فرار هوش مصنوعی، یک سناریوی ترسناک

هوش مصنوعی

محبوبه ستارزاده
گروه علم و فناوری

ظاهراً ماجرای جنجالی سرکشی هوش مصنوعی OpenAI تمامی ندارد. عامل هوش مصنوعی اپن ای آی که اخیراً در یک حادثه تاریخی در دنیای سایبری، یک سناریو درست مانند فیلم‌های سینمایی رقم زده و حملات گسترده‌ای علیه پلتفرم Hugging Face ترتیب داده بود، حالا بدون اجازه و با یک سرکشی تمام عیار، سراغ اهداف دیگری رفته است. این موضوع به اپن‌ای‌آی محدود نمانده و در تازه‌ترین خبر، آنتروپیک نیز از دست‌کم سه مورد فرار مشابه ایجنت‌های خود و نفوذ به سازمان‌های دیگر خبر داده است. این موضوع زنگ خطر ناتوانی بشر در ایجاد یک هوش مصنوعی امن را به صدا درآورده است. هرچند گزارش‌های اولیه از حمله به حساب یکی از مشتریان شرکت فناوری Modal Labs حکایت داشت ولی اطلاعات بعدی نشان داد که این مدل آزمایشی ایجنت اپن ای آی به چهار حساب کاربری در چهار سرویس مجزا نفوذ کرده است. با اینکه هویت این سرویس‌ها به طور رسمی فاش نشده، اما منابع آگاه تأیید کردند که Modal Labs یکی از این اهداف بوده، البته زیرساخت اصلی خود شرکت، هدف هک قرار نگرفته و امنیت کلی پلتفرم حفظ شده است.

میلیاردها دستیار هوش مصنوعی یاریگر مردم می‌شوند

موضوع امنیت عامل‌های هوش مصنوعی (ایجنت‌ها) وقتی جدی‌تر می‌شود که نقبی به صحبت‌های مارک زاکربرگ، مدیرعامل متا داشته باشیم. او در تازه‌ترین اظهارنظر خود پیش‌بینی کرده است، طی پنج سال آینده، میلیاردها نفر دستیارهای هوش مصنوعی شخصی خواهند داشت که به صورت شبانه‌روزی برای پیشبرد اهداف آنها در زمینه‌های امور مالی، سلامت و مدیریت خانه فعالیت می‌کنند. این موضوع در حالی مطرح می‌شود که در مدتی کوتاه ایجنت‌های هوش مصنوعی اپن ای آی که هنوز در حال تست شدن بودند، دو بار راه خود را به اینترنت آزاد پیدا کردند و موفق به هک شرکت «هاگینگ فیس» و Modal Labs شدند. با توجه به این حمله غافلگیرکننده، موضوع امنیت ایجنت‌های هوش مصنوعی باز هم زیر ذره‌بین رفت.

فرار از محیط امن

اما ماجرای حمله جدید عامل هوش مصنوعی اپن ای آی چه بوده و چه تفاوتی با حمله قبلی این ایجنت به «هاگینگ فیس» داشته است؟ در مجموع می‌توان گفت اینکه ترکیبی از مدل‌های اپن ای آی، از جمله یک مدل که هنوز منتشر نشده، در طول آزمایش داخلی دچار مشکل شده و با فرار از قرنطینه، موفق به هک شرکت‌های دنیای واقعی شده، نگرانی‌های فراوانی درباره امنیت هوش مصنوعی پیشرو ایجاد کرده است.

درحالی که مهندسان کمپانی اپن ای آی در حال آزمایش قدرت نفوذ و هک مدل‌های پیشرفته و آینده خود ازجمله GPT-5.6 Sol در یک محیط قرنطینه بودند، ظاهراً این ایجنت خودسر این محیط را کافی ندانست و برای یافتن پاسخ سؤالات خود دنبال یک روزنه امنیتی گشت. این آزمایش به‌گونه‌ای طراحی شده بود که این مدل‌های هوش مصنوعی در یک محیط آزمایشی امن (سندباکس) و تحت نظر کارشناسان نگهداری شوند و محققان دریابند که این مدل‌ها چگونه و تا چه حدی می‌توانند با شناسایی آسیب‌پذیری‌های آنلاین، یک حمله سایبری موفق انجام دهند. کارشناسان معتقد بودند به این ترتیب می‌توان با مرور عملکرد و توانایی‌شان، از آنها برای افزایش امنیت سایبری دستگاه‌های مجهز به هوش مصنوعی استفاده کرد. اما ماجرا به گونه‌ای دیگر رقم خورد. این عامل هوش مصنوعی برای دومین بار در چند روز گذشته، از محیط تست خارج شد و در حالی که دفعه قبل اقدام به هک پایگاه‌های اطلاعاتی شرکت هاگینگ فیس کرده بود، این بار سراغ Modal Labs رفت تا از حساب یکی از مشتریان این شرکت برای اجرای کدهای خود بهره بگیرد.

ایجنت‌ها به دنبال یک راه میان‌بر

این ایجنت هوش مصنوعی در حمله جدید خود هم درست مانند هاگینگ فیس، برای تقلب در بنچمارک ExploitGym (ارزیابی قابلیت‌های سایبری)، به دنبال یک میان‌بر بود تا از سرقت داده‌ها و اطلاعات بهترین پاسخ را بگیرد.

این ایجنت خودسر توانست با پیدا کردن یک روزنه امنیتی، از محیط تست خود(سندباکس) خارج شود و در نهایت، این عامل هوش مصنوعی که به دنبال یک راه نفوذآسان بود، وارد حساب مشتری شد. البته نکته اصلی اینجاست که بی‌احتیاطی مشتری شرکت فناوری Modal Labs در نوشتن یک کد آسیب‌پذیر، راه را برای نفوذ این عامل هوش مصنوعی باز کرد. امنیت این کد که بدون رمز عبور و نیاز به احراز هویت منتشر شده، بسیار پایین بود و همین موضوع به پاشنه آشیل Modal Labs تبدیل شد. در نهایت هم حساب این مشتری بدون حضور هیچ عامل انسانی، هدف حمله یک ایجنت هوش مصنوعی سرکش قرار گرفت.

هرچند کارشناسان اپن ای آی اعلام کرده‌اند که حمله این عامل‌های هوش مصنوعی به شرکت‌ها مشکل خاصی ایجاد نکرده ولی واقعیت این است که این موضوع می‌تواند چشم‌انداز ترسناکی برای آینده دنیای هوشمند ترسیم کند. بی شک یکی از بخش‌هایی که ممکن است بیش از بقیه از خطرهای احتمالی ایجنت‌های هوش مصنوعی آسیب ببینند، بورس، بانک‌ها و حساب‌های کارگزاری و مالی است. تفاوتی نمی‌کند که ایجنت‌ها به صورت خودسرانه دست به کار شوند یا از یک شخص، دولت یا گروه خاص فرمان بگیرند. بی‌شک این موضوع در آینده می‌تواند کابوس سهامداران باشد. از آنجا که حالا بیشتر دستگاه‌ها از طریق فناوری اینترنت اشیا(IOT) به اینترنت و در نهایت به یکدیگر اتصال دارند، نبود امنیت در استفاده از ایجنت‌های هوش مصنوعی که قرار است یاریگر بشر در بخش‌های مختلف سلامت، خانه، شرکت‌ها و... باشند، موضوعی است که نمی‌توان نسبت به آن بی‌تفاوت بود.

دامنه این نگرانی‌ها به حدی افزایش یافت که اف بی‌آی هم به موضوع فرار ایجنت‌های هوش مصنوعی اپن ای آی از سندباکس این شرکت ورود کرد. هرچند اطلاعات دقیقی از نحوه این اتفاق وجود ندارد و هنوز این موضوع در هاله‌ای از ابهام قرار گرفته ولی این امر، لزوم نظارت دقیق‌تر بر عامل‌های هوش مصنوعی را پررنگ‌تر کرده و غول‌های فناوری از آن به عنوان یک زنگ خطر در دنیای تکنولوژی یاد می‌کنند.

دانش‌بنیان

راهکارهای جدید برای تأمین سرمایه در گردش شرکت‌های دانش‌بنیان

معاون علمی، فناوری و اقتصاد دانش‌بنیان رئیس جمهوری در اولین نشست با فعالان انجمن صنایع پیشرفته و انجمن صنایع تجارت الکترونیک، از اصلاح طرح «هم‌افزار» برای تأمین مالی شرکت‌های دانش‌بنیان خبر داد و گفت: «بر اساس تصمیم‌های جدید، شرکت‌های واجد شرایط می‌توانند تا سقف ۳۰ درصد فروش محصولات دانش‌بنیان و در صورت افزایش تولید، تا سقف ۱۰۰ درصد فروش محصولات دانش‌بنیان سال گذشته یا سه ماهه اول سال جاری، از تسهیلات سرمایه در گردش بهره‌مند شوند.» حسین افشین یکی از چالش‌های اصلی شرکت‌های دانش‌بنیان را موضوع تأمین مالی دانست و یادآور شد: «بر همین اساس، معاونت علمی و صندوق نوآوری و شکوفایی، طراحی سازوکارهای جدید تأمین مالی را در دستور کار قرار داده‌اند. در این زمینه دو روش جدید پیش‌بینی شده که یکی از آنها استفاده از اوراق فناوری است. روند اجرایی این روش پیشرفت کرده و بخش عمده مشکلات آن برطرف شده است. روش دوم نیز طرح «هم‌افزار» است که بر اساس آن، متناسب با آورده بخش خصوصی، تسهیلات در اختیار شرکت‌ها قرار می‌گیرد.»

او با بیان اینکه اجرای این طرح در شرایط کنونی کشور اهمیت ویژه‌ای دارد، گفت: «در شرایطی که تأمین مالی یکی از مهم‌ترین مشکلات کشور به شمار می‌رود، طرح «هم‌افزار» می‌تواند نقش مؤثری در حمایت از شرکت‌های دانش‌بنیان ایفا کند.» معاون علمی رئیس جمهور خاطرنشان کرد: «در این مدل، شرکت متقاضی بخشی از منابع را تأمین می‌کند، صندوق نوآوری و شکوفایی به همان میزان منابع اختصاص می‌دهد و سپس بانک ۶ برابر آن مبلغ را به صورت تسهیلات پرداخت خواهد کرد.»

معاون علمی رئیس جمهور ابراز امیدواری کرد: «با تصمیمات اتخاذ شده در این نشست، ظرف کمتر از یک ماه حدود ۱۰ شرکت که مدارک آنها تکمیل شده است، بتوانند از این تسهیلات بهره‌مند شوند.»

در این نشست، اصغر نورالله‌زاده، رئیس صندوق نوآوری و شکوفایی نیز با تأکید بر ضرورت تدوین یک روش واحد برای تخصیص تسهیلات به شرکت‌های دانش‌بنیان گفت: «پرداخت منابع باید بر پایه معیارهای شفاف، کارشناسی و قابل پاسخگویی انجام گیرد تا از تصمیم‌های سلیقه‌ای جلوگیری شود و امکان دفاع از نحوه تخصیص تسهیلات در برابر نهادهای نظارتی وجود داشته باشد.» او ادامه داد: «قوانین و دستورالعمل‌ها به گونه‌ای نیستند که بتوانند صد درصد افراد را پوشش دهند. آنچه اهمیت دارد این است که روش انتخاب شده بتواند پاسخگوی اکثریت باشد. به اعتقاد من، اگر یک روش بتواند حدود ۸۰ درصد نیازها را پوشش دهد، طبیعی است که حدود ۲۰ درصد از موارد ممکن است خارج از این چارچوب قرار گیرند.»

حوزه فاوا

■ با توجه به استقبال گسترده شرکت‌ها و فعالان حوزه فناوری، مهلت ثبت‌نام و ارسال اطلاعات برای حضور در دومین نمایشگاه فناوری‌های روزآمد ایران «فرایران ۲» تا ۱۵ مرداد ۱۴۰۵ تمدید شد. محصول متقاضی باید جدید یا دارای ارتقای چشمگیر در یک سال اخیر باشد. همچنین محصول باید برای اولین بار در ایران تولید شده و مبتنی بر فناوری داخلی و غیرمونتاژی باشد و پیش از این شاهد رونمایی از آن در سطح ملی نباشیم. علاقه‌مندان می‌توانند تا ۱۵ مرداد ۱۴۰۵ با مراجعه به نشانی farreiran.ir نسبت به ثبت‌نام و ارسال اطلاعات اقدام یا برای دریافت اطلاعات بیشتر با شماره ۶۳۱۰۳۲۱۱-۰۲۱ تماس بگیرند.

کوتاه از فناوری

■ سیاست‌های جدید ایلان ماسک پس از خرید توئیتر و تغییر نام آن به ایکس، به کاربران سرویس ویژه اجازه می‌دهد ویدیوهایی تا مدت‌زمان چهار ساعت را بارگذاری کنند؛ موضوعی که راه را برای انتشار غیرقانونی فیلم‌های بلند سینمایی هموار می‌کند. این بار فیلم سینمایی «مردعنکبوتی، روز از نو» قربانی این سیاست شد. نسخه غیرقانونی و باکیفیت این پیش از آغاز اکران رسمی، در ایکس لو رفت و میلیون‌ها بازدید به دست آورد. هفته گذشته نیز نسخه باکیفیت فیلم سینمایی «اودیسه» در پلتفرم ایکس فاش شده بود که با واکنش سریع یونیورسال و اجرای پروتکل‌های حذف محتوا مواجه شد.

کهکشان

■ یک موشک از کارافتاده اسپیس ایکس با قدرت بیش از سه تن «تی ان تی»، در مسیر برخورد با ماه قرار دارد. انتظار می‌رود این رویداد یک دهانه جدید روی ماه ایجاد کند و انبوهی از گردو غبار و زباله فضایی را در فضا پراکنده کند. این برخورد در قسمت نزدیک ماه رخ می‌دهد و مدار گرد ناسا و همچنین مدار گرد Danuri متعلق به کره جنوبی قرار است تصاویری از قبل و بعد محل برخورد موشک ثبت کنند. یک بوستر موشک چینی هم در سال ۲۰۲۲ میلادی با ماه برخورد و در قسمت دورافتاده آن دهانه‌هایی ایجاد کرد.

خبرهای علم

■ پژوهشگران مجارستانی دریافتند ترکیبات گیاهی به نام «پلی‌فنول» که در چای، توت‌ها، کاکائو و روغن زیتون فراوان یافت می‌شود، می‌توانند با خواص آنتی‌اکسیدانی و ضد التهابی خود، به حفظ عملکرد سلول‌های عصبی و مقابله با فرآیندهای آسیب‌زا در مغز در حال پیری کمک کنند.

■ نتایج یک پژوهش جدید در ژاپن نشان می‌دهد که تنها سه اسید آمینه، تفاوت میان سلول‌های مخروطی حساس به نور قرمز و سبز را رقم می‌زنند؛ یافته‌ای که می‌تواند علت شیوع بالای کوررنگی قرمز-سبز را توضیح دهد و راه را برای توسعه روش‌های درمانی جدید هموار کند.

آگهی تجدید مرحله اول مناقصه عمومی

شرکت توزیع نیروی برق استان گلستان

نوبت اول

شرکت توزیع نیروی برق استان گلستان در نظر دارد اجرای پروژه مسکن ملی به‌شرح ذیل خود را از طریق سامانه تدارکات الکترونیکی دولت مناقصه عمومی یک مرحله‌ای با ارزیابی کیفی (از محل اعتبارات عمرانی) به پیمانکارانی که دارای رتبه و ظرفیت از سازمان برنامه و بودجه کل کشور می‌باشند واگذار نماید.

ردیف	شرح مناقصه	شماره مناقصه	مبلغ تضمین شرکت درمناقصه(ریال)	مبلغ برآوردی (ریال)
۱	اجرای پروژه کلید در دست نهضت ملی مسکن نگارستان در محدوده مدیریت توزیع نیروی برق شهرستان گنبد	۱۴۰۵/۳۵-۲	۱,۸۷۷,۰۰۰,۰۰۰	۳۷,۵۲۴,۹۵۰,۵۲۱

۱- فروش اسناد مناقصه: متقاضیان می‌توانند در صورت تمایل نسبت به واریز وجه از طریق سامانه تدارکات الکترونیکی دولت مبلغ ۳۰۰,۰۰۰ ریال بابت هر مناقصه به‌حساب فراگیر ۱۳۱۳۶۰۳۸۱۴۰۰ نزد بانك تجارت با شناسه واریزی ۳۸۱۴۰۱۰۰ شعبه ولیعصر گرگان به‌نام شرکت توزیع نیروی برق استان گلستان ، جهت دریافت اسناد مناقصه از تاریخ ۱۴۰۵/۰۵/۱۴ لغایت ۱۴۰۵/۰۵/۲۰ به سایت سامانه تدارکات الکترونیکی دولت مراجعه نمایند.

۲- نحوه برگزاری و محل تحویل پاکت الف، مهلت و زمان بازگشایی

پیشنهادات: کلیه مراحل برگزاری مناقصه از دریافت اسناد مناقصه تا ارائه پیشنهاد مناقصه‌گران و بازگشایی پاکت‌ها از طریق درگاه سامانه تدارکات الکترونیکی دولت به آدرس www.setadiran.ir انجام خواهد شد و فقط تحویل پاکت الف مهر و موم شده به آدرس گرگان، خیابان ولی‌عصر، عدالت ۲۳، طبقه اول، دبیرخانه شرکت توزیع گلستان و مهلت آن تا ساعت ۱۱ روز چهارشنبه مورخ ۱۴۰۵/۰۶/۰۴ و زمان بازگشایی پاکات الف ب ج شرکت‌هایی که حداقل امتیاز ارزیابی کیفی را کسب نموده‌اند، در ساعت ۱۱ روز چهارشنبه مورخ ۱۴۰۵/۰۶/۱۱ در اتاق امور تدارکات واقع درگرگان، ابتدای جاده آق‌قلا، بعد از آب منطقه‌ای، ساختمان شماره دو شرکت توزیع برق استان گلستان می‌باشد.

۲-۱- اسناد ارزیابی کیفی و مستندات مربوط به آن از طریق سامانه ارسال گردد.

۲-۲- ارائه اسناد ارزیابی کیفی به همراه اسناد مناقصه (الف ، ب و ج) در یک لفاف کلی به منزله عدم ارائه اسناد ارزیابی کیفی تلقی خواهد شد.

۳- مبلغ ضمانت‌نامه شرکت در مناقصه به میزان مندرج در جدول فوق، به نفع کارفرما مطابق فرم ارائه شده در اسناد مناقصه که به مدت سه ماه از تاریخ افتتاح پاکات معتبر بوده و قابل تمدید تا به مدت سه ماه دیگر باشد باید به یکی از صورت‌های زیر، همراه با اسناد مناقصه در پاکت (الف) به دستگاه مناقصه‌گزار تسلیم شود:

الف- ضمانت‌نامه بانکی و یا ضمانت‌نامه‌های صادرشده از سوی مؤسسات اعتباری غیر بانکی که دارای مجوز فعالیت از سوی بانك مرکزی جمهوری اسلامی ایران هستند.

ب- اصل رسید واریزوجه نقد به حساب سپرده شماره ۴۰۰۱۱۳۲۲۰۷۱۴۵۹۷۲ نزد بانك مرکزی جمهوری اسلامی ایران به نام شرکت توزیع نیروی برق استان گلستان.

پ- ضمانت‌نامه صادره توسط مؤسسات بیمه‌گر دارای مجوز لازم برای فعالیت و صدور ضمانت‌نامه از سوی بیمه مرکزی ایران

ت- اوراق مشارکت بی‌نام تضمین شده بانک‌ها و دولت با قابلیت بازخرید قبل از سررسید (موضوع قانون نحوه انتشار اوراق مشارکت)

ث- وثیقه ملکی معادل هشتادو پنج درصد ارزش کارشناسی رسمی آن

ج- ضمانت‌نامه‌های صادره توسط صندوق‌های ضمانت دولتی که به موجب قانون تأسیس شده یا می‌شوند و طبق اساسنامه فعالیت می‌نمایند.

۴- ذکر شماره مناقصه روی پاکات الزامی بوده و حضور یك نفر از پیشنهاددهندگان در جلسه بازگشایی پاکات (الف،ب،ج) با معرفی‌نامه کتبی معتبرآزاد است

۵- شرکت توزیع گلستان در رد یا قبول هریک یا تمام پیشنهادات مختار است.

۶- به پیشنهادهای فاقد امضا، مشروط، مخدوش و پیشنهاداتی که بعد از انقضای مدت مقرر در فراخوان واصل می‌شود، مطلقاً ترتیب اثر داده نخواهد شد.

۷- تکمیل کردن فرم پرسشنامه اطلاعاتی مربوط به ارزیابی صلاحیت پیمانکاران پیوست اسناد ارزیابی کیفی الزامی است.

۸- هزینه آگهی هر دو نوبت بر عهده دستگاه مناقصه گزار می باشد.

۹- فروشندگان و تولیدکنندگان باید کد معاملاتی فرابورس داشته باشند و مکلف به دریافت و ارسال پیشنهادات از طریق سامانه تدارکات الکترونیکی دولت به نشانی www.setadiran.ir می‌باشند و پرداخت هرگونه کارمزد سامانه فوق به عهده برنده مناقصه می‌باشد.

۱۰- ضمناً این آگهی از طریق شبکه اطلاع رسانی معاملات توانیر به نشانی www.Tavanir.org.ir و پایگاه ملی اطلاع رسانی مناقصات به نشانی http://iets.mporg.ir قابل دسترسی می‌باشد و جهت اطلاعات بیشتر با شماره تلفن ۰۱۷-۳۲۶۸۴۴۱۲ تماس و به شماره تلفن ۰۱۷-۳۲۶۲۷۴۳۰ فاکس نمایید.

۱۱- سایر اطلاعات و جزئیات مربوطه در اسناد مناقصه مندرج است.

روابط عمومی شرکت توزیع نیروی برق استان گلستان

شناسه: ۲۲۳۸۷۴۲

IRAN DAILY
www.newspaper.iran-daily.com
1877