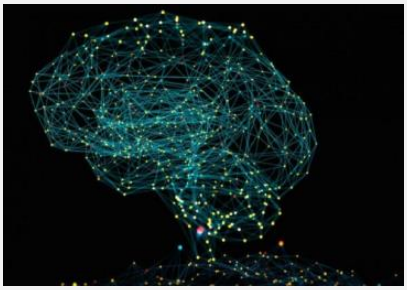

دوشنبه 21 بهمن 1398 - 07:27

محققان ام آی تی هوش مصنوعی گوگل را فریب دادند

تا به حال از شیوه‌های مختلفی برای فریب سیستم‌های هوش مصنوعی استفاده شده و در تازه‌ترین رویداد از این دست، محققان دانشگاه ام آی تی سیستم هوش مصنوعی گوگل را فریب داده اند.

تا به حال از شیوه های مختلفی برای فریب سیستم های هوش مصنوعی استفاده شده و در تازه ترین رویداد از این دست، محققان دانشگاه ام آی تی سیستم هوش مصنوعی گوگل را فریب داده اند.

به گزارش خبرگزاری مهر به نقل از نکست وب، پژوهشگران این دانشگاه یک سیستم متنی موسوم به تکست فولر ابداع کرده اند که می تواند مدل های هوش مصنوعی که از سیستم پردازش زبان های طبیعی استفاده می کنند را گول بزنند.

بسیاری از دستیارهای صوتی مانند الکسای آمازون و سیری اپل از سیستم پردازش زبان های طبیعی برای درک دستورات کاربران استفاده می کنند و لذا فریب آنها می تواند امنیت چنین سیستم هایی را به خطر بیاندازد. همچنین فریب سیستم مذکور موجب سوءاستفاده از آنها برای ارسال هرزنامه یا متون غیرمؤدبانه می شود.

تکست فولر یک سیستم فریبنده است که با درک نقص ها و ضعف های سیستم پردازش زبان های طبیعی آنها را فریب می دهد.

این سیستم جملاتی را با دستکاری چند کلمه آنها به خورد سیستم پردازش زبان های طبیعی می دهد، بدون اینکه دستکاری یادشده موجب تغییر معنا یا ایجاد غلط های دستور زبانی شود.

بعد از این کار و بررسی واکنش سیستم پردازش زبان های طبیعی به این تغییر، به تدریج تغییرات جدی تر و عمیق تری در جملات ایجاد می شود تا در نهایت از حساسیت و دقت این سیستم کاسته شود و بتوان آن را فریب داد.

محققان دانشگاه ام آی تی می گویند با همین روش سه مدل متداول در سیستم پردازش زبان های طبیعی را دستکاری کرده و فریب داده اند.

یکی از این مدل ها که برت نام دارد، یک مدل زبانی متن باز ابداع شده توسط گوگل است که تنها تغییر ۱۰ درصد از بخش های هر جمله توسط تکست فولر به فریب آن منجر شد. بر همین اساس انتظار می رود شرکت های فناوری برای ارتقای سیستم پردازش زبان های طبیعی اقدام کنند تا از دستکاری آن جلوگیری کنند.