

OUCH!

ماهنامه آگاهی از امنیت اطلاعات برای شما

هوش مصنوعی : آنچه میبایست بدانیم

چيست و چرا بايد به آن اهميت بدهم؟

هوش مصنوعی (AI) سیستم هایی را توصیف میکند که برنامه ریزی شده اند مانند انسانها فکر کرده و پاسخ دهند. در واقع، ما همین سوال را از راهکارهای هوش مصنوعی ChatGPT پرسیدیم و این پاسخ را دریافت کردیم.

هوش مصنوعی چیست؟

هوش مصنوعی (AI) به شبیه سازی هوش انسانی در ماشین هایی اشاره دارد که برنامه ریزی شده اند مانند انسانها فکر کرده و یاد بگیرند. آنها شامل الگوریتم های توسعه یافته و برنامه های رایانه ای هستند که می توانند کارهایی را انجام دهند که معمولاً به هوش انسانی نیاز دارند، مانند تشخیص گفتار، درک طبیعی زبان، تصمیم گیری و انجام بازی ها. انواع مختلفی از هوش مصنوعی وجود دارند، از جمله هوش مصنوعی مبتنی بر قوانین، سیستم های خبره (Expert systems) و یادگیری ماشینی (machine learning).

دلیلی که هوش مصنوعی را بسیار قدرتمند می کند این است که می تواند هوش و توانایی استدلال ذهن انسان را شبیه سازی کند، اما می تواند به صورت فزاینده ای اطلاعاتی بسیار بیشتر از هر انسان دیگری را تجزیه و تحلیل نماید و آن را به طور تصاعدی سریعتر انجام بدهد.

هوش مصنوعی مفهوم جدیدی نیست. در اصل در زمان های علمی تخیلی آورده شده است، هوش مصنوعی چیزی است که دهه ها در حال توسعه بوده است. دلیلی که اکنون در مورد آن بسیار می شنوید این است که برای اولین بار، هر کسی این فرصت را دارد که با عملکرد واقعی هوش مصنوعی تعامل داشته و عملکرد واقعی آن را ببیند.

ChatGPT، بات (bot) چت هوش مصنوعی آنلاین، یکی از اولین راه حل های است که در دسترس عموم قرار گرفته است و می تواند مانند یک انسان واقعی پاسخ داده و چیزی به نام تست تورینگ را پشت سر بگذارد. این تست توانایی ماشین برای نشان دادن رفتار هوشمند از طریق تعامل یک انسان واقعی با دستگاه از طریق یک کانال چت مبتنی بر متن را تعیین می کند. اگر انسان نتواند تشخیص دهد که آیا با یک دستگاه یا شخصی واقعی در حال تعامل است، گفته می شود که دستگاه آزمایش را با موفقیت پشت سر گذاشته است. راه حل های هوش مصنوعی امروزی اولین راهکار در دسترس عموم هستند که دقیقاً همین کار را انجام می دهند.

با این حال، مکالمات آنلاین تنها آغازی است برای کارهایی که هوش مصنوعی می تواند انجام دهد. امروزه راه حل های هوش مصنوعی وجود دارند که می توانند ویدیویی از یک فرد را در حال تدریس در یک کلاس به هر زبانی ساخته، سوابق سلامتی را تجزیه و تحلیل کنند و به سرعت تشخیص دهند که چه کسی به احتمال زیاد سرطان دارد، مقاله های خبری یا مقاله هایی درباره موضوع انتخابی شما ایجاد کنند، تصاویری را برای کتاب های کودکان تولید کرده، یا برای برنامه های کامپیوتری جدید، کد بسازند. اگرچه لزوماً هوش مصنوعی چیزی نیست که باید از آن ترسید، اما خطراتی وجود دارد که باید از آنها مطلع باشید.

خطرات هوش مصنوعی:

1. **بازآفرینی شما:** راه حل‌های هوش مصنوعی می‌توانند صدای یک فرد - صدای شما - را ضبط کنند و سپس از آن برای ایجاد صدایی لحظه‌ای که دقیقاً شبیه شما باشد استفاده نمایند و هر چه می‌خواهند برای جعل کردن هویت شما بگویند. بنابراین، یک مهاجم سایبری می‌تواند یک پیام صوتی تلفنی را ضبط کند که صدای آن شبیه صدای شما باشد و همکاران، بانک شما یا یکی از اعضای خانواده تان را فریب دهد تا فکر کنند شما تماس گرفته‌اید و از آنها خواسته‌اید که کاری را انجام دهند. همچنین هوش مصنوعی می‌تواند این کار را با تصاویر یا ویدئو نیز انجام دهد. یک راه حل هوش مصنوعی که گاهی اوقات Deep Fakes نامیده می‌شود نیز وجود دارد که می‌تواند یک عکس یا ویدیویی موجود از شما را گرفته و از آن برای بازسازی تصاویر یا ویدیوهای کاملاً جدید (شامل صدای شما) استفاده نماید که به نظر برسد کارهایی را انجام می‌دهید که هرگز انجام نداده‌اید.
2. **پاسخ‌های اشتباه:** در مورد داده‌ها یا پاسخ‌هایی که هوش مصنوعی ارائه می‌دهد، راه حل‌ها ممکن است اشتباه باشند. هوش مصنوعی اغلب از اطلاعات عمومی موجود در اینترنت استفاده می‌کند و پاسخ‌های آن می‌تواند تحت تأثیر تعصبات توسعه دهندگانش باشد. در حالی که موتورهای جستجوی معمولی برای ارائه «بهترین» یا صحیح‌ترین پاسخ به سؤالات شما طراحی شده‌اند، راه حل‌هایی مانند هوش مصنوعی ممکن است به گونه‌ای طراحی شده باشند که شبیه‌ترین پاسخ انسانی را به شما بدهند. اینکه کدام یک بهتر است بستگی به این دارد که شما به دنبال چه دست آوردن چه هدفی هستید.
3. **همه یکسان نیستند:** با تبدیل شدن هوش مصنوعی به جدیدترین فناوری داغ روز، به معنای واقعی کلمه در حال حاضر صدها شرکت نوپا خدمات هوش مصنوعی مختلفی را ارائه می‌کنند. بسیاری از آنها اطلاعات یا کارت اعتباری شما را برای نسخه آزمایشی می‌خواهند. مراقب باشید - همه خدمات هوش مصنوعی قابل اعتماد نیستند. تحقیقات خود را قبل از ثبت نام و استفاده از یک سرویس هوش مصنوعی انجام دهید.
4. **حریم خصوصی شما:** هر زمان که از یک سیستم هوش مصنوعی استفاده کرده یا با آن تعامل می‌کنید، مانند هنگام چت آنلاین با ChatGPT، توجه داشته باشید که هر اطلاعاتی که وارد سیستم می‌کنید نه تنها می‌تواند توسط آن پردازش شود، بلکه نگهداری شده و برای پاسخ دادن به دیگران نیز استفاده خواهد شد. این بدان معناست که اگر شما هرگونه اطلاعات شخصی در مورد خود یا هرگونه اطلاعات محرمانه از محل کار را وارد نمایید، آن اطلاعات ذخیره شده و به طور بالقوه با دیگران به اشتراک گذاشته شده و یا به آنها فروخته می‌شود. اطلاعاتی از محل کارتان را که حساس، شخصی یا محرمانه می‌دانید به اشتراک نگذاشته یا وارد نکنید.

آینده هوش مصنوعی

هوش مصنوعی هنوز به شدت در مراحل اولیه رشد خود میباشد، مانند جایی که شبکه اینترنت بیست تا سی سال پیش بود. در حالی که می‌توانیم انتظار تکامل و پذیرش سریع هوش مصنوعی را داشته باشیم، پیش‌بینی اینکه تأثیر آن در آینده چگونه خواهد بود بسیار دشوار میباشد. فقط حواستان باشد که این قابلیت‌ها در اینترنت وجود دارند و بسیار مراقب باشید هنگام استفاده از هوش مصنوعی، چه اطلاعاتی را وارد کرده و به اشتراک می‌گذارید.

منابع

چت جی پی تی: <https://chat.openai.com/chat>
تست تورینگ: https://en.wikipedia.org/wiki/Turing_test

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجوا

OUCH! توسط SANS Security Awareness منتشر شده است و تحت مجوز Creative Commons BY-NC-ND 4.0 میباشد. شما آزاد هستید که این ماهنامه را برای بقیه اشتراک گذاشته یا آن را توزیع نمائید به شرطی که آن را به فروش نرسانده یا تغییری در آن ایجاد نکنید. هیئت تحریریه: Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.