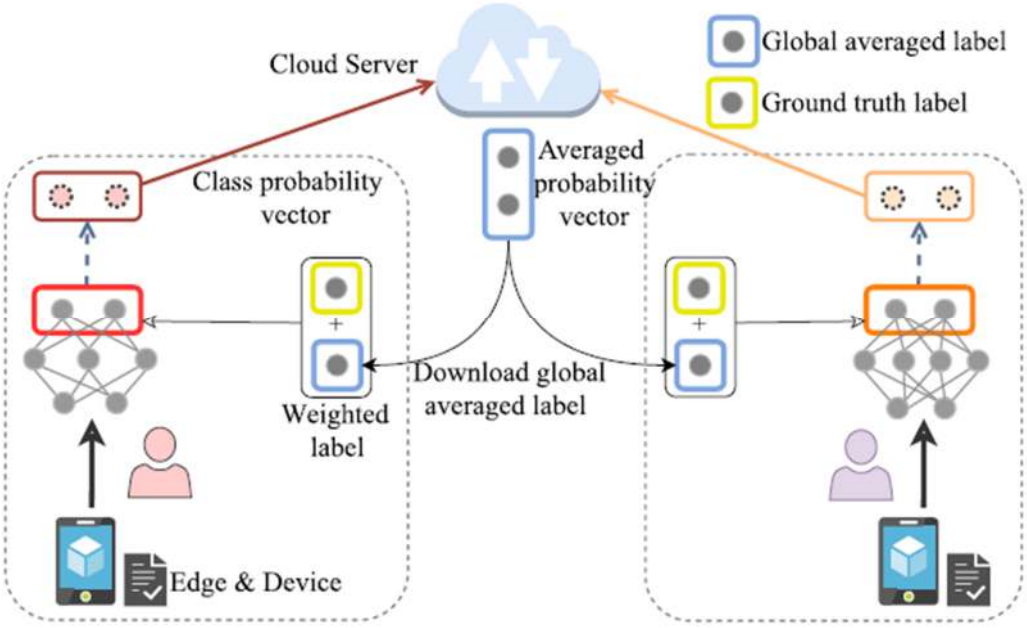
همانطور که در شکل ۳ نشان داده شده است ، در فرآیند آموزش یادگیری چند وظیفه‌ای متحد، سرور ابری روابط مدل را در میان وظایف یادگیری چندگانه براساس پارامترهای مدل آپلود شده توسط دستگاه‌های IoT یاد می‌گیرد .و سپس هر دستگاه می‌تواند پارامترهای مدل خود را با داده‌های محلی و روابط مدل فعلی به روز رسانی کند



FEDERATED DISTILLATION

در چارچوب یادگیری متحد اصلی، همه مشتریان (به عنوان مثال، یال‌ها و دستگاه‌های شرکت‌کننده)باید بر روی یک معماری خاص از مدل آموزش‌دیده بر روی هر دو سرور جهانی و مشتریان محلی توافق کنند .با این حال، در برخی محیط کسب‌وکار واقع گرایانه، مانند بهداشت و درمان و امور مالی، هر شرکت‌کننده ظرفیت و تمایل به طراحی مدل منحصر به فرد خود را دارد، و ممکن است به دلیل مسائل حریم خصوصی و مالکیت معنوی مایل به به اشتراک گذاشتن جزئیات مدل نباشد .این نوع ناهمگونی مدل چالش جدیدی برای یادگیری متحد سنتی ایجاد می‌کند . مرحله ترجمه دانش می‌تواند با تقطیر دانش اجرا شود، برای مثال، با استفاده از احتمالات کلاس تولید شده توسط مدل مشتری به عنوان فرمت استاندارد همانطور که در شکل نشان‌داده شده‌است .

طبق شکل ۴



در اینجا، شایان‌ذکر است که برای انجام تقطیر دانش در یادگیری متحد، یک مجموعه داده عمومی مورد نیاز است زیرا خروجی‌های معلم و دانش‌آموز باید با استفاده از یک نمونه داده آموزشی یک‌سان ارزیابی شوند .

DATA AUGMENTATION

از آنجا که داده‌های شخصی ایجاد شده توسط کاربر به طور طبیعی نوع توزیع بسیار نامتوازن و غیر IID را نشان می‌دهد که ممکن است عملکرد مدل را تا حد زیادی تنزل دهد، کاره‌ای در حال ظهور با تمرکز بر افزایش داده برای تسهیل یادگیری متحد شخصی وجود دارد .

یک استراتژی به اشتراک گذاری داده را با توزیع مقدار کمی از داده‌های جهانی شامل یک توزیع یکنواخت بر روی کلاس‌ها از ابر به مشتریان لبه پیشنهاد کردند . به این ترتیب، توزیع بسیار نامتعادل داده‌های مشتری می‌تواند تا حدی کاهش یابد و سپس عملکرد مدل شخصی سازی می‌تواند بهبود یابد . با این حال، توزیع مستقیم داده‌های جهانی به مشتریان حاشیه، خطر نشت حریم خصوصی زیادی را تحمیل خواهد کرد، این رویکرد برای ایجاد توازن بین حفاظت از حریم خصوصی داده‌ها و بهبود عملکرد مورد نیاز است .

ارزیابی و بررسی

در مطالعه ی این مقاله یادگیری شخصی برای برنامه‌های کاربردی IoT هوشمنددریک چارچوب مبتنی بر لبه ابررا بررسی کردیم.که از یک از یک چارچوب یادگیری متحد شخصی در یک معماری لبه ابر برای برنامه‌های IoT هوشمند استفاده کردیم.

جمع بندی

در این مقاله، ، یک چارچوب یادگیری متحد شخصی را در یک معماری لبه ابر برای برنامه‌های IoT هوشمند با حفاظت از حریم خصوصی داده‌ها پیشنهاد می‌کنیم .با جمع‌آوری به روز رسانی های محلی از دستگاه‌های IoT توزیع‌شده و استفاده از مزایای محاسبات لبه، امکان یادگیری یک مدل مشترک جهانی را فراهم می‌کند .برای مقابله با ناهمگونی دستگاه، آماری، و مدل در محیط‌های IoT، PerFitبه طور طبیعی می‌تواند انواع روش‌های یادگیری متحد شخصی شده را ادغام کند و در نتیجه به شخصی سازی و افزایش عملکرد برای دستگاه‌ها در برنامه‌های کاربردی IoT دست یابد .ما اثربخشی PerFit را از طریق مطالعه موردی وظیفه شناسایی فعالیت انسان نشان می‌دهیم، که تایید می‌کند PerFit می‌تواند یک رویکرد امیدوار کننده برای توانمندسازی بسیاری از برنامه‌های کاربردی IoT هوشمند باشد .