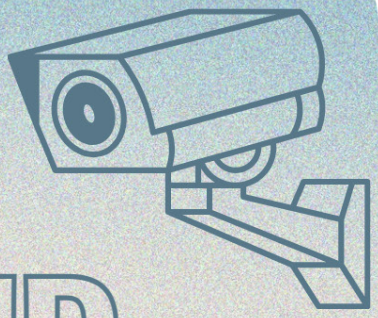
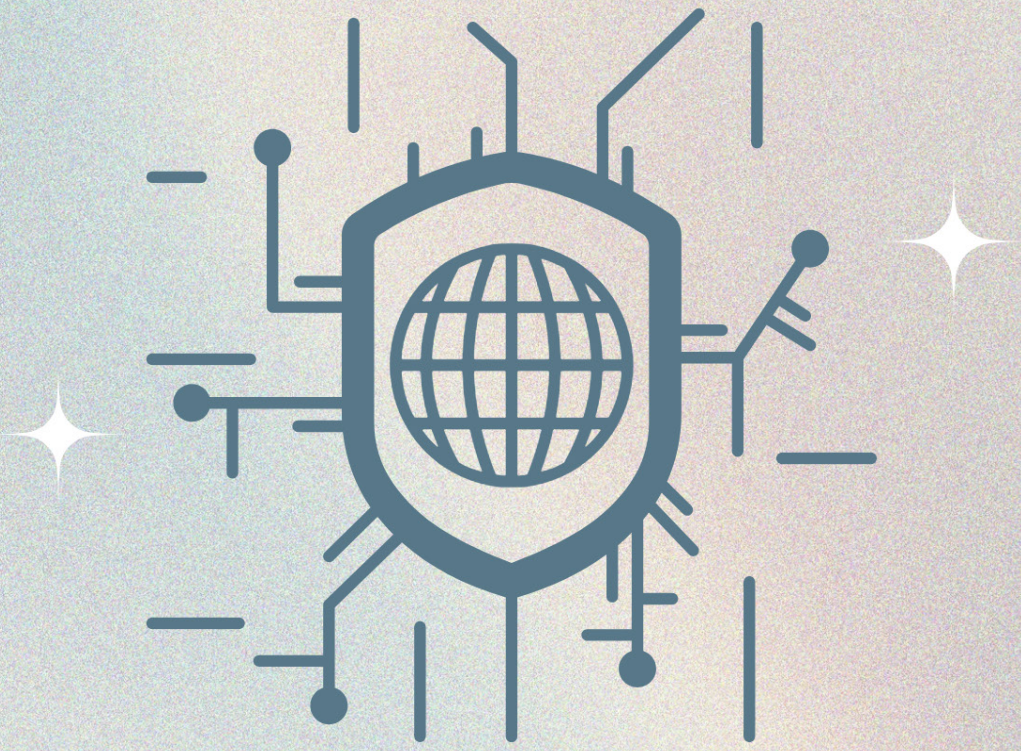
security



INTELLIGENTLAND



spring 2024

بنام خداوند جان و خرد

نشریه علمی زمین هوشمند Intelligent Land
زمستان ۱۴۰۲

سردبیر و مدیرمسئول :
زینب خوش‌نما

نویسندگان این شماره :
کوثر درزی
مصطفی سرحان
زینب خوش‌نما

صاحب امتیاز نشریه:
انجمن علمی برق دانشگاه اصفهان

طراح گرافیک :
زینب‌خوش نما

معاونت
فرهنگی اجتماعی

فهرست

۵ مقدمه

۶ کاربردهای هوش مصنوعی در امنیت سایبری

۸ آینده هوش مصنوعی در امنیت سایبری

۱۰ مانیتورینگ دوربین‌های مداربسته

۱۱ مراجع

امروزه هوش مصنوعی با قابلیت‌های پیشرفته در نظارت، تحول عظیمی در سیستم‌های امنیتی به وجود آورده است. سیستم‌های نظارتی بر هوش مصنوعی قادرند تصاویر ویدیویی زنده را تجزیه و تحلیل کرده، افراد وارد شده به منطقه را بررسی و شناسایی کنند و رفتارهای مشکوک مانند ورود افراد متفرقه یا دسترسی غیرمجاز را تشخیص دهند. این سیستم‌ها از الگوریتم‌های یادگیری ماشین برای یادگیری مداوم و بهبود توانایی خود در تشخیص فعالیت‌های عادی و خطرات امنیتی بالقوه استفاده می‌کنند. با خودکار کردن فرآیند نظارت و هشدار به پرسنل امنیتی در مورد ناهنجاری‌ها، هوش مصنوعی کارآیی و پاسخگویی امنیتی کلی را افزایش می دهد و محیط را برای افراد، ایمن تر می‌سازد.
از سوی دیگر، هوش مصنوعی نقش بسیار مهمی در امنیت سایبری ایفا می‌کند که در ادامه به بررسی آن خوهیم پرداخت.

در این جلد از مجله **زمین هوشمند** به بررسی هوش مصنوعی و امنیت می‌پردازیم.

کاربردهای مختلف هوش مصنوعی در امنیت سایبری

هـوش مصنوعـی (AI) در امنیـت سـایبری می‌توانـد در بسـیاری از زمینه‌هـا و کاربردهـا مـورد اسـتفاده قـرار گیـرد. در زیر، بـه برخـی از کاربردهـای مختلف هوش مصنوعـی در امنیـت سـایبری اشـاره می‌کنـم: اولیـن مـورد تشـخیص تهدیـدات و حمـلات اسـت. هـوش مصنوعـی می‌توانـد بـرای تشـخیص و شناسـایی تهدیـدات و حمـلات سـایبری مـورد اسـتفاده قـرار گیـرد. بـا تحلیـل الگوهـای ترافیـک شـبکه، رفتـار کاربـران، فایل‌هـا و فعالیت‌هـای مشـکوک، مدل‌هـای هـوش مصنوعـی می‌تواننـد تهدیـدات را تشـخیص داده و هشـدارهای لازم را بـه مدیـران ارائـه دهنـد. تشـخیص تقلـب و سوءاسـتفاده یکـی دیگـر از کاربردهـای مهمی هـوش مصنوعی در حـوزه امنیـت اسـت. بـا اسـتفاده از الگوریتم‌هـای یادگیری ماشـین، هـوش مصنوعی می‌توانـد الگوهـای تقلـب و سوءاسـتفاده را در فعالیت‌هـای آنلایـن شناسـایی کنـد کـه شـامل تشـخیص تقلـب در تراکنش‌هـای مالـی، کلاهبـرداری آنلایـن، اسـتفاده غیرمجـاز از حسـاب‌های کاربـری و سـایر فعالیت‌هـای غیرمجـاز اسـت. همچنیـن، نقـش مهمـی در تحلیـل تهدیـدات امنیتـی اسـت. بـه بیـان دقیق‌تـر، ایـن امـکان وجـود دارد کـه از هـوش مصنوعـی در زمینـه تحلیـل و پیش‌بینـی تهدیـدات امنیتـی اسـتفاده کـرد. بـا تجزیـه و تحلیـل داده‌هـای امنیتـی از منابـع مختلـف، ماننـد رویدادهـای سیسـتم، خبرهـا، گزارشـات امنیتـی و اطلاعـات ورودی دیگـر، هـوش مصنوعـی می‌توانـد الگوهـای تهدیـدات را شناسـایی کنـد و بـه تشـخیص زودهنـگام و پیشـگیری از حمـلات کمـک کنـد. یکـی دیگـر از کاربردهـای مهـم در ارتبـاط بـا تشـخیص نفـوذ اسـت. بـا اسـتفاده از هـوش مصنوعـی، می‌تـوان عملکـرد سیسـتم‌های تشـخیص نفـوذ (IDS) و سیسـتم‌های جلوگیـری از نفـوذ (IPS) را بهبـود بخشـید. بـا تحلیـل ترافیـک شـبکه، شناسـایی الگوهـای حمـلات و انـواع نفـوذ، هـوش مصنوعـی می‌توانـد اقدامـات لازم بـرای مسـدود کـردن حمـلات را انجـام داده و امنیـت سیسـتم را تقویـت کنـد. پیش‌بینـی آسـیب‌پذیری‌ها را بایـد یکـی دیگـر از کاربردهـای نوظهـور هـوش مصنوعـی توصیـف کنیـم.

هـوش مصنوعـی می‌توانـد بـرای پیش‌بینـی آسـیب‌پذیری‌ها و ضعف‌هـای امنیتـی در سیسـتم‌ها و نرم‌افزارهـا اسـتفاده شـود. بـا تحلیـل اطلاعـات امنیتی، بررسـی آسـیب‌پذیری‌های نرم‌افزارهـا، مقایسـه بـا الگوهـای شـناخته شـده و اسـتفاده از الگوریتم‌هـای یادگیـری ماشـین، هـوش مصنوعـی می‌توانـد بـه صـورت خـودکار آسـیب‌پذیری‌ها را تشـخیص داده و بـه مدیـران سیسـتم هشـدار دهـد تـا اقدامـات لازم بـرای رفـع آن‌هـا را انجـام دهنـد. تامیـن امنیـت شـبکه یکـی از موضوعـات مـورد علاقـه متخصصـان هـوش مصنوعـی و امنیـت اسـت. هـوش مصنوعـی می‌توانـد در بهبـود امنیـت شـبکه‌ها موثـر باشـد.

بـا تحلیـل ترافیـک شـبکه، تشـخیص حمـلات DDoS، تشـخیص تهدیـدات داخلـی و خارجـی، تشـخیص نفـوذ و رصـد فعالیت‌هـای غیرمعمـول، هـوش مصنوعـی می‌توانـد بهبـود امنیـت شـبکه و پاسـخگویی سـریع در مواجهـه بـا تهدیـدات را فراهـم کنـد. همچنیـن، امـکان اسـتفاده از ایـن فنـاوری در ارتبـاط بـا تحلیـل رفتـار کاربـران وجـود دارد. هـوش مصنوعـی می‌توانـد در تحلیـل رفتـار کاربـران و شناسـایی الگوهـای مشـکوک مـورد اسـتفاده قـرار گیـرد. بـا بررسـی فعالیت‌هـا، رفتارهـا، الگوهـای اسـتفاده و دسترسـی کاربـران، مدل‌هـای هـوش مصنوعـی می‌تواننـد تغییـرات مشـکوک را تشـخیص داده و در صـورت لـزوم، اقدامـات مـورد نیـاز را انجـام دهنـد. بـا رشـد روزافـزون اینترنـت اشـیا، امنیـت ایـن دسـتگاه‌ها نیـز بسـیار مهـم اسـت. هـوش مصنوعـی می‌توانـد بـرای تشـخیص حمـلات و ضعف‌هـای امنیتـی در دسـتگاه‌های اینترنـت اشـیا اسـتفاده شـود و امنیـت آن‌هـا را تقویـت کنـد و تحلیـل اطلاعـات امنیتـی را بـه شـکل دقیقـی انجـام دهـد. بـا حجـم زیـادی از اطلاعـات امنیتـی کـه روزانـه تولیـد می‌شـود، هـوش مصنوعـی می‌توانـد در تجزیـه و تحلیـل و اسـتخراج اطلاعـات مفیـد از ایـن داده‌هـا بـه کار گرفتـه شـود. بـا اسـتفاده از تکنیک‌هـای هـوش مصنوعـی، می‌تـوان الگوهـا، روابـط و اطلاعـات مهـم را در میـان داده‌هـای امنیتـی شناسـایی کـرده و تصمیم‌گیری‌هـای امنیتـی هوشـمندتری اتخـاذ کـرد.

آینده هوش مصنوعی در امنیت سایبری چگونه خواهد بود؟

آینده هوش مصنوعی در امنیت سایبری با ورود به دوره‌ای از تحولات عمده روبه‌رو خواهد بود. در آینده، هوش مصنوعی به عنوان یک ابزار قدرتمند در مقابله با تهدیدات سایبری به کار گرفته خواهد شد. الگوریتم‌ها و مدل‌های هوش مصنوعی بهبود یافته و قدرت تشخیص و پیش‌بینی تهدیدات را بهبود خواهند بخشید. از جمله تحولات مهم در این زمینه می‌توان به توسعه شبکه‌های عصبی عمیق و الگوریتم‌های یادگیری تقویتی، استفاده از فناوری‌های پردازش زبان طبیعی برای تجزیه و تحلیل متن و تشخیص تهدیدات و استفاده از تکنیک‌های پیشرفته در حوزه یادگیری ماشین برای مقابله با تهدیدات نوظهور اشاره کرد. همچنین، همکاری بین هوش مصنوعی و انسان در تصمیم‌گیری و اجرای اقدامات امنیتی نیز تقویت خواهد شد. در کل، آینده هوش مصنوعی در امنیت سایبری افزایش قدرت و کارآمدی در تشخیص، پیش‌بینی و مقابله با تهدیدات سایبری خواهد شد.

انقلابی در مانیتورینگ دوربین‌های مداربسته

هوش مصنوعی با افزایش چشمگیر قابلیت‌های نظارت دوربین‌های مداربسته، اقدامات امنیتی را متحول می‌کند. سیستم‌های نظارت تصویری مبتنی بر هوش مصنوعی می‌توانند فیلم‌های دوربین را به صورت لحظه ای بررسی و تحلیل کنند و فعالیت‌های مشکوک مانند تلاش برای دسترسی غیرمجاز، پرسه زدن یا حرکات نامنظم را شناسایی کنند. فناوری تشخیص چهره، یکی از کاربردهای کلیدی هوش مصنوعی در امنیت، امکان شناسایی سریع افراد در حال ورود یا خروج از محل را فراهم می‌کند و با علامت‌گذاری فوری افراد یا تهدیدات احتمالی، ایمنی را افزایش می‌دهد. علاوه بر این، هوش مصنوعی با استفاده از روش‌های احراز هویت بیومتریک مانند تشخیص چهره یا اثرانگشت، کنترل دسترسی را افزایش می‌دهد و اطمینان حاصل می‌کند که فقط پرسنل مجاز وارد می‌شوند. این پیشرفت‌ها نه تنها تدابیر امنیتی را تقویت می‌کنند، بلکه عملیات را ساده‌تر می‌کنند و زمان پاسخگویی سریع‌تر و تخصیص منابع کارآمدتر در مدیریت پروتکل‌های امنیتی را امکان‌پذیر می‌سازند.

مراجع :

https://lavanertebat.com/ai-in-cyber-security/

https://www.ncsc.gov.uk/guidance/ai-and-cyber-security-what-you-need-to-know

https://lavanertebat.com/ai-in-cyber-security

bing.com

“Humans need and want more time to interact with each other. I think AI coming about and replacing routine jobs is pushing us to do what we should be doing anyway: the creation of more humanistic service jobs.”

Kai-Fu Lee