حفظ حریم خصوصی چالش های یادگیری ماشین و رویکرد راه حل برای آموزش داده ها در سیستم های ERP

چکیده

تحول دیجیتال در همه جا وجود دارد و باعث می شود شرکت های ERP الگوریتم های یادگیری ماشین بیشتری را در اختیار داشته باشند تا بتوانند از طریق آن قابلیت های هوشمندانه تصمیم گیری در زمان واقعی را در اختیار داشته باشند. سیستم های ERP با استفاده از داده های عظیم سازمانی ، ابر و قابلیت های محاسبه ، موارد استفاده از یادگیری ماشین را ترکیب کرده اند. با این حال ، حفظ حریم خصوصی داده ها همچنان یک چالش است. حریم خصوصی داده ها هسته اصلی مدل یادگیری ماشین است که روی اطلاعات حساس کاربرد دارد. این نه تنها برای مشاغل سودآور ، بلکه اگر در قالب حفظ حریم خصوصی به اطلاعات حساس پزشکی دسترسی نداشته باشند ، حتی تلاش های دانشگاهی در زمینه پزشکی نیز نمی توانند پیشرفت کنند. استفاده از یک مدل ML بدون حتی درک کامل آنچه در لایه های پنهان آن اتفاق می افتد ، می تواند فاجعه بار باشد و خطرات ناشی از آن منجر به عواقب قانونی شود. بنابراین ، در چند سال گذشته تکنیک های حفظ حریم خصوصی هوش مصنوعی در حال تکامل هستند. حوزه حفظ حریم خصوصی هوش مصنوعی هنوز در حال رشد است و در سازمان ها و افراد یک شکاف تفاهم وجود دارد که باعث می شود حریم خصوصی نقض یا مصالحه شود که این یک چالش گسترده کسب و کار است. این مقاله بر روی چالشهای اساسی شرکتهای ERP تا آنجا که به مدلهای یادگیری ماشین آموزش داده های سازمانی آنها مربوط می شود و اینکه چگونه می توان با استفاده از ناشناس سازی داده ها و تکنیک های حفظ حریم خصوصی ، بر این چالش ها غلبه کرد تمرکز دارد.

مقدمه

اطلاعات شخصی در هنگام ارائه کالا یا خدماتی که برای کاربر شخصی سازی شده است تا ارزش بیشتری به کالاها و خدمات بدهد ، توسط یک کسب و کار جمع آوری می شود. این اطلاعات جمع آوری شده می تواند ویژگی های کل ، بیومتریک - فیزیولوژیکی ، بیولوژیکی یا رفتاری از جمله DNA باشد که می تواند به تنهایی یا در ترکیب با یکدیگر یا با سایر داده های شناسایی برای تعیین هویت فردی استفاده شود. اطلاعات بیومتریک شامل تصاویر عنبیه ، شبکیه ، اثر انگشت ، صورت ، دست ، کف دست ، الگوهای رگ و ضبط صدا است ، که از آنها یک الگوی شناسایی ، مانند چاپ صورت ، یک قالب کوچک ، یا می توان یک اثر صوتی را استخراج کرد و الگوهای ضربه کلید یا ریتم ها ، الگوی راه رفتن و داده های مربوط به خواب ، سلامتی یا ورزش که حاوی اطلاعات شناسایی هستند را می توان استخراج کرد. این اطلاعات می تواند به سازمان ها کمک کند تا مشتریان با ارزش را شناسایی کنند ، رفتارهای آینده را پیش بینی کنند و تصمیمات مبتنی بر بینش را فراتر از آنچه در سیستم های پشتیبانی تصمیم ممکن است ، فراهم نمایند. با ظهور قابلیت های محاسبه و ذخیره سازی همراه با افزایش چشمگیر داده ها ، سازمان ها از هوش مصنوعی که عمدتا تکنیک های یادگیری ماشین را به کار می برند استفاده می کنند .آن ها از الگوریتم های پیچیده آموزش داده های گذشته استفاده می کنند و روابط پنهان را برای ساخت مدل هایی که می توانند توسط سازمان ها برای پیش بینی کسب و کار استفاده شوند ، درک می کنند. نتایج استفاده از الگوریتم های ML در سال های اخیر برای کشف فرصت های جدید تجاری و مدل های تجاری جذابیت زیادی پیدا کرده است تا حدی که حریم خصوصی اطلاعات شخصی کاربر ، که در هسته اصلی آن است ، به خطر می افتد. این موضوع منجر به تدوین مقررات مختلف مانند به عنوان GDPR(Europe), CCPA(California) و برخی دیگر از قوانین حریم خصوصی که سازمان ها را مجبور می کند امنیت و حریم خصوصی را به خاطر منافع خود جدی بگیرند. این امر منجر به حفظ حریم خصوصی مدلهای AI / ML می شود. به طور گسترده اذعان شده است که نیاز به محافظت از حریم شخصی در "عصر داده های بزرگ" و احتمال موفقیت در آینده با استفاده از تکنیک هایی که امکان محاسبه داده های رمزگذاری شده را دارند ، تأیید می شود . حوزه حفظ حریم خصوصی هوش مصنوعی هنوز در حال رشد است و در سازمان ها و افراد یک شکاف تفاهم وجود دارد که باعث می شود حریم خصوصی نقض یا مصالحه شود ، یک چالش گسترده کسب و کار است. امروزه تحول دیجیتالی سازمان ها را مجبور به استفاده از فن آوری های یادگیری ماشین در سیستم های مختلف سازمانی می کند و سیستم های ERP نیز از این قاعده مستثنی نیستند ، اکثر سیستم های ERP شروع به ارائه قابلیت های یادگیری ماشین می کنند ، اما حفظ حریم خصوصی هنوز چشمگیر است. روشهای یادگیری ماشین مانند حریم خصوصی تشخیص دهنده و k-anonymization تا حد زیادی مورد توجه قرار گرفته است اما اجرای آنها در سیستمهای ERP در مرحله نوپایی است

پیشینه تحقیق

حریم خصوصی داده ها در هسته اصلی یک مدل یادگیری ماشین است که در مورد اطلاعات حساس آموزش دیده است. نه فقط برای مشاغل سودآور ، بلکه اگر در قالب حفظ حریم خصوصی به اطلاعات حساس پزشکی دسترسی نداشته باشند ، حتی تلاش های دانشگاهی در زمینه پزشکی نیز نمی توانند پیشرفت کنند. استفاده از یک مدل ML بدون حتی درک کامل آنچه در لایه های پنهان آن اتفاق می افتد ، می تواند فاجعه بار باشد و خطرات ناشی از آن منجر به عواقب قانونی شود. یک نقطه شروع برای حفظ حریم خصوصی ، ناشناس سازی داده ها در مجموعه آموزش است که تمام اطلاعات قابل شناسایی شخصی را حذف می کند. نتفلیکس میزبان یک چالش میلیون دلاری برای انجمن علوم داده بود که شامل بررسی فیلم های ناشناس 500000 کاربر ناشناس برای 17،770 فیلم بود. با این حال ، آرویند نارایانان و ویتالی شماتیکوف با استفاده از داده های موجود در دسترس پایگاه داده فیلم های اینترنتی (IMDB) ، تکنیک قوی Deanonymizationرا به نمایش گذاشتند و سوابق Netflix کاربران شناخته شده و سایر اطلاعات بالقوه حساس را با موفقیت شناسایی کردند. تحقیق C. Dwork در مورد حریم خصوصی تشخیص دهنده نشان می دهد که این یک مفهوم از حریم خصوصی متناسب با تجزیه و تحلیل داده های خصوصی است ، جایی که هدف یادگیری اطلاعات مربوط به کل جمعیت است ، در حالی که از حریم خصوصی هر فرد محافظت می کند ، حریم خصوصی تشخیص دهنده تضمین می کند که سیستم اساساً همان رفتار را خواهد داشت ، فارغ از اینکه هر فردی به پایگاه داده وارد یا از آن خارج شود. به طور شهودی ، داده های هیچ فردی تأثیر زیادی بر توزیع خروجی مکانیسم ندارد.سازمانهایی که وظیفه نگهداری اطلاعات شخصی آنها را دارند ، اعم از سلامتی بیمار یا سایر داده ها ، از توانایی خود در یادگیری ماشین (ML) بدبین هستند ، بخشی از این امر به دلیل عدم شفافیت در سیاست های استفاده از چنین داده هایی است و بخشی نیز به دلیل ترس از نقض ناآگاهانه حریم خصوصی افراد که ممکن است در روند استخراج چنین اطلاعاتی رخ دهد

**چالش های موجود در حفظ حریم خصوصی یادگیری ماشین در سیستم های ERP**

تبدیل مدل یادگیری ماشین به حفظ حریم خصوصی با حفظ مدل هوش مصنوعی چالش های بی شماری وجود دارد مانند:

* آموزش مهندسی معکوس داده ها
* مدل وزن یا ابر پارامتر مدل stealing
* مدل stealing
* حفظ Backdoor

با این حال ، در سیستم های ERP 3 مدل آخر در مقایسه با مدل اول یعنی آموزش مهندسی معکوس داده ها ، از اهمیت کمتری برخوردارند زیرا سیستم های ERP ستون فقرات IT هر سازمان هستند چرا که داده های اختصاصی - معاملاتی یا داده اصلی ذخیره می شوند و هر داده مشتری که حاوی اطلاعات حساس باشد ، می تواند به طور منحصر به فرد شناسایی کند که مشتری نیاز به حفظ حریم خصوصی دارد.

**آموزش مهندسی معکوس داده ها**

داده های آموزشی می توانند برای رمزگشایی داده های شخصی حساس مهندسی معکوس شوند.

Arvind Narayanan و Vitaly Shmatikov با استفاده از سوابق Netflix از کاربران شناخته شده و سایر اطلاعات بالقوه حساس ، تکنیک گمنامی را به نمایش گذاشتند. وزن های مدل ، ابر پارامترها را می توان برای ساخت مجدد داده های آموزشی مهندسی معکوس کرد و مدل های مهندسی معکوس چالش بزرگی که تصور می شود نیست. داده های ورودی کاربران توسط ایجاد کننده مدل قابل مشاهده است و خروجی یک مدل به همراه کاربری که از اطلاعات وی استنباط می شود برای دیگران نیز قابل مشاهده است. هر مدلی می تواند اطلاعات را به روشهای غیرمنتظره و غیر عمدی نشت کند. مدل می تواند داده های آموزشی را که در مراحل اولیه اتفاق می افتد و بیشتر غالب است ، حفظ کند و اینکه اطلاعات خاص به ندرت اتفاق می افتد اهمیتی ندارد. وقتی مدلی 100٪ دقت در داده های آموزشی را نشان می دهد اما در داده های آزمون عملکرد ضعیفی دارد ، می توان نتیجه گرفت که داده های آموزش تصادفی را حفظ کرده است. برای مقابله با چالش های داده های آموزشی ، روش های حفظ اطلاعات حفظ حریم خصوصی مختلف وجود دارد که به طور کلی می توان به روشهای زیر تقسیم بندی نمود:

* روش های ناشناس سازی مانند k-anonymization ، پوشاندن داده ها
* روش های حفظ حریم خصوصی دیفرانسیل

**حفظ داده های آموزشی در ERP**

قبل از بررسی اینکه بدانیم یک سیستم ERP چگونه حریم خصوصی داده های آموزشی را حفظ و کنترل می کند ، به بررسی اینکه این تکنیک به چه معناست می پردازیم.

**ناشناس سازی**

روش ناشناس سازی داده ها با حذف جزئیات خصوصی یا جایگزینی آنها با مقادیر تصادفی مانند شماره تلفن ها و کد پستی بسیار ناکافی است و حریم خصوصی که ارائه می دهد به سرعت تخریب می شود زیرا دشمنان اطلاعات کمکی در مورد افراد در مجموعه داده را به دست می آورند. در سیستم های ERP مانند SAP S / 4 HANA که حافظه آن پایگاه داده HANA است ، اولین فروشنده ای است که روش های ناشناس سازی را در سیستم SAP HANA هسته اصلی خود قرار داد نشان داد که ناشناس ماندن داده ها در سطح مشاهده و داده ها در سطح جدول بدون تغییر باقی می ماند.

SAP HANA دو روش مختلف ناشناس سازی را ارائه می دهد: k-anonymization و پوشاندن اطلاعات. علاوه بر این ، ما همچنین می توانیم تعریف سفارشی نماهای ناشناس سازی ، دسترسی به نماهای گزارشگری را اضافه کنیم و از یکپارچه سازی در چارچوب مجوز استفاده کنیم. بنابراین ، روش های ناشناس ماندن SAP HANA مزایای بی نظیر تجاری زیر را برای شرکت ها فراهم می کند

* ناشناس ماندن داده های SAP HANA مشتریان را قادر می سازد بدون استفاده از حریم خصوصی افراد ، از داده های شخصی استفاده کنند
* در تجزیه و تحلیل و سناریوهای یادگیری ماشین از اطلاعات شخصی ناشناس کمک می کند
* با استفاده از ارزش داده های سازمانی ، ROI مشتری را افزایش می دهد
* تجزیه و تحلیل زمان واقعی داده های ناشناس در استخراج بینش از داده ها

پوشاندن داده SAP HANA روش دیگری است که به ناشناس ماندن داده کمک می کند و به موارد زیر کمک می کند

* پنهان کردن اطلاعات حساس از DBA ها و کاربران با دسترسی گسترده تر.
* اطلاعات حساس را بسته به نقش کاربر به عنوان مثال نمایش داده و پنهان

**حریم خصوصی دیفرانسیل**

حریم خصوصی دیفرانسیل ، یک مدل ریاضی حفظ حریم خصوصی است که در آن نویز اضافه می شود و تصادفی بدون تأثیر بر توزیع نمونه به مجموعه داده وارد می شود و انکار پذیری قابل قبول را حفظ می کند ، بنابراین افراد نمی توانند به طور منحصر به فرد در مجموعه داده ها جدا شوند و نتایج به هیچ یک از داده های فردی وابسته نیست.

حریم خصوصی دیفرانسیل - هر کس دارای حریم خصوصی همان حذف نقاط داده خود از نمونه است. عملکرد denoising می تواند در بازیابی اطلاعات اصلی به ما کمک کند. حریم خصوصی دیفرانسیل دارای برخی از خصوصیات اصلی است که آن را به چارچوبی غنی و امیدوار کننده تبدیل می کند مانند:

: 1 کمی سازی از بین رفتن حریم خصوصی:از بین رفتن حریم خصوصی با epsilon ε نشان داده می شود و با محافظت از حریم خصوصی متناسب است. این یک معیار برای مقایسه بین تکنیک های مختلف است. از دست دادن حریم خصوصی کمتر به معنای محافظت بهتر از حریم خصوصی است. از بین بردن حریم خصوصی می تواند کنترل شود تا از بین رفتن حریم خصوصی و دقت اطمینان حاصل شود.

. 2 ترکیب : کمی سازی میزان از دست دادن تجزیه و تحلیل و کنترل از دست دادن انباشت حریم خصوصی بر روی چندین محاسبه است. درک رفتار مکانیسم های متفاوت با خصوصیات مختلف ، امکان طراحی و تجزیه و تحلیل الگوریتم های متفاوت با خصوصیات متفاوت از بلوک های ساختاری متفاوت با خصوصیات متفاوت را فراهم می کند

. 3 حریم خصوصی:حریم خصوصی گروهی امکان تجزیه و تحلیل و کنترل از دست دادن حریم خصوصی گروه ها ، مانند خانواده ها را فراهم می کند

. 4 بستن تحت فرآیند پس از پردازش : حریم خصوصی دیفرانسیل از پردازش پس از آن مصون است ، یعنی یک دشمن ، بدون داشتن دانش اضافی در مورد پایگاه داده خصوصی ، نمی تواند تابعی از الگوریتم متفاوت و خصوصی را محاسبه کند و آن را از نظر افتراقی کمتر خصوصی کند.

با این حال ، اگر کسی داده ها را برای مدت طولانی مشاهده کند و عملکردی را که با استفاده از آن نویز اضافه می شود ، رمزگشایی کند ، می توان حریم خصوصی دیفرانسیل را نقض کند. مثالهایی از روشهای حفظ حریم خصوصی دیفرانسیل عبارتند از:

Differential Private Stochastic Gradient decent, GAN’s creating synthetic data

نتیجه گیری

تحول دیجیتالی سیستم های ERP را چابک و هوشمندتر کرده است. با این وجود ، چالشهای بی شماری وجود دارد که باید مورد توجه قرار گیرند و الزاماتی که باید قبل از استفاده از داده های حساس و ارزش آنها از قبل برآورده شوند. مدلهای یادگیری ماشین ، محصول اصلی و IP بسیاری از سازمان ها را با داشتن یک مدل تشکیل می دهند ، یا داده های آموزش یا ابر پارامترها یک تهدید جدی است و می تواند پیامدهای منفی قابل توجهی در کسب و کار داشته باشد و به اعتبار آن آسیب برساند.در مورد تکنیک های حفظ حریم خصوصی ، انتخاب های زیادی وجود دارد. با این حال ، تکنیک های طبقه بندی متفاوت است و توانایی استفاده از این روش های مختلف برای تضمین حفظ حریم خصوصی به حداکثر رسیده است ، این چیزی است که یک سازمان موفق را از یک سازمان ناموفق متمایز می کند.

مطالعات آینده

این مقاله تحقیقاتی با هدف آموزش حفظ حریم خصوصی داده ها برای حفظ چالش ها و رویکرد راه حل از دیدگاه ERP انجام شده است ، تحقیقات آینده می تواند جنبه های دیگری مانند سرقت مدل یا ابرپارامتر را نیز در بر بگیرد.