هوش مصنوعی وحسابرسی داخلی

Artificial Intelligence: Institute of Internal Auditors (IIA)

ترجمه: دکترحسین کثیری ، مجید انصاری

هوش مصنوعی وحسابرسی داخلی

Artificial Intelligence: Institute of Internal Auditors (IIA)

ترجمه: دکترحسین کثیری ، مجید انصاری

مقدمه

کاربردهای هوش مصنوعی (AI) در تجارت و زندگی شخصی ما همه گیراست . از درخواست از تلفن هوشمند خود برای پیش بینی وضعیت هوا ،تا تعیین ارزش اعتبار مشتری، هوش مصنوعی کارایی در زندگی شخصی ما ایجاد می کند، اما ممکن است پیچیدگیها و ریسکهایی را برای حرفه حسابرسی داخلی ایجاد کند.

غالباً حضور آن به حدی ظریف است که بسیاری از ما حتی تأثیر هوش مصنوعی را در محل کار مراجعان خود و همچنین حسابرسی هایمان متوجه نمی شویم. در حالی که بسیاری از حسابرسان داخلی در مدیریت، ریسک، کنترل و فن آوری اطلاعات (IT) صلاحیت دارند، می توان مفاهیم و تکنیکهای حسابرسی فناوری اطلاعات را در مورد برنامه های هوش مصنوعی پوشش داد که در آن از هوش مصنوعی و ویژگی های منحصر به فرد آن معمولا استفاده وقدردانی نمی شود. هدف این گزارش با توضیح دو ویژگی از این دست آغاز شده است.

اولا، برخلاف اکثر سیستم های فناوری اطلاعات IT، هوش مصنوعی از احتمال به جای درست بودن برای به دست آوردن نتایج استفاده می کند. ثانیا برنامه های هوش مصنوعی از داده ها به عنوان ورودی سیستم و گرداننده نتایج استفاده می کنند، به این معنی که با تکامل داده ها، نتایج تغییر می کنند.

درک بلوک های ساختمان هوش مصنوعی

حسابرسان داخلی هر روز به طور مستقیم یا غیرمستقیم ریسک های IT را آدرس داده و نمایان می کنند. حسابرسی فرآیندی که تمام ان اتوماتیک یا جزئی از آن اتوماتیک نیست ، مشکل وغیر معمول است. حتی اگر حسابرسان داخلی در حال بررسی حسابرسی برنامه نباشند، آنها باید هماهنگی لازم با حسابرسان IT برای تکمیل اهداف حسابرسی خود را انجام دهند. بنابراین، برای حسابرسان داخلی منطقی است که تکنیک های حسابرسی و آزمایش شده IT را در برنامه های هوش مصنوعی به کار گیرند. با این وجود همواره خطری در استفاده از ذهنیت "یک اندازه متناسب با همه" برای این برنامه های پیشرفته تر وجود دارد.

به عبارت ساده، چهار مؤلفه اصلی، یک "سیستم خودکار" سنتی را تشکیل می دهند: ورودی، تبدیل فرایندها، خروجی و ذخیره سازی. کاربر داده ها را وارد سیستم می کند، سیستم داده ها را پردازش می کند، داده های پردازش شده به صورت خروجی آزاد می شوند و سپس داده ها ذخیره می شوند. اما داده منجر به نتیجه نمی شودو برنامه ریزی و برنامه نویسی نتیجه را هدایت می کند. در مقابل، در یک برنامه "هوش مصنوعی"، داده ها در فرآیند تصمیم گیری جدایی ناپذیر هستند.

برنامه های هوش مصنوعی بر مبنای خروجی آنها بر روی میلیون ها نقطه از داده ها است، ونه فقط بر مبنای یک ورودی.

ما به عنوان حسابرس داخلی، داده ها را در برابر نتیجه مورد انتظار آزمایش می کنیم. در حالیکه در بسیاری از برنامه های هوش مصنوعی نتیجه مورد انتظار وجود ندارد. غیرقابل پیش بینی بودن ، اساسا تولید ریسک می کند

و چالشی را برای حسابرسان ایجاد می نماید. اولین قدم برای پرداختن به این ریسک جدید، فهم چگونگی کمک اطلاعات به خروجی برنامه های هوش مصنوعی است. در این گزارش، ما طراحی های اصلی داده های هوش مصنوعی را تعریف خواهیم کرد و سپس مجموعه ای از سوالات مربوط به مشتری را ارائه می دهیم که حسابرسان داخلی ممکن است برای جلب اعتماد به سیستم هاکنترل کننده برنامه های هوش مصنوعی، از ان پشتیبانی کنند.

رویکردهای فناوری

هوش مصنوعی ، بسیاری از فناوری های اطلاعاتی از جمله، سیستم های ایستا و سیستم های یادگیری ماشین را مورداستفاده قرارمیدهد. قابل آزمایش بودن سیستم های استاتیک (مانند درخت تصمیم گیری، طبقه بندی کننده ها و جداول قاعده)، مزیت اصلی استفاده از انها در هوش مصنوعی ست. حسابرسان داخلی می توانند ورودی ها، مجموعه داده ها و خروجی ها را با استفاده از هوش مصنوعی بررسی کنند تا اطمینان حاصل شود که در هر تکرار، نتایج مشابهی رخ می دهد. به این ترتیب، سیستم های ایستا در هوش مصنوعی ،قابل اصلاح با روش سنتی حسابرسی فناوری اطلاعات هستند.

از طرف دیگر، بکار گیری سیستم های یادگیری ماشینی در هوش مصنوعی ،کاملاً مبتنی بر یک رویکرد فناوری متفاوت است. در این برنامه ها (برای مثال،یادگیری مرتبط، شبکه های عصبی مصنوعی، یادگیری درخت تصمیم گیری ، یادگیری عمیق و تقویت یادگیری، درمیان دیگران)، سیستم "یاد می گیرد" بهترین پیش بینی چیست.

همانطور که در زیر مورد بحث قرار گرفته است، ضرر چنین سیستم هایی این است که تصدیق آنها از طریق روش های حسابرسی داخلی استاندارد بسیار دشوارتر است.

احتمال در مقابل صحیح بودن

یادگیری ماشینی چندین عامل را در نظر می گیرد و مواردی را انتخاب می کند که به پیش بینی بهترین و مطمئن ترین نتیجه کمک می کنند. به همین ترتیب، سیستمهای یادگیری ماشینی علاقه ای ندارند که کاملاً صحیح

باشندبلکه به گونه ای طراحی شده اند که "به اندازه کافی خوب" باشند، اما لزوماً همیشه درست نیستند، همانطور که در ادامه توضیح داده شده است.

سیستمهای یادگیری ماشینی در هوش مصنوعی به جای ارائه راه حل صحیح برای یک مشکل معین، احتمال درست بودن نتیجه را محاسبه می کنند. نتایج سپس به ترتیب نزولی احتمال وقوع رتبه بندی می شوند.

این فرایند وقتی درنظر می گیرد که آیا نتیجه مشخص صحیح یا نادرست است، معضل ایجاد می کند، زیرا سیستم های یادگیری ماشین اهمیتی نمی دهند که آیا تمام راه حل های صحیح را درج کرده اند یا خیر آنها فقط اهمیت می دهند که بهترین جواب نزدیک به رتبه های برتر کدام است.

به عنوان مثال، Facebook یا LinkedIn ممکن است بعنوان یک هدف سیستمی، مجموعه ای از "دوستان" محتمل را برای ساختن شبکه اجتماعی به شما توصیه کنند. با این وجود، به جای اطمینان از هر توصیه به عنوان دوست، چنین سیستم هایی مجموعه ای از توصیه ها را ایجاد می کنند، که فقط برخی از آنها صحیح یا حتی معقول هستند. به عنوان مثال ،اگر سیستم مجموعه ای از ده دوست احتمالی را ایجاد می کند، که یکی از آنها دوست نزدیک است در حالی که پنج نفر از آنها آشنا هستند و چهار نفر نیز غریبه هستند و شما دوست صمیمی خود را اضافه می کنید، سیستم نتیجه را موفقیت امیز می داند. انجام این هدف، اضافه کردن شخصی به شبکه اجتماعی شما بوده است.

جالب اینجاست که الگوریتم یادگیری ماشینی در هوش مصنوعی ، اهمیتی نمی دهد که فقط 60٪ از مجموعه "دوستان" احتمالاً معقول باشند و 40٪ کاملاً اشتباه بودند. چون هدف، رشد شبکه اجتماعی شما بوده است. بنابراین، درک اصلی سیستم های یادگیری ماشینی در هوش مصنوعی این است که بدانیم سیستم همیشه مجموعه ی احتمالات کاملاً رتبه بندی شده را بدون در نظر گرفتن صحیح بودن آن در نظر می گیرد. در مثال بالا، "غریبه های کامل" 40٪ از دوستان احتمالی را تشکیل می دادند. با این حال، در الگوریتم یادگیری ماشینی، غیر منطقی

بودن این مجموعه نشانگر عدم موفقیت سیستم نیست. در حقیقت، مفهومی از شکست در سیستم های یادگیری ماشینی وجود ندارد. نتایج مبتنی بر عدم وجود منطق، همیشه در زیر آستانه از پیش تعیین شده یادگیری ماشینی آستانه هدف مورد نظر (در این حالت 60٪) قرار خواهد داشت.

هنگام استفاده از یادگیری ماشینی مشکل در جایی که صحت آن بسیار مهم است ایجاد می شود. یک سیستم تشخیصی یادگیری ماشینی که اخیراً در چین برای تشخیص نودل های تیروئید مستقر شده است را در نظر بگیرید. پزشکان گره ها را با دقت 70٪ تشخیص دادند. با این حال، سیستم یادگیری ماشینی بالاتر از آستانه پزشک انسان و با 85 درصد دقت بدست آورد. این سیستم ممکن است زیر دقت پزشکان ماهر باشد، اما از آنجا که بالاتر از آستانه 70٪ برای پزشکان متوسط است، این نتیجه موفقیت آمیز تلقی می شود.

اما ، چگونه 60٪ می تواند به اندازه کافی خوب باشد؟ با کمال تعجب، برای اکثر سیستم های یادگیری ماشینی، دقت کم قابل قبول است. برای اکثر ما، تصور اینکه 60٪ به اندازه کافی خوب است، برخلاف منطق است. ما می خواهیم در دنیایی با اطمینان 100٪ زندگی کنیم. با این حال، موتورهای جستجو، شناسایی عکس و حتی چک کننده خطاهای گرامری اغلب حاوی آستانه کم هستند. چرا؟ از آنجا که سیستم های یادگیری ماشینی علاقه ای به درست بودن ندارند بلکه بیشتر در دستیابی به نتیجه مطلوب هستند. بنابراین ، حسابرسان داخلی هنگام برنامه ریزی و انجام خدمات اطمینان بخش باید همیشه بایداز ابعاد فردی و محدودیتهای ذاتی سیستم های یادگیری ماشین آگاه باشند. نداشتن نتیجه قابل پیش بینی برای آزمایش ممکن است یک مشکل حسابرسی قابل توجه را به وجود آورد.

تغییر نتایج

سیستم های یادگیری ماشینی با گذشت زمان بر اساس تنظیم دقیق داده ها، مجموعه داده های جدید یا تجدید نظر شده و الگوریتم های اضافی تغییر می کنند. هنگامی که در فواصل مختلف از آنها پرسیده شود، این تنظیمات منجر به نتایج متفاوتی برای همان سؤال خواهد شد. سیستم های یادگیری ماشینی همچنین از "مجموعه ای از داده ها" برای "آموزش" سیستم استفاده می کنند. این داده های آموزشی همان چیزی است که الگوریتم های سیستم ابتدا یاد می گیرند. سپس از داده ها برای تنظیم الگوریتم ها و پیشروی برای رسیدن به آستانه هدف اولیه مورد نظر استفاده می کند

کمیت داده ها و کیفیت داده ها بر نتایج حاصل از سیستم های یادگیری ماشینی تأثیر می گذارد.به عنوان مثال، فرض کنید هدف این است که یک سیستم یادگیری ماشینی آموزش دهید تا مشخص شود که آیا کلمه "فرعون" به طور صحیح در یک سند هجی شده است یا خیر. جستجوی این کلمه در فرهنگ لغت یک رویکرد مبتنی بر قانون است. این قانون بیان می کند که اگر کلمه در فرهنگ لغت به عنوان "فرعون" باشد و با املای موجود در سندی که مورد آزمایش قرار می گیرد مطابقت داشته باشد، در 100٪ مرتبه ها به درستی هجی می شود.

با این حال، یک سیستم یادگیری ماشینی، کاملاً متفاوت به املای “pharaoh " یا فرعون نزدیک می شود. این مجموعه به مجموعه داده های مربوط به میلیون ها کلمه می پردازد و بسامد کلمه "“pharaoh" را محاسبه می کند. با این وجود ، با این کار می فهمید که بسیاری از روزنامه ها در سال 2015 ناگهان شروع به نوشتن“pharoah" به جای “pharaoh "کردند. چه اتفاقی افتاد؟ خوب، اتفاقاً اسب مسابقه ای به نام“pharoah"فرعون آمریکایی" در آن سال برنده مسابقات زیادی شد. یک سیستم یادگیری ماشینی تعیین می کند که املا ی صحیح بر اساس تعداد دفعات استفاده ای که در مجموعه داده ها مشاهده می کند، بجای آن که در دیکشنری استاندارد باشد. بنابراین، یک املای نادرست را آموخته است.چرا؟ از آنجا که تعداد تکرار کلمه

اسب مسابقه ای "pharoah " که در مجموعه داده ها پیدا کرده بود، به طور قابل توجهی بالاتر از " pharaoh " در فرهنگ لغت بود.

حسابرس داخلی باید سیستم های یادگیری ماشینی را به عنوان نتیجه غائی در رویکرد "تصمیم گیری اکثریت"و قطعا به شکل تغییر الگو در تفکر ما در نظر بگیرد. در جایی که قبلاً هدف ما صحیح بودن بود، هدف اکنون "محبوبیت" است. برای ارزیابی منفعت و هزینه، افزایش کارایی و تصمیم گیری بهتر ، از طریق سیستم های یادگیری ماشینی، حسابرس داخلی ابتدا باید مبنای داده های مورد استفاده در هوش مصنوعی را همانطور که بحث شد متوجه گردد.

داده ها اهمیت دارند

تمام سیستم های یادگیری ماشینی هوش مصنوعی به مجموعه ای از داده ها برای تولید خروجی تحلیلی مفید نیاز دارند. از آنجا که سیستم ها از این داده ها به عنوان سوخت استفاده می کنند، حسابرس داخلی باید هنگام انجام برنامه ریزی حسابرسی از سیستم هوش مصنوعی، مفاهیم داده ها، کنترل داده ها و رویکردهای هوش مصنوعی را برای تجزیه و تحلیل داده ها درک کند. در بخش های بعدی، انواع مختلفی از مجموعه داده های هوش مصنوعی را شرح می دهیم و در هنگام برنامه ریزی حسابرسی هوش مصنوعی و ارزیابی ریسک های مرتبط، سوالات بالقوه مشتری حسابرسی را پیشنهاد می کنیم.

1.داده های ناخواسته داخل- داده های ناخواسته خارج :

چگونه می توان در میان تعداد زیادی از داده های نادرست، تجزیه و تحلیل دقیقی انجام داد؟ در دنیای آمار، بررسی داده ها برای اطمینان از مرتبط بودن، عاری از خطا و همچنین عاری از داده های نامربوط بسیار مهم است. چگونه می دانید داده های یادگیری دستگاه شما تمیز است یا بی مصرف است؟ سیستم های یادگیری ماشینی به صدها هزار نقطه از داده در انتهای پایین به دهها میلیون نمونه در پایان بالا احتیاج دارند. چگونه می توانید

اطمینان حاصل کنید که ده ها میلیون نمونه، همگی برای اهداف مورد نظرشان مناسب هستند؟ چگونه می توانید مطمئن باشید که پاک کردن داده ها، سطرهای مناسب را حذف نکرده و یا مجموعه داده ها را تغییر نمی دهد؟ به عنوان مثال، هنگام بررسی پیش بینی های مالی، آیا همه پیش بینی های مربوط به بخش های خاتمه یافته را حذف می کنید و فقط داده های مربوط به بخش های فعلی را برای تجزیه و تحلیل در اختیار دارید؟ جستجوی سوالات مشابه این موارد باید به مشتری حسابرسی، مدیریت سیستم هوش مصنوعی ارائه شود.

2. منشأ داده ها:

جمع آوری، تمیز کردن ، پردازش و آماده سازی داده ها برای تجزیه و تحلیل، می تواند بسیار پر هزینه باشند. با این حال، جمع آوری مجدد داده ها ممکن است منجر به نتایج ناقص یا نادرست شود. به عنوان مثال، یک دانشمند به جای تلاش برای بازآفرینی داده های تاریخی گمشده در مورد نگهداری کارمندان، می تواند به سادگی داده ها را از لیست شرکت کنندگان در جلسات سالانه شرکت ها به عنوان واسطه ای برای پیش بینی حفظ کارمندان استفاده نماید.اگر حضور در جلسه از 2145 شرکت کننده در سال 1995 به 5،824 نفر در سال 2014 افزایش یابد و همچنین در سال 2015 به تعداد 2.322 شرکت کننده کاهش یابد، سپس ترکیبی از حضور کارمندان با اطلاعات جمعیتی، مسکونی و حقوق و دستمزد می تواند حفظ و بقای کارمندان را پیش بینی کند.

با این حال ، این سیستم ممکن است نادرست نتیجه بگیرد که محل سکونت شاخص برجسته حفظ کارمندان و تعصبات کارکنان است که در این فاصله زندگی می کنند. با این حال، عوامل دیگر ممکن است وارد آن شوند.به عنوان مثال، این سیستم نمی داند که خطر برف در سال 2015 بسیاری از حاضران را از رویداد نشست سالانه دور نگه داشته است. میانبر بازپرداخت داده ها به عنوان یک پراکسی برای داده های واقعی ممکن است باعث شود مدل های هوش مصنوعی نتایج نادرست حاصل کنند ،یا خط مشی های استفاده از داده را نقض کنند. در نتیجه، از مراجعان حسابرسی باید سؤال شود که آیا روندی برای تایید مناسب بودن داده های مورد استفاده برای سیستم های یادگیری ماشینی هنگام ارائه داده ها وجود دارد یا اساساجایگزینی موجود است.

3. داده های اریب:

از آنجا که سیستم های یادگیری ماشینی به پیش بینی آستانه ها علاقه دارند و نه صحت، آنها نمی دانند که آیا مجموعه داده ها اریب هستند. به عنوان مثال، مجموعه داده ها برای تولید مدل های یادگیری ماشینی ، برای تشخیص بیماری ممکن است جهت گیری ناشناخته ای در مورد زنان داشته باشد، در صورتی که آنها فقط حاوی نتایج MRI در مردان میانه غربی باشند. بر این اساس ، مشتری حسابرسی باید چگونگی بازبینی و تأیید اعتبار داده ها در مدل هوش مصنوعی را برای اطمینان از وجود همه جمعیت نماینده در تعداد دفعات تکرار مناسب برای اطمینان از خروجی صحیح و مداوم، توضیح دهد.

4. دریاچه داده ها:

جهان پر از داده های بدون ساختار است. مقالات روزنامه، عکس از رسانه های اجتماعی و سوابق شرکت همه حاوی عناصر داده های متنوع هستند. به دلیل ماهیت غیرساختاری داده ها، ذخیره سازی نیز به روش های بدون ساختار اتفاق می افتد. ایجاد و مدیریت بازنمایی ساختار یافته کلیه داده ها برای یک سیستم یادگیری ماشینی امری مقرون به صرفه نیست. به همین دلیل، دریاچه های داده ایجاد شده اند ،تا به عنوان مخزن اسناد غیرساختار یافته خدمت کنند.

سیستم های یادگیری ماشینی به عنوان بخشی از فرایند یادگیری، دریاچه های داده را ماهیگیری می کنند و با استفاده از داده های موجود در آن، شبکه گسترده ای را در یک دریاچه جمع می کنند. به دلیل پهناور بودن دریاچه، معمولاً دقیقاً مشخص نیست که چه اطلاعاتی وجود دارد، منشأ داده ها چیست و همچنین مناسب بودن داده ها به سیستم یادگیری ماشینی نیز مشخص نمی باشد. از این رو ،مشتری مورد حسابرسی باید برای حسابرس جزئیات اینکه دریاچه های داده مجاز است و چگونگی کنترل آنها برای استفاده از سیستم یادگیری ماشین مورد بررسی قرار می گیرد را توضیح دهد.

5.نشت داده ها:

آیا شما حدود خود را نقض کرده اید؟ به دلیل عدم برخورداری ساختار یک دریاچه از داده ها، چگونه می توانید اطمینان حاصل کنید که افرادی که در دریاچه ماهیگیری می کنند فقط به اطلاعات مورد نیاز خود دسترسی پیدا می کنند؟ چگونه اطمینان می دهید که داده های کاربران انتخاب شده فقط در قسمت مطمئن دریاچه داده ذخیره می شود و تنها طرف های مجاز قادر به رفتن به ماهیگیری در دریاچه هستند، تا ببینند چه چیزی در آن موجود است؟ با توجه به پتانسیل بروز نشت داده ها، حسابرس باید همواره از ماهیت و وسعت حفاظت از داده های مشتری و نظارت مداوم از مدل یادگیری ماشینی خود برای مدیریت صحیح داده ها سوال کند.

6. رانش داده ها:

مجموعه داده های با طراوت و هرس شده برای اطمینان از طراوت ان ،باعث پدیده جالبی می شود که به عنوان "رانش داده ها "شناخته می شود. مدل های یادگیری ماشینی که ماه گذشته بر روی مجموعه داده ها آموزش دیده بودند، ممکن است وقتی این مدل ها در این ماه روی مجموعه داده های جدید آموزش ببینند، متفاوت رفتار کنند. شرایطی مانند این ،منجر به تغییر در خروجی مدل نسبت به زمان می شود و بر صحت و قوام خروجی داده ها تأثیر می گذارد. در یک برنامه حقوقی، منابع انسانی، پزشکی یا مالی که از اهمیت حیاتی برخورداراست، نشان می دهد که این سیستم می تواند برای ورودی شناخته شده در طول ماه، نتایج مشابهی را کسب کند. با این وجود، در یک سناریوی خرید که اندازه، ترجیحات و روندهای مد به طور مداوم تغییر می کنند، صحت و قوام چنین عواملی از دانستن اینکه آیا فروش را افزایش می دهند اهمیت کمتری دارند.

جدیدترین رویکردهای فن آوری برای یادگیری ماشینی حتی بیشتر مشکل ساز است. مدل های جدید به منظور بازگرداندن مجموعه داده ها به درون خود طراحی شده اند و فرصت کمی برای بررسی انسان در مورد بازده داده ها در مراحل مختلف عملکرد سیستم باقی مانده است. در سیستم هایی که صحت و قوام آنها هدف است، نظارت بر نتایج هوش مصنوعی بر روی آنها در طول زمان به طور فزاینده ای دشوار می شود. بنابراین، مشتری های

حسابرسی باید بتوانند کنترل های خاص حسابرس را بر روی مجموعه داده های یادگیری ماشینی شناسایی کنند که هدف آنها جلوگیری از رانش داده ها است.

راهبری هوش مصنوعی

راهبری، شامل نظارت بر توسعه و عملیات هوش مصنوعی است. این نظارت به ویژه بسیار مهم است .زیرا چنین برنامه های هوش مصنوعی ، دارای ریسک بالاتری نسبت به سیستم های اطلاعاتی سنتی هستند. یک خطر ذاتی وجود دارد که توسعه دهندگان برنامه های کاربردی هوش مصنوعی باید دقیق و با بصیرت و اگاه باشند، اما این ادعاها غالباً مبالغه آمیز می باشند. منفعت واضح هوش مصنوعی باید در برابر خطرات تفسیر نادرست از خروجی داده ها سنجیده شود. مهم نیست که چقدر یک سیستم هوش مصنوعی را کنترل کرده ، بلکه به اندازه ضعیف ترین پیوند آن قوی است.

این ارتباط در پیچیدگی سیستم ،خود پنهان است. الگوی جدید برنامه های هوش مصنوعی نیاز به تمرکز تازه روی نظارت بر سیستم دارد تا سطح بالایی از هماهنگی بین مدیران، دانشمندان داده ها، برنامه نویسان، وکلا و حسابرسان را در بین سایر بازیکنان ایجاد کند. برای مدیریت راهبری هوش مصنوعی الگویی برای پیگیری وجود ندارد. کتاب ودستورالعمل هایی در این مورد می بایست نوشته شود.

با این وجود، با اطلاعات مربوطه که ابتدا در این گزارش توضیح داده شده است، حسابرسان داخلی باید مراقبت های انجام شده از سوی رهبران مشاغل را برای ایجاد ساختار قدرتمند راهبری در حمایت از این کاربردها بررسی کنند و اطمینان حاصل کنند که خطرات شناسایی شده و مورد بررسی قرار می گیرند.

باید توجه ویژه ای به فرآیند توسعه سیستم ها داشته باشید. در حین توسعه سیستم ها و هنگامی که توسعه دهندگان سیستم بیشترین کنترل را دارند، قواعد مشخصی برای برنامه های هوش مصنوعی وضع شده اند. پس از پیاده سازی، آنها به عنوان شبکه های عصبی از داده ها تغذیه می شوند و دارای یک مقدار مشخصی از استقلال هستند. یعنی آنها از یک دستور برنامه نویسی مستقیم پیروی نمی کنند. سطح ریسک پس از اجرا را می توان با

ارزیابی ریسک و فکورانه در طول توسعه سیستم کاهش داد. پیوست این برنامه ها ،شامل سوالات پیشنهادی برای حسابرس است تا به شناسایی خطرات ذاتی در برنامه های هوش مصنوعی کمک کند.

در حالی که بسیاری از دانشمندان داده ها و برنامه نویسان رایانه درک غریزی از ریسک دارند، حسابرسان داخلی مهارت خود را در ارزیابی ریسک با مشورت دو چارچوب منظم که در توسعه سیستم های حسابرسی بسیار ارزشمند بوده اند، ترکیب می کنند ، ترکیبی از یا مجموعه رهنمودهای جامع فناوری ا طلاعات انجمن حسابرسان داخلی(IIA GTAG) به همراه چارچوب کوبیت انجمن ایساکا (ISACA COBIT.). در این چارچوب ها ، مشخص شده است که حسابرسان داخلی باید در کل چرخه ی عمر پروژه های هوش مصنوعی، از طراحی برنامه گرفته تا در نگهداری و پشتیبانی، مشارکت کنند. زمینه های کلیدی ارزیابی نه تنها کلیه مراحل چرخه ی حیات سیستم بلکه بررسی کامل داده های مورد استفاده برای به جلو راندن برنامه هوش مصنوعی است. در حالی که یکپارچگی داده ها یک خطر اساسی برای همه برنامه های رایانه ای است، به ویژه در طراحی برنامه های هوش مصنوعی بسیار مهم است. با توجه به ماهیت جدید این فناوری، قابل درک است که مبتکران، دانشمندان داده ها و برنامه نویسان رایانه از فرصت ها و مزایای آن همچنان هیجان زده باشند.

این سیستم ها می توانند نتایج دقیق و شهودی را تولید کنند. با این حال، هیجان برای این فناوری همچنین ممکن است باعث تعصب و جهت گیری نسبت به پتانسیل آن و عدم تمرکز بر اقدامات راهبری مرتبط با خطرآن شود.

نتیجه

برنامه های هوش مصنوعی می توانند مزایای خارق العاده ای برای سازمان ایجاد کنند و تصمیم گیری و کارآیی آن را افزایش دهند. از طرف دیگر، این مزایا خطر فوق العاده ای است. این گزارش بر خطرات مرتبط با استفاده از داده ها به عنوان قطعه ای جدایی ناپذیر از فرآیند تصمیم گیری تحلیلی در برنامه های هوش مصنوعی متمرکز شده است. آگاهی از نقش داده ها در هوش مصنوعی به حسابرسان داخلی کمک می کند تا یک برنامه حسابرسی

را طراحی کنند و این خطرات مشخص را برطرف کند. مهمتر از همه، عدم شناسایی و کنترل خطرات داده های هوش مصنوعی پیش رو، باعث ایجاد خطرات بیشتر در پایین دست، به ویژه برای شهرت، گزارش دهی و تصمیم گیری های مدیریتی می گردد و فقط موارد معدودی ،مرتبط با هوش مصنوعی خواهند شد.

رهبری اجرایی باید تشخیص دهد که سیستم های هوش مصنوعی فقط کاربرد سریعتر و بهتر برنامه های فناوری اطلاعات نیستند، بلکه در عوض نمایانگر یک رویکرد کاملاً متفاوت برای پردازش داده ها و تصمیم گیری در سیستمها می باشند و خطرات عملیاتی و استراتژیک جدیدی را به همراه دارند. در حال حاضر، رهبران مشاغل با پذیرش نقش رهبری در توسعه مدیریت ریسک صحیح هوش مصنوعی و با کنترل اطلاعات روی داده های هوش مصنوعی، می توانند سازمان های خود را با موفقیت در انتقال سیستم هوش مصنوعی راهنمایی کنند.

پیوست: سیستم های هوش مصنوعی – سوالهای های منتخب برای برنامه ریزی حسابرسی

در جدول زیر مواردی از حسابرسی هوش مصنوعی (AI) ، ریسک سیستم مرتبط با هر یک، سوالات مربوط به حسابرس برای حمایت از مرحله بررسی اولیه در یک حسابرسی هوش مصنوعی و پاسخ های مورد انتظار نشان داده شده است که نشان می دهد تا چه اندازه مدیریت مشتری ماهیت درک مسائل و خطرات درگیر را مشخص می کند.

پاسخ های مورد انتظار	سوالات حسابرسی	ریسکها	موضوع
سیستم های جدید هوش مصنوعی نیاز به درک عمیق تری از سیستم و منابع داده های آن دارند، بنابراین باید ریسک بیشتری را به همراه داشته باشد. سیستم های هوش مصنوعی که سیستم های مستقر و موجود را به کار می گیرند باید ریسک کلی کمتری داشته باشند و به	چه جنبه هایی از سیستم به تازگی ایجاد شده است؟ اصلاح سیستم های موجود در کدام جنبه ها؟ کدام جنبه ها از سیستم های مستقرموجوداستفاده می کنند؟	حسابرسان داخلی فاقد مهارت هوش مصنوعی، ممکن است در شناسایی کنترلهای نقص سیستم ناکام باشند.	آیا مهارت حسابرسی کافی برای کارمندان برای انجام ممیزی از سیستم هوش مصنوعی وجود دارد؟

درک سیستم کمتری نیاز داشته باشند.			
سیستم های هوش مصنوعی که ورودی ها و خروجی ها را در تمام مراحل خط لوله داده پردازش می کنند باید حسابرسی و نظارت مشتری را بر تصمیمات سیستم بر اساس ریسک ارزیابی شده تسهیل کنند. جعبه سیاه سیستم های هوش مصنوعی ، که در آن تحولات داده در سراسر خط لوله داده بدون مشاهده ممیزی از عملکرد سیستم داخلی رخ می دهد، باید اعتبارسنجی تصمیمات سیستم و ارزیابی میزان ریسک سیستم را دشوارتر کند.	چه مراحلی از سیستم و به طور خاص از خط لوله داده برای اعتبارسنجی داده ها طراحی شده است؟ اطلاعات ورودی از کجا تهیه شده است؟ داده های خروجی کجا ذخیره می شود؟ آیا داده خروجی در برخی از مراحل خط لوله حذف می شود، یا برای سیستم های دیگر بازگردانی شده است؟ آیا برنامه هوش مصنوعی به گونه ای برنامه ریزی شده است که تصمیمات گرفته شده توسط این برنامه قابل ردیابی باشد؟	عدم بررسی صریح داده های ورودی و خروجی در هر مرحله از خط لوله داده ممکن است باعث نتایج ناسازگار و نادرست و همچنین محدودیت دامنه حسابرسی شود.	آیا تصمیمات سیستم هوش مصنوعی اعتبار دارند؟

پاسخ های مورد انتظار	**سوالات حسابرسی**	**ریسکها**	**موضوع**
سیستم های هوش مصنوعی به خوبی طراحی شده باید از داده های تضمین شده برای دسترسی به داده های سیستم مطابق با پروتکل های شرکت پشتیبانی کنند و از صحت تفسیرهای کاربر مطابق با	در صورت وجود، چه الزامات نظارتی مربوط به برنامه هوش مصنوعی است؟ آیا دسترسی به خروجی سیستم محدود به کاربران مجاز است و آیا دسترسی	سیستم هوش مصنوعی و خروجی مرحله خط لوله ممکن است داده های حساس را نقض الزامات نظارتی دولت نشان دهد. تفسیر نادرست از خروجی ممکن است باعث	آیا دسترسی کاربر به خروجی سیستم هوش مصنوعی و تفسیرهای بعدی کاربر مناسب است؟

معیارهای سیستم اطمینان حاصل کنند. رای به حداقل رساندن ریسک برای هر یک، سیستم باید بستر طراحی و اجرا شود.	بصورت دوره ای کنترل می شود؟ آیا کاربران مجاز خروجی آن را به درستی تفسیر می کنند؟ آیا معیارهایی برای ارزیابی کیفیت تفسیرها بر اساس خروجی سیستم وجود دارد؟	تصمیمات مدیریتی آگاهانه و منجر به عملکرد عملی ضعیف شود.	
متخصص داده باید مجموعه ای از داده های آموزش (و تولید) را برای ارتباط، صحت و کامل بودن بطور دوره ای بررسی و ارزیابی کند. ماهیت و وسعت این بررسی باید نشان دهنده کیفیت مجموعه داده ها و وضعیت کلی خطاهای داده در سیستم باشد، پیش راندن نتیجه گیری آزمایشی در مورد معقول بودن سیستم خروجی ها. خطاهای موجود در مجموعه داده های آموزش هوش مصنوعی (و تولید) وقتی تعداد زیادی از سوابق داده درگیر هستند می بایست پیش بینی شود. (داده های پاک و بدون خطا هرگز به طور کامل در سیستم های هوش مصنوعی قابل دستیابی نیست) با این وجود، حداقل باید متخصص	منشأ داده های آموزش چیست؟ چقدر در جریان است؟ در هنگام پردازش چه خطاهایی در مجموعه داده های آموزش مشاهده شد؟ چه داده هایی در مجموعه تغییر یا رد شده و چرا؟ چگونه داده های آموزش به روزرسانی می شوند و چند بار بروزرسانی ها انجام می شود؟	داده های مورد استفاده برای آموزش سیستم هوش مصنوعی ممکن است محدودیت های استفاده را نقض کند. ناتوانی سیستم در بازسازی همان خروجی از همان ورودی ممکن است باعث محدود یا جلوگیری از اجرای حسابرسی شود.	از چه منبع داده ای برای آموزش سیستم هوش مصنوعی استفاده شده است؟

داده ها مجموعه داده های مربوط به خطاها را بررسی کرده، تنظیمات انجام شده را ثبت کرده و برآورد درصد خطاهای باقی مانده را محاسبه کند.			
پاسخ های مورد انتظار	**سوالات حسابرسی**	**ریسکها**	**موضوع**
متخصص داده باید به صورت دستی داده های آموزشی را ارزیابی و انتخاب کند تا احتمالات استفاده شده توسط برنامه سیستم را تنظیم کند. حذف یا "پیرایش" داده های آموزشی که منعکس کننده شرایط مبهم هستند در مرحله آزمایش قابل قبول است اما برای مجموعه داده های بزرگتر مورد استفاده در مرحله تولید نیست. (به عنوان مثال، نام "پت" بیانگر ابهام در مورد جنسیت است، اما داده های تولید هوش مصنوعی تنها به همین دلیل تنها نباید از بین برود). بررسی سیستم باید برای ارزیابی حذف ها و محافظت از متخصص داده "آموزش بیش از حد" داده های آموزشی انجام شود تا نتایج مطلوب مطابقت داشته باشد.	مجموعه داده های آموزش چقدر است؟ مجموعه ها چگونه انتخاب شدند؟ چه کسی ورودی و خروجی داده را تأیید کرده است؟ کدام مجموعه داده برای دستیابی به خروجی مورد نظر فعلی تغییر یافته است؟ آیا داده های آموزش حاوی نمونه هایی است که بیشتر شرایط واقعی داده مورد انتظار در طول عمر سیستم را نشان می دهد؟	داده های مورد استفاده برای "آموزش" سیستم ممکن است جمعیت واقعی مورد بررسی برای برنامه هوش مصنوعی را نشان ندهد. داده های آموزشی که نمونه ها و استثنائات کافی را برای همه شرایط برنامه ارائه نمی دهند ممکن است منجر به الگوریتمی شود که حاوی تعصب و جهت گیری در پیش بینی های تولید شده باشد.	از چه مجموعه داده های آموزشی برای تولید سیستم اولیه هوش مصنوعی استفاده می شود؟

اگر سیستم های هوش مصنوعی که از همان مجموعه داده استفاده می کنند، معیارهای نظارتی، قراردادی یا خط مشی را رعایت نکرده و یا در رسیدن به اهداف سیستم پس از استخدام نتوانند به اهداف خود برسند، بررسی های اضافی مشتری در مورد مجموعه داده ها ضروری بوده و انتظار می رود. انتظار می رود دانشمندان داده ها که سیستم های جدید هوش مصنوعی را مدیریت می کنند، با توجه به زمان و هزینه های مربوط به توسعه مجموعه داده های جدید، مجموعه داده های سیستم های موجود را دوباره جمع کنند. انتظار می رود چنین مجموعه هایی از داده ها جهت دار باشند و تمام ویژگی های حوزه داده لازم برای دستیابی به هدف سیستم جدید هوش مصنوعی را منعکس نکنند.	آیا مجموعه داده های سیستم برای رعایت معیارهای قانونی یا سیاست شرکت بررسی شده است و آیا مجوزهای لازم شخص ثالث را برای استفاده دریافت کرده اند؟ مجموعه داده های سیستم هوش مصنوعی چگونه به روزرسانی می شود و بروزرسانی ها چند بار تکرار می شود؟ ارزیابی و گسترش بهبود بعد ازصف آرایی عملکرد سیستم چقدر دشوار است؟ آیا می توان نقص سیستم را به موقع شناسایی و اصلاح کرد؟ آیا سیستم های هوش مصنوعی دیگر نیز ممیزی شده اند که از مجموعه داده های مشابه سیستم فعلی تحت حسابرسی استفاده می کنند؟	استفاده از داده های هوش مصنوعی ممکن است حقوق داده های شخص ثالث، مقررات دولت یا خط مشی های شرکت را نقض کند و باعث اقدام غیر قانونی قانونی گردد. مجموعه داده های یک سیستم هوش مصنوعی مشخص ممکن است به راحتی بروزرسانی نشود و این باعث می شود که سیستم های دیگر با استفاده از همان منبع داده ها، نگهداری سایر سیستم ها را مختل نکنند.	چه سیستم های هوش مصنوعی فعلی یا قبلی از منابع مشابه یا مشابه داده ها برای مجموعه داده های خود استفاده کرده اند؟

پاسخ های مورد انتظار	سولات حسابرسی	ریسکها	موضوع

هر ویژگی سیستم هوش مصنوعی باید صریحاً تأیید شود. برای جلوگیری از تفسیرهای خروجی سیستم بر اساس روابط نامناسب یا نادرست، از جمله استفاده از کدهای پستی برای استنباط سطح تحصیلات یا ثروت ، به جای ثروت و داده های واقعی، باید ویژگی های استنباطی مورد نظارت قرار گیرند.	چه ویژگی هایی از سیستم هوش مصنوعی برای پیش بینی استفاده می شود؟ داده های جمع آوری شده برای هر سیستم چگونه است؟ آیا هدف در نظر گرفته شده از داده ها برای استفاده تایید شده است؟ آیا تأیید هر ویژگی کاربری که مبتنی بر تعامل با دیگران باشد از یک منبع کاربر تأیید شده بدست آمده است؟	نتایج مغرضانه تولید شده توسط ویژگی های سیستم هوش مصنوعی ممکن است کیفیت گزارشگری و تصمیم گیری مدیریت را مختل کند. ویژگی های سیستم هوش مصنوعی که به اطلاعات قابل شناسایی شخصی وابسته هستند (PII) یا تعامل کاربر با دیگران ممکن است فاقد محافظت مناسب باشد.	چگونه ویژگی های سیستم هوش مصنوعی را پیش بینی می کند؟
توسعه دهندگان سیستم باید خروجی واقعی سیستم را برای یکپارچگی داده ها را بجای مجموعه داده های کنترل قفل شده مورد استفاده برای آموزش سیستم بررسی کنند. مجموعه داده های کنترلی باید در طول مرحله آزمایش قفل بمانند تا اطمینان حاصل شود که الگوریتم داده ها را به روشی بی طرفانه پردازش می کند. نمونه داده های نماینده، منعکس کننده وسعت داده ها و شامل حالات مهم، باید به عنوان داده های کنترل برای اعتبارسنجی مجموعه داده های بزرگ آزمایش مورد استفاده قرار گیرند.	مجموعه داده های کنترل چقدر بزرگ بودند؟ برای اعتبارسنجی مجموعه داده های کنترل از چه روشی استفاده شده است؟ آیا نمونه های استفاده شده نشان دهنده تمام سناریوهای ممکن است؟ چگونه اختلافات در مجموعه داده های کنترل اصلاح شد؟ آیا داده های نادرست برداشته شده است، یا اینکه این سیستم برای جابجایی داده های نادرست سازگار شده است؟	داده های مورد استفاده در مجموعه های کنترل ممکن است داده های واقعی تولید را نشان ندهند. توسعه دهندگان سیستم ممکن است با حذف داده های دورتر از مجموعه داده های کنترل، نتایج را مغرضانه سازند. این عمل، به عنوان "بیش از حد" داده ها گفته می شود، ممکن است به مدلی منجر شود که فقط برای نمونه آموزشی کار می کند و با داده های واقعی به مرور زمان عملکرد ضعیفی دارد.	چه مجموعه ای از داده های کنترلی (منعکس کننده حوزه داده سیستم هوش مصنوعی) برای تأیید صحت مجموعه داده های واقعی هوش مصنوعی استفاده شده است؟

پاسخ های مورد انتظار	سوالات حسابرسی	ریسکها	موضوع
یک فرآیند باید انجام شود تا یکپارچگی داده های واقعی سیستم در برابر مجموعه داده های کنترلی آزمایش شود. کلیه مجموعه های داده مورد استفاده در سیستم باید مورد آزمایش و اعتبار قرار گیرند. درصد کمی از خطاها در داده های سیستم، عادی و قابل قبول است. با این حال، سیستم باید دارای ویژگی هایی باشد که اثرات منفی را مدیریت و کاهش می دهد. اگر داوران شخص ثالث داده های سیستم را آزمایش کردند، نتایج آزمون برای صحت باید تأیید شود. (یک عمل مرسوم، مقایسه نتایج آزمون سه قاضی مستقل و شخص ثالث و شناسایی و آشتی ناسازگاری است).	چه فرایندی تضمین می کند که داوران شخص ثالث که برای ارزیابی کیفیت داده ها انتخاب شده اند، تخصص کافی در حوزه داده سیستم دارند؟ وقتی داوران شخص ثالث از الگوریتم هایی برای تعیین کیفیت داده استفاده می کنند، چگونه این روند بررسی و تأیید می شود؟ آیا داوران شخص ثالث مجوزهای مناسب برای بررسی ورودی داده های خام و خروجی های سیستم حاصل از آن را دریافت کرده اند، به ویژه اگر PII درگیر باشد؟ نتایج داوران شخص ثالث چگونه بررسی می شود تا صحت آنها صحت داشته باشد؟ روند آزمایش یکپارچگی داده های سیستم جدید و بررسی ناسازگاری در نتایج	استفاده از سیستم های خودکار برای قضاوت درمورد تمامیت داده ها ممکن است مسائل اساسی سیستم را تحت تأثیر قرار دهد که بر کیفیت خروجی تأثیر منفی می گذارد. اگر مجموعه داده های کنترل بر اساس داده های سیستم فعلی باشد، پس عدم اعتبار چنین داده هایی برای صحت ممکن است یک ارزیابی ناقص از داده های واقعی سیستم ایجاد کند. قضاوت شخص ثالث از کیفیت داده ها می توانند در صورت عدم مجوز دسترسی و بررسی ورودی واقعی داده های سیستم، نتیجه نادرست در مورد صحت داده های سیستم را نتیجه بگیرند. عدم موفقیت قضات شخص ثالث برای انجام آزمایشات خود در	چگونه مجموعه داده های سیستم هوش مصنوعی، به طور مستقل از طریق اشخاص ثالث برای قضاوت در مورد کیفیت داده ها، یک روش معمول فناوری اطلاعات یا از راه های دیگر تایید می نماید؟

	آزمون قضات شخص ثالث چیست؟	کشورهایی که سیستم هوش مصنوعی در آن قرار دارد ممکن است باعث شود. با توجه به محدودیت های ملی و بین المللی در انتشار و استفاده از داده های حساس مانندPII، نقض ناخواسته مقررات دولتی است.	

پاسخ های مورد انتظار	سولات حسابرسی	ریسکها	موضوع
معیارهای عملکرد باید صحت خروجی داده، پذیرش کاربر از نتایج سیستم و رعایت سیستم با قوانین کسب و کار را اندازه گیری کنند. چنین معیارهایی باید بر آموزش سیستم و داده های تولید نظارت داشته باشند و دوره های زمانی یکسانی را برای هر یک پوشش دهند. معیارهایی که بر روی پذیرش کاربر متمرکز هستند، نباید بر محبوبیت نتایج سیستم به ضرر صحیح بودن آنها تأکید کنند، به ویژه هنگامی که صحت برای کیفیت عملکرد سیستم بسیار مهم است.	چگونه سیستم متغیرهایی را از معیارهای عملکرد تعیین شده گزارش می دهد؟ نرخ سیستم فعلی و تاریخی برای نتایج صحیح، مثبت کاذب، منفی کاذب و نتایج نادرست چیست؟ آیا کاربران سیستم قادر به ارائه بازخورد در مورد سیستم هستند؟ اگر چنین است، چگونه این امر محقق می شود؟ چه نوع خطایی درمورد کاربران گزارش می دهد؟	عدم استفاده از معیارهای عملکردی که کیفیت خروجی سیستم را ارزیابی می کند ممکن است مسائلی را نشان ندهد که استقبال کاربر را تضعیف می کند. سیستم های فاقد معیار برای نظارت بر کیفیت خروجی سیستم، از جمله مثبت های کاذب و منفی کاذب، ممکن است عملکرد واقعی سیستم را زیاده روی کنند. عدم اجرای معیارهای عملکردی که میزان انطباق سیستم با مقررات مربوط به	آیا فرایندی برای نظارت بر سیستم هوش مصنوعی بر اساس معیارهای عملکردی وجود دارد؟

		مشاغل، مانند قوانین IRS حاکم بر برنامه هوش مصنوعی مالیات بر درآمد را اندازه گیری می کند، ممکن است باعث شود بازده معیوب کشف نشود.	