هوش مصنوعی مراقب ماست

حفاظت از دانش‌آموزان یا تهدید حریم خصوصی؟

هوش مصنوعی در حال پیشرفت است و دیگر به حضور این موجود ناشناخته در لابه‌لای خبرهایی که می‌خوانیم و می‌شنویم عادت کرده‌ایم. ادعا می‌شود هوش مصنوعی قادر است اسلحه‌های پنهان‌شده در مدرسه‌ها را بیابد و با این کار مانع کشتار دانش آموزان شود هرچند که در حال حاضر احتمال اشتباه زیاد است و به‌راحتی فریب می‌خورد. هوش مصنوعی تا کجا در زندگی ما پیش خواهد رفت؟ تا کجا مراقب ما خواهد بود؟ هوش مصنوعی دیگر یک داستان نیست؛ واقعیت محضی است که باید مراقبش باشیم.

از زمان تیراندازی مشهور دبیرستان کلمباین در سال ۱۹۹۹ تا به امروز بیش از ۱۸۷ هزار دانش‌آموز در مدرسه‌های آمریکا مورد تهاجم مسلحانه قرار گرفته‌اند. Tim Button که یکی از نزدیکانش قربانی تیراندازی در مدارس آمریکاست، تصمیم گرفته با تاسیس شرکتی و استفاده از جدیدترین سامانه‌های امنیتی، راهکاری برای شناسایی افرادی که احتمال می‌رود در مدرسه دست به تیراندازی بزنند، ارائه کند. این شرکت به‌نام Shielded Students در ابتدا همکاری خود را با چند شرکت دیگر آغاز کرد؛ از جمله شرکت کانادایی Patriot One که با ترکیب یک اسکنر ریزموج و **هوش مصنوعی** قادر است اسلحه‌های مخفی‌شده را شناسایی کند. Shielded Students امید دارد که بتواند با ترکیب چنین فناوری‌هایی در قالب یک بسته، مانع کشتار دانش‌آموزان در مدرسه‌ها شود. درحالی‌که قانون‌گذاران و وکلا مشغول سروکله زدن با قوانین مربوط به حمل اسلحه در آمریکا هستند، شمار شرکت‌های حامی Shielded Students رو به افزایش است. بسیاری از این شرکت‌ها مدعی هستند که قادرند با کمک روش‌های **هوش مصنوعی** و با تحلیل تصاویر زنده یا بررسی تصاویر دوربین‌های نظارتی، حاملان اسلحه را به‌طور خودکار شناسایی کنند. اگر چه ممکن است این ادعا در حالت کلی خیال بسیاری از والدین را آسوده کند، اما برخی از کارشناسان از این نگران هستند که مدرسه‌ها به‌طور گسترده زیر نظارت چشم‌های پنهان قرار گیرند و شرکت‌های خصوصی با کمک **هوش مصنوعی** بتوانند حجم بسیار زیادی از داده‌های مربوط به دانش‌آموزان را جمع‌آوری کرده و دست به تجزیه‌وتحلیل آن‌ها بزنند. مهم‌تر این‌که هنوز اطلاعات کافی در مورد عملکرد این سامانه‌های هوشمند شناسایی اسلحه در محیط شلوغ یک مدرسه وجود ندارد. Shielded Students در حال مذاکره با مسئولان مدرسه‌ها است تا آن‌ها را متقاعد کند این سامانه امنیتی را بیازماند و اگرچه Button معتقد است که شاید این سامانه‌ها موفق به شناسایی همه موارد نشوند، اما اطمینان می‌دهد که استفاده از **هوش مصنوعی** تأثیر زیادی بر کاهش آمار قربانیان خواهد داشت.

□□□□□□□
LabSix
□□□□
□□□□□□
□□ □□
□□□□□□
□□□□□□□
□□□□□□
□□□□□
□□□□□□
□□□□ □□
□□□□
□□□□.
□□□
□□□□□□
□□□□□□
□□
□□□□□□□
□□□□□ □□□□□□□ □□□□ □□□.

Virtual eForce از دیگر، استارت‌آپ‌هایی است که قصد دارد با استفاده از فناوری‌های پیشرفته و بررسی تصاویر دوربین‌های نظارتی، مهاجمین مسلح در مدرسه‌ها را شناسایی کند. درصورتی‌که سامانه به فردی مشکوک شد، انتظامات مدرسه را آگاه می‌کند و آن‌ها با بررسی بیشتر، تصمیم نهایی را می‌گیرند که آیا این یک تهدید جدی است و به دخالت پلیس نیاز دارد یا خیر. در سامانه‌های فعلی امکان اشتباه زیاد است، به‌طوری‌که ممکن است سامانه به‌اشتباه یک شی دیگر را به‌جای اسلحه شناسایی کند. اغلب این شرکت‌ها وعده داده‌اند که امکان تشخیص چهره را نیز به سامانه تشخیص اسلحه بیفزایند. این مورد می‌تواند نگرانی‌ها را در زمینه حفظ حریم خصوصی دانش‌آموزان بیشتر کند.

مطلب پیشنهادی

ترفندی برای حفظ حریم شخصی در هنگام کار با ویندوز
با این اپ ویندوز جلوی استفاده مخفی برنامه‌ها از وب‌کم دستگاه را بگیرید

علاوه بر بحث حریم خصوصی، نگرانی‌هایی نیز در مورد امنیت این سامانه‌ها مطرح است. مثلا این‌که هکرها با نفوذ به چنین سامانه‌هایی و تغذیه آن‌ها با هزاران یا میلیون‌ها تصویر جعلی، راهی برای به اشتباه انداختن سامانه بیابند (فرایندی که در حوزه **هوش مصنوعی** به adversarial attack معروف است) Andrew Ilyas، دانشجوی دکترای علوم کامپیوتر از دانشگاه ام‌آی‌تی می‌گوید: «به عقیده من اولویت نخست این است که بپذیریم چنین حملاتی وجود دارند و بدانیم اگر یک مهاجم انگیزه کافی برای در هم شکستن یک سامانه مبتنی بر یادگیری عمیق را داشته باشد، راهی برای این کار پیدا خواهد کرد.» او و همکارانش در گروه تحقیقات **هوش مصنوعی** LabSix دانشگاه ام‌آی‌تی چندین بار موفق شده‌اند، به همین روش، ابزارهای مبتنی بر یادگیری عمیق را فریب دهند. البته به گفته Anish Athalye، از دیگر اعضای این گروه نمی‌توان گفت که فریب‌دادن یک سامانه نظارتی مبتنی بر **هوش مصنوعی** چه میزان ساده است و تاکنون کسی به‌طور علنی ادعای اجرای موفقیت‌آمیز یک حمله adversarial روی چنین سامانه‌های نظارتی نداشته است.

تاریخ انتشار:

14 دی 1397

نشانی منبع:
https://www.shabakeh-mag.com/security/13971/%D8%AD%D9%81%D8%A7%D8%B8%D8%AA-%D8%A7%D8%B2-%D8%AF%D8%A7%D9%86%D8%B4%E2%80%8C%D8%A2%D9%85%D9%88%D8%B2%D8%A7%D9%86-%DB%8C%D8%A7-%D8%AA%D9%87%D8%AF%DB%8C%D8%AF-%D8%AD%D8%B1%DB%8C%D9%85-%D8%AE%D8%B5%D9%88%D8%B5%DB%8C%D8%9F