شنبه 29 آذر 1404 - 04:44

مرورگرهای هوش مصنوعی تا چه اندازه قابل اطمینان هستند؟

اجازه دادن به هوش مصنوعی برای وبگردی تا زمانی که مشکلی پیش نیاید، عالی به نظر می‌رسد، اما در صورت بروز مشکل قطعا ما را درگیر خواهد کرد.

اجازه دادن به هوش مصنوعی برای وبگردی تا زمانی که مشکلی پیش نیاید، عالی به نظر می رسد، اما در صورت بروز مشکل قطعا ما را درگیر خواهد کرد.

به گزارش ایسنا، مرورگرهای مبتنی بر هوش مصنوعی با اقدام مستقیم از طرف ما تغییر نحوه جستجو، خرید و کار آنلاین ما را نوید می دهند. آنها قرار است نحوه استفاده ما از اینترنت را متحول کنند و اساساً نحوه جست وجوی اطلاعات و کار آنلاین ما را تغییر دهند.

به نقل از فوربس، مرورگرهای مبتنی بر هوش مصنوعی، نسل جدیدی از مرورگرهای وب هستند که براساس هوش مصنوعی عامل محور ساخته شده اند و قادر به دیدن صفحه نمایش ما و به دست گرفتن کنترل برای انجام وظایف از طرف ما هستند، اما یک علامت سؤال بزرگ درباره ایمنی آنها وجود دارد. از این گذشته، اگر مرورگرها می توانند وب سایت ها را باز کنند، جزئیات را پوشش دهند، ایمیل ها را بخوانند و حتی خرید کنند، چگونه می توانیم مطمئن باشیم که آنها همیشه به نفع ما کار می کنند؟

حتی اگر فعلاً مسئله توهم هوش مصنوعی را کنار بگذاریم، این واقعیت که هوش مصنوعی اغلب چیزهایی را از خودش درمی آورد یا به شیوه هایی عمل می کند که ما حتی نمی توانیم آنها را درک کنیم، نشان می دهد احتمال این خطر وجود دارد که افراد مخرب بتوانند بر رفتار هوش مصنوعی تأثیر بگذارند و آن را متقاعد کنند که به ما آسیب برساند.

مرورگرهای مبتنی بر هوش مصنوعی، نسل جدیدی از مرورگرهای وب هستند که براساس هوش مصنوعی عامل محور ساخته شده اند و قادر به دیدن صفحه نمایش ما و به دست گرفتن کنترل برای انجام وظایف از طرف ما هستند.واقعیت این است که این فناوری بسیار جدید است و هیچ کس دقیقاً نمی داند خطرات آن می تواند تا چه حد باشد، اما کارشناسان در حال حاضر احتیاط شدید را توصیه می کنند و چندین تهدید جدی را نیز مطرح کرده اند که هوش مصنوعی می تواند ایجاد کند.

بنابراین، باید این پرسش را بررسی کنیم که مرورگرهای مبتنی بر هوش مصنوعی تا چه اندازه امن هستند و اگر قرار است از آنها استفاده کنیم، چه اقداماتی می توانیم انجام دهیم که تا حد امکان از خود محافظت کنیم.

به نقل از سرافیک سکیوریتی، یک مرورگر هوش مصنوعی با ویژگی های هوش مصنوعی ارتقاء یافته است تا نحوه تعامل کاربران با محتوای وب و استفاده از آن را بهبود ببخشد.

برخلاف مرورگرهای سنتی که عمدتاً بر رندر صفحات و ارائه دستی مسیر تمرکز دارند، مرورگرهای هوش مصنوعی ویژگی هایی را مانند جست وجوی زبان طبیعی، خلاصه سازی در لحظه، توصیه های محتوای شخصی سازی شده و گردش های کاری خودکار در خود جای داده اند. این عملکردها توسط مدل های هوش مصنوعی مولد پشتیبانی می شوند که به تحلیل قصد کاربر می پردازند، نیازها را پیش بینی می کنند و اقدامات پیشگیرانه انجام می دهند.

مرورگرهای هوش مصنوعی از پیشرفت های هوش مصنوعی برای کمک به کاربران در انجام وظایف پیچیده مستقیماً در محیط مرورگر استفاده می کنند. آنها می توانند حقایق کلیدی را از مقالات استخراج کنند، خلاصه های مختصری تولید کنند، فرم ها را پر کنند، در تعاملات همراه با گفت وگو شرکت داشته باشند و حتی وظایف پیچیده چندمرحله ای را به صورت خودکار انجام دهند.

یک مرورگر هوش مصنوعی با ویژگی های هوش مصنوعی ارتقاء یافته است تا نحوه تعامل کاربران با محتوای وب و استفاده از آن را بهبود ببخشد.در ادامه گزارش، برخی از محبوب ترین و نوآورانه ترین مرورگرهای هوش مصنوعی موجود در بازار را بررسی خواهیم کرد.

۱. «چت جی پی تی اطلس»(ChatGPT Atlas). ادغام چت جی پی تی با حافظه و خودکارسازی عامل که در یک مرورگر مستقل عمل می کند.

۲. «پرپلکسیتی کامت»(Perplexity Comet). یک مرورگر وظیفه گرا که با ادغام صدا و ایمیل/تقویم، تحقیق، مدیریت تب ها و برنامه ریزی را خودکار می کند.

۳. «اپرا آریا»(Opera Aria). دستیار هوش مصنوعی تعبیه شده در مرورگر اپرا که با کنترل تب ها، ابزارهای نوشتاری و تحلیل تصویر از طریق دستورات زبان طبیعی کار می کند.

۴. «مایکروسافت اج کوپایلت»(Microsoft Edge Copilot). دستیار داخلی که خلاصه صفحات، تولید محتوا و اطلاعات ویدئویی را مستقیماً در مرورگر اج ارائه می دهد.

۵. «بریو لئو»(Brave Leo). مرورگری با محوریت حریم خصوصی و دستیار هوش مصنوعی که بدون نیاز به ورود به سیستم برای خلاصه سازی، ترجمه و تولید محتوا در صفحه کار می کند.

۶. «مکستون»(Maxthon). یک مرورگر امن و سازگار با Web۳ که به چت هوش مصنوعی داخلی، VPN و همگام سازی بین پلتفرمی مجهز است.

۷. «دیا»(Dia). مرورگر متمرکز بر دستیار که با کنترل های حریم خصوصی محلی، کمک هوش مصنوعی درون خطی را برای نوشتن، تحقیق و برنامه ریزی ارائه می دهد.

۸. «سیگما»(Sigma). مرورگر عامل محور با خودکارسازی کامل گردش کار، ورود به سایت و قابلیت های پژوهش عمیق با استفاده از زبان ساده کار می کند.

۹. «فلو»(Fellou). مرورگر کاملاً مستقل که برای اجرای وظایف چندپلتفرمی، تحقیق و ادغام دسکتاپ از طریق زبان طبیعی طراحی شده است.

۱۰. «داک داک گو»(DuckDuckGo). مرورگری با اولویت حفظ حریم خصوصی که به ادغام چت ناشناس هوش مصنوعی می پردازد و ردیاب ها، تبلیغات و جمع آوری داده ها را به طور پیش فرض مسدود می کند.

کاربردهای مرورگر هوش مصنوعی

۱. گردش های کاری تحقیق و دانش مبتنی بر هوش مصنوعی. مرورگرهای هوش مصنوعی به ویژه برای گردش های کاری فشرده تحقیقاتی مانند تحقیقات دانشگاهی یا حرفه ای سودمند هستند.

این مرورگرها با خلاصه سازی خودکار اسناد طولانی، استخراج استنادها و پیشنهاد منابع مرتبط، فرآیند جمع آوری، درک و ارجاع متقابل حجم زیادی از اطلاعات را ساده می کنند. کاربران می توانند به جای جمع آوری و پیمایش دستی داده ها، بر تجزیه و تحلیل و ترکیب تمرکز کنند.

۲. تعامل خودکار در وب و پر کردن فرم. مرورگرهای مبتنی بر هوش مصنوعی می توانند زمان صرف شده برای کارهای تکراری وب مانند پر کردن فرم ها، مدیریت ثبت نام های آنلاین یا تعامل با پورتال های مبتنی بر وب را به میزان قابل توجهی کاهش دهند.

این مرورگرها با استفاده از یادگیری ماشینی برای تشخیص فرم های رایج و پر کردن خودکار آنها براساس ورودی های قبلی کاربر یا پروفایل های ذخیره شده، میزان خطا را کاهش می دهند و گردش کار را ساده می کنند.

*مرورگرها با خلاصه سازی خودکار اسناد طولانی، استخراج استنادها و پیشنهاد منابع مرتبط، فرآیند جمع آوری، درک و ارجاع متقابل حجم زیادی از اطلاعات را ساده می کنند.***۳. داشبوردهای اطلاعات شخصی سازی شده.** *مرورگرهای هوش مصنوعی می توانند اطلاعات را براساس علایق کاربر جمع آوری و شخصی سازی کنند و آنها را در داشبوردهایی که به صورت پویا به روزرسانی می شوند، سازماندهی کنند.*

این داشبوردها با یادگیری رفتار و ترجیحات کاربر، اخبار، هشدارها، رویدادهای تقویم و اسناد مرتبط را بدون نیاز به بازدید از چندین وب سایت ارائه می دهند. مرورگر محتوا را گردآوری می کند، نویز را فیلتر می کند و اطلاعات عملی را برجسته می کند.

۴. مرور و دسترسی مبتنی بر صدا. مرورگرهای هوش مصنوعی به طور فزاینده ای از هدایت صوتی پشتیبانی می کنند و به کاربران امکان می دهند که بدون دخالت دست با محتوای وب تعامل داشته باشند.

کارهای پیچیده از جست وجوی صوتی گرفته تا دیکته کردن ایمیل ها یا پیمایش بین تب ها می توانند به طور دقیق از طریق دستورات زبان طبیعی انجام شوند. این امر، دسترسی را برای کاربران مبتلا به اختلالات حرکتی یا افرادی که ورودی صوتی را به روش های سنتی ترجیح می دهند، امکان پذیر می کند.

خطرات

۱. تزریق سریع. یکی از خطرات مطرح شده توسط کسانی که نگرانی های ایمنی را پیرامون وبگردی با مرورگرهای هوش مصنوعی برجسته می کنند، تزریق سریع است.

به عبارت ساده، تزریق سریع زمانی رخ می دهد که شخصی با نیت بد، دستورالعمل هایی را در یک وب سایت یا کد آن پنهان می کند. از آنجا که مرورگرها با خواندن و درک وب سایت ها کار می کنند، در برخی شرایط می توان آنها را فریب داد تا از دستورالعمل ها پیروی کنند. این کار می تواند شامل ارسال اطلاعات به یک وب سایت مخرب، افشای اطلاعات شخصی که می تواند به آن دسترسی پیدا کند یا دانلود و نصب بدافزار باشد.

پژوهش منتشرشده توسط توسعه دهندگان مرورگر «بریو»(Brave) که بر حریم خصوصی تمرکز دارد، نشان داد که دستورالعمل های مخرب می توانند در تصاویر پنهان شوند و مرورگرها می توانند آنها را به عنوان دستوراتی برای انجام دادن اقدام تفسیر کنند.

۲. گرفتن هویت کاربر. مرورگرها برای این که بتوانند از طرف شما کار کنند، اغلب باید هویت شما را به خود بگیرند. این به معنای داشتن قابلیت احراز هویت شما برای دسترسی به خدمات یا انجام خرید است.

بخش زیادی از زندگی ما اکنون به صورت آنلاین انجام می شود. برای مثال، بانکداری، خرید و تعامل با خدمات دولتی در حال حاضر به صورت آنلاین انجام می شوند و کمتر کاری وجود دارد که به صورت دیجیتالی قابل انجام شدن نباشد.

۳. شعاع انفجار. هر مدل، پلتفرم یا وب سایت جدیدی که به آن اجازه دسترسی به داده هایمان را می دهیم، برای ما راحتی به ارمغان می آورد اما اگر مشکلی پیش بیاید، شعاع انفجار را نیز افزایش می دهد.

در اینجا برای بروز مشکل حتی به یک عامل مخرب هم نیازی نیست. یک عامل با پیکربندی نادرست یا بسیاری از شکل های دیگر خطای انسانی، برای ایجاد خسارت کافی هستند.

۴. توهم. علاوه بر خطای انسانی باید نگران خطای ماشینی نیز بود که یکی از آنها توهمات بدنام هوش مصنوعی است.

هر کسی که از چت جی پی تی یا برنامه های مشابه استفاده کرده باشد، می داند که بیان همراه با اعتمادبه نفس حقایق و ادعاهایی که پایه و اساس کمی در واقعیت دارند یا اصلاً ندارند، اصلاً غیرمعمول نیست. انسان ها هم کامل نیستند و هوش مصنوعی معمولاً وقتی ما متوجه نقص هایش می شویم، با کمال میل اشتباهاتش را می پذیرد و خودش را اصلاح می کند، اما تا وقتی مطمئن نشویم هوش مصنوعی هنگام تصمیم گیری درباره این که داده های ما را در اختیار چه کسی بگذارد یا پول ما را کجا خرج کند، با همان اعتمادبه نفس نابه جا عمل نخواهد کرد، بهتر است به آن فرصت اشتباه کردن ندهیم.

حفظ امنیت

اگر با وجود این که خطرات را درک کردید هنوز می خواهید با مرورگرها کار کنید، چند مرحله وجود دارد که باید برای به حداقل رساندن احتمال آسیب دیدن انجام دهید.

۱. از محیط مجوزدهی مرورگر عامل محور انتخابی خود آگاه باشید. مرورگرها با یکدیگر متفاوت هستند و روش های مجاز دسترسی، محدود کردن دسترسی، مشاهده و انجام دادن اقدامات در آنها دائم در حال تغییر است، اما پیش از این که حتی یک گام به سوی دنیای مرورگر عامل محور بردارید، مطمئن شوید که نحوه کنترل این موضوع را کاملاً درک کرده اید.

در این مرحله، به هیچ وجه توصیه نمی شود به مرورگرها که بیشتر آنها هنوز نسخه های آزمایشی هستند، دسترسی به هر نوع داده حساس مانند ورود به حساب های بانکی یا ایمیل خود را بدهید.

۲. نحوه نظارت بر فعالیت مرورگر عامل محور را بررسی کنید. بیشتر مرورگرها گزارش هایی را از اقداماتی که انجام می دهند، ارائه می کنند. مراقب این موارد باشید و در صورت مشاهده بازدیدهای غیرمعمول از سایت یا اشتراک گذاری داده ها به روش هایی که شما نمی فهمید، فوراً اجازه خود را لغو کنید.

علاوه بر خود عامل، به یاد داشته باشید که مجوزهای مربوط به هر افزونه مرورگری را که نصب کرده اید، به دقت زیر نظر داشته باشید زیرا توابع عامل در مرورگر ممکن است بتوانند آنچه را که در دسترس آنهاست، ببینند.

*از مرورگرهای هوش مصنوعی نباید انتظار معجزه داشته باشیم، زیرا آنها هنوز در مرحله آزمایش هستند.***۳. از حساب کاربری خود محافظت کنید.** *ایجاد حساب های کاربری جدید و قرارگرفته در بخش «سندباکس»(sandbox) را برای برنامه هایی مانند ایمیل یا سرویس های فضای ابری مانند «Google Docs» و «Microsoft 365» در نظر بگیرید. به این ترتیب، می توانید بدون این که ریسک*

دسترسی آنها به حساب های کاربری واقعی تان را بپذیرید، ارزیابی کنید که آنها چقدر خوب با مرورگرها کار می کنند.

۴. از جدیدترین اطلاعیه های امنیتی درباره نقض داده ها، آسیب پذیری ها و ممیزی ها آگاه باشید. این چشم انداز به سرعت در حال تغییر است و دنبال کردن تحقیقات جامعه از طریق پلتفرم ها می تواند ایده خوبی باشد.

یک دنیای جدید

مرورگرها بسیار جدید هستند و می توان گفت که خطرات و فرصت های آنها هنوز به طور کامل درک نشده است. تا زمانی که ممیزی های امنیتی بیرونی و جامع در دسترس نباشند، بهتر است جانب احتیاط را رعایت کنیم. همچنین، باید گفت که هنوز نباید انتظار معجزه داشته باشید و این فناوری هنوز آزمایشی است.

خیلی جالب است که به یک عامل هوش مصنوعی بگویید چه کاری انجام دهد و سپس شاهد باشید که در اینترنت می چرخد، اطلاعات جمع آوری می کند و با سرویس های آنلاین تعامل دارد، اما در حال حاضر احتمالاً متوجه خواهید شد که با کار دستی به ویژه در کارهای پیچیده تر، نتایج بهتر و دقیق تری را به دست می آورید.

فقط یک دلیل برای روشن کردن یکی از این مرورگرهای عامل محور جدید امروزی وجود دارد و آن دلیل این است که نگاهی اجمالی به آینده داشته باشید. تا زمانی که اقدامات احتیاطی لازم را انجام دهید، این یک روش امن و جذاب است.