دوشنبه 20 اسفند 1397 - 07:13

عارضه پیشرفت هوش مصنوعی

پژوهشگران دانشگاه نیویورک می‌گویند پیشرفت هوش مصنوعی هک کردن سیستم‌های بیومتریک را تسهیل می‌کند و بدین ترتیب این سیستم‌ها دیگر امن‌ترین روش برای حفظ اطلاعات و حریم شخصی نخواهند بود.

پژوهشگران دانشگاه نیویورک می گویند پیشرفت هوش مصنوعی هک کردن سیستم های بیومتریک را تسهیل می کند و بدین ترتیب این سیستم ها دیگر امن ترین روش برای حفظ اطلاعات و حریم شخصی نخواهند بود.

به گزارش ایسنا و به نقل از فرچون، فناوری شناسایی اثر انگشت و تشخیص چهره از جدیدترین و امن ترین اشکال حفظ امنیت اطلاعات در حال حاضر هستند که از این دو نشانه منحصر به فرد برای حفظ اطلاعات خصوصی و حریم شخصی استفاده می کنند. این سیستم ها را سیستم های بیومتریک می نامند.

در عصری که هر چند ماه یک بار یک نقص امنیتی در یک شرکت بزرگ فناوری اطلاعات هویت کاربران را در قلمرو دیجیتال فاش می کند یا این اطلاعات هک می شوند، مهم است که کاربران از خود محافظت کنند. در حالی که سیستم های بیومتریک به آن اندازه که فکر می کنید ایمن نیستند.

اگر شما یک کاربر تلفن همراه هوشمند هستید احتمالاً گوشی شما دارای یک اسکنر اثر انگشت یا فناوری تشخیص چهره یا هر دو است. وقتی سیستم های بیومتریک برای اولین بار به صورت تجاری عرضه شدند، به عنوان اشکال نهایی فناوری امنیتی معرفی شدند.

این ادعا اغراق آمیز هم نبود، چرا که اثر انگشت و چهره هر فرد منحصر به خودش است و هیچ کس نمی تواند آن را کپی کند. با این حال تحقیق جدید محققان دانشگاه نیویورک می گوید که سیستم های بیومتریک ممکن است به آن اندازه که فکر می کنیم، ایمن نباشند.

پیشرفت های هوش مصنوعی به طور بالقوه به هکرها این قدرت را می دهد که یک سیستم بیومتریک را گول بزنند و در آینده ای نزدیک اطلاعات شما را سرقت کنند.

در صورتی که هکر بخواهد اطلاعات شما را با استفاده از چهره یا اثر انگشت شما سرقت کند آن قدر هم پیچیده نیست و راه های مختلفی برای انجام این کار وجود دارد. اول و مهم تر از همه اینکه یک هکر می تواند اثر انگشت یا اسکن چهره شما را جایگزین کند و به طور غیر مجاز به سیستم شما دسترسی پیدا کند.

بزرگترین مسئله زمانی اتفاق می افتد که شما نتوانید رمز عبور خود را بازیابی کنید. وقتی اطلاعات بیومتریک شما منحصر به بدن شما است، در صورت دزدیده شدن این اطلاعات چه راه دیگری برای دسترسی به اطلاعات شخصی خود خواهید داشت؟

بنابراین پیشرفت هوش مصنوعی می تواند دردسرساز شود چرا که هوش مصنوعی می تواند فرآیند سرقت هویت شما را بسیار ساده کند.

محققان دانشگاه نیویورک در این راستا یک ابزار ایجاد کرده اند که می تواند به منظور باز کردن دستگاه های کاربران اثر انگشت جعلی بسازد.

آنها حتی نشان داده اند که چگونه شبکه های عصبی مصنوعی عمیق را می توان در طول زمان آموزش داد تا چهره هایی جدید بسازند.

اگر چه این ایده که کسی که با استفاده از هوش مصنوعی دستگاه اندروید کسی را هک کند چیزی در یک فیلم علمی-تخیلی به نظر می رسد، اما این اتفاق اکنون به واقعیت بسیار نزدیک شده است.

اکنون این پرسش مطرح می شود که آیا سیستم های بیومتریک در دراز مدت برای تأمین امنیت کافی خواهند بود یا ما

باید در آن تجدید نظر کنیم؟