KNO-1201-4705

نقش هوش مصنوعی برای کشف نفوذ در سیستم های امنیتی

شهاب ترکیshahab.torki1383@gmail.com

دانشجوی مهندسی کامپیوتر دانشگاه ملی مهارت شهرکرد

احسان سلیمانی ehsan.soeimani@maybodiau.ac.ir

دانشجوی دکتری مهندسی کامپیوتر دانشکده مهندسی دانشگاه ازاداسلامی واحد میبد

چکیده

نقش هوش مصنوعی در امنیت سایبری و شناسایی تهدیدات مانند حملات نفوذ، بدافزارها و فیشینگ بررسی شده است. این فناوری با تحلیل رفتارهای غیرعادی، ترافیک شبکه و تشخیص الگوهای مشکوک، به صورت خودکار به مسدودسازی حملات و تقویت حفاظت کمک می‌کند. نمونه‌های کاربردی شامل سیستم‌های تشخیص نفوذ، تحلیل تراکنش‌های بانکی و شناسایی محتوای فریبنده است. در نهایت، هوش مصنوعی نقش مهمی در افزایش امنیت فضای ابری و پاسخ سریع به تهدیدات دارد و آینده امنیت سایبری با توسعه این فناوری قابل تصور است.

کلید واژه: هوش مصنوعی ، امنیت سایبری، شناسایی نفوذ، سیستم‌های امنیتی تحلیل رفتار کاربر، شناسایی بدافزا

مقدمه

در عصر حاضر، امنیت سایبری به عنوان یک چالش اساسی مطرح میگردد، چرا که حجم و تنوع حملات سایبری به طور چشمگیری افزایش یافته و تهدیدات نوظهوری در این حوزه پدیدار گشتهاند. با توجه به پیشرفتهای شگرف در عرصه فناوری و پیچیدگی روزافزون حملات، روشهای سنتی امنیتی به تنهایی قادر به مقابله مؤثر با تهدیدات مذکور نیستند. در این راستا، هوش مصنوعی (Artificial Intelligence)به عنوان یک فناوری پیشرفته، نقش بسزایی در شناسایی و پیشگیری از نفوذ به سیستمهای امنیتی ایفا مینماید.

هوش مصنوعی با بهره گیری از الگوریتمهای یادگیری ماشین، تحلیل ناهنجاریها و پردازش دادههای کلان، قادر است تهدیدات سایبری را در زمان واقعی تشخیص داده و اقدامات مقتضی را جهت حفاظت از سیستم های حیاتی به انجام رساند. این فناوری نه تنها سرعت و دقت در شناسایی تهدیدات را افزایش میدهد، بلکه سازمانها را قادر میسازد تا به صورت پیشگیرانه از وقوع حملات سایبری جلوگیری نمایند.

مقاله حاضر به بررسی نقش هوش مصنوعی در کشف نفوذ به سیستمهای امنیتی میپردازد و روشهایی که این فناوری در راستای مقابله با تهدیدات سایبری ارائه میدهد را مورد تجزیه و تحلیل قرار میدهد. همچنین، نمونه هایی از کاربردهای موفق هوش مصنوعی در تشخیص حملات، شناسایی بدافزارها، پیشگیری از حملات فیشینگ و ارتقاء امنیت فضای ابری ارائه میگردد تا تصویری روشن از قابلیتهای این فناوری در حوزه امنیت سایبری ترسیم شود.

هوش مصنوعی برای کشف نفوذ در سیستمهای امنیتی:

هوش مصنوعی نقش محوری در بهبود امنیت سایبری ایفا میکند و میتواند در کشف نفوذ به سیستمهای امنیتی بسیار مؤثر واقع شود. در این مقاله، امکان بحث پیرامون روشهای استفاده از هوش مصنوعی برای تشخیص تهدیدات امنیتی، الگوریتمهای یادگیری ماشین به منظور تحلیل رفتارهای مشکوک و تکنیکهای پیشرفتهای نظیر شبکههای عصبی و یادگیری عمیق فراهم است.

هوش مصنوعی چگونه میتواند در پیشگیری از حملات سایبری مؤثر باشد؟

هوش مصنوعی میتواند نقش قابل توجهی در پیشگیری از حملات سایبری ایفا نماید، چرا که از توانایی تحلیل حجم عظیمی از داده ها و تشخیص الگوهای مشکوک برخوردار است. برخی از روشهای بهره گیری از هوش مصنوعی در حوزه امنیت سایبری به شرح ذیل است:

- **شناسایی تهدیدات در زمان واقعی:** الگوریتمهای یادگیری ماشین قادرند به صورت مستمر فعالیتهای شبکه را تحلیل نموده و رفتارهای غیرعادی را شناسایی نمایند.
- **تشخیص ناهنجاریها:** مدلهای هوش مصنوعی با بررسی داده های تاریخی، قادر به شناسایی فعالیتهای مشکوک پیش از وقوع حمله میباشند.
- **پیشبینی حملات:** با استفاده از تحلیل الگوهای پیشین حملات، هوش مصنوعی میتواند نوع حملهای که احتمال وقوع آن وجود دارد را پیشبینی نموده و اقدامات پیشگیرانه را توصیه نماید.
- **خودکارسازی پاسخ به تهدیدات:** سیستمهای هوشمند میتوانند به صورت خودکار حملات را مسدود نموده و اقدامات لازم را جهت کاهش خسارات وارده به انجام رسانند.
- **شناسایی بدافزارهای جدید:** مدلهای یادگیری عمیق قادر به شناسایی انواع جدیدی از بدافزارها هستند که ممکن است هنوز در پایگاههای داده امنیتی ثبت نشده باشند.

شکل1:حمله سایبری

هوش مصنوعی چگونه تهدیدات را در زمان واقعی شناسایی میکند؟

هوش مصنوعی میتواند تهدیدات سایبری را به صورت لحظه ای شناسایی نماید، چرا که قادر به تحلیل سریع دادهها و تشخیص الگوهای غیرعادی است. برخی از تکنیکهایی که هوش مصنوعی در این راستا به کار میگیرد عبارتند از:

- **تحلیل رفتار کاربران و سیستمها:** الگوریتمهای یادگیری ماشین میتوانند الگوهای معمول عملکرد کاربران را فرا گرفته و هرگونه رفتار غیرعادی را شناسایی نمایند.
- **سیستمهای تشخیص ناهنجاری:** مدلهای هوش مصنوعی داده های شبکه را تحلیل نموده و هرگونه فعالیت مشکوکی که از الگوهای معمول خارج باشد را شناسایی مینمایند.
- **تحلیل ترافیک شبکه:** با استفاده از پردازش بیدرنگ دادههای شبکه، سیستمهای مبتنی بر هوش مصنوعی قادر به تشخیص سریع فعالیتهای مشکوک و ارائه هشدار میباشند.
- **شناسایی تهدیدات مبتنی بر امضا و الگو:** برخی از سیستمها از پایگاههای داده تهدیدات شناختهشده استفاده میکنند، اما مدلهای پیشرفته هوش مصنوعی میتوانند تهدیدات جدید را بدون نیاز به پایگاه داده کشف نمایند.
- **همکاری با سیستمهای امنیتی دیگر:** هوش مصنوعی میتواند داده ها را از منابع مختلف جمع آوری و پردازش نماید تا دید کاملی از وضعیت امنیتی ایجاد نماید.

مثالی از شناسایی تهدید با هوش مصنوعی:

یکی از نمونه های موفق شناسایی تهدیدات سایبری با استفاده از هوش مصنوعی، سیستمهای تشخیص نفوذ(IDS) است که در سازمانهای مختلف به منظور محافظت از شبکهها به کار گرفته میشوند.

مثال: تصور نمایید که یک بانک دارای یک سیستم امنیتی هوش مصنوعی است که به طور مداوم فعالیتهای شبکه را رصد میکند. این سیستم از الگوریتمهای یادگیری ماشین استفاده میکند تا الگوهای عادی تراکنشهای مالی و ارتباطات درون شبکهای را شناسایی نماید. در یک روز مشخص، هوش مصنوعی متوجه میشود که حجم قابل توجهی از دادهها به طور ناگهانی از یک سرور خاص به مقصدی نامشخص ارسال میگردد—این رفتاری غیرمعمول تلقی میگردد.

با بررسی دقیقتر، سیستم متوجه میشود که این رفتار مشابه یک حمله استخراج داده(Data Exfiltration Attack)است که در آن مهاجمان در تلاش برای استخراج اطلاعات محرمانه کاربران هستند. در نتیجه، هوش مصنوعی به تیم امنیتی هشدار میدهد، انتقال دادهها را متوقف میکند و آدرسهای مشکوک را به لیست سیاه اضافه میکند تا از وقوع حمله جلوگیری به عمل آید.

نتیجه: در غیاب این سیستم هوش مصنوعی، احتمال سرقت اطلاعات حساس بانکی و بروز خسارتهای سنگین وجود داشت. اما به دلیل تشخیص سریع تهدید و انجام اقدامات فوری، امنیت اطلاعات حفظ گردید.

نمونه های بیشتر از کاربرد هوش مصنوعی در امنیت سایبری

در ذیل، نمونههای دیگری از کاربردهای هوش مصنوعی در امنیت سایبری ارائه شده است:

- **شنا سایی و پی شگیری از حملات فی شینگ:** هوش مصـنوعی میتواند هزاران ایمیل را به صـورت آنی تحلیل نماید تا تلاشهای فیشینگ را شناسایی کند. با بررسی الگوها، زبان و رفتار فرستنده، فیلترهای ایمیل مبتنی بر هوش مصنوعی قادر به مسدود نمودن ایمیلهای مخرب پیش از رسیدن به کاربران میباشند.
- **شکار خودکار تهدیدات:** سیستم های امنیتی هوش مصنوعی به طور مداوم شبکه ها را اسکن میکنند تا رفتارهای غیرعادی را شناسایی نموده و تهدیدات مخفی را پیش از آنکه مهاجمان از آسیب پذیری ها سوءاستفاده نمایند، آشکار سازند.
- **تحلیل و شناسایی بدافزارها:** نرم افزارهای آنتی ویروس سنتی معمولاً برای شناسایی بدافزارها به امضاهای شناخته شده متکی هستند، اما هوش مصنوعی میتواند با تحلیل رفتار بدافزار، حتی نسخههای جدید آن را شناسایی نماید، که برای مقابله با تهدیدات روز صفر بسیار مؤثر است.

- **تشخیص تقلب در سیستمهای مالی:** بانکها و مؤسسات مالی از هوش مصنوعی برای نظارت بر تراکنش ها و شناسایی فعالیت های مشکوک استفاده مینمایند. در صورت شناسایی رفتار غیرعادی توسط هوش مصنوعی، نظیر برداشت های ناگهانی با مبالغ بالا یا انتقال به مکانهای نامتعارف، هشدارهای امنیتی فعال شده و یا تراکنش مسدود میگردد.
- **مدیریت هویت و دسترسی) (IAM):**هوش مصنوعی امنیت احراز هویت را با تحلیل الگوهای ورود و شناسایی ناهنجاری ها بهبود میبخشد، تا اطمینان حاصل شود که تنها کاربران مجاز به سیستم های حساس دسترسی دارند.
- **اتوماسیون امنیتی:** هوش مصنوعی قادر به انجام پاسخهای خودکار به تهدیدات، نظیر جداسازی دستگاههای آلوده، مسدود نمودن آدرسهای IP مخرب یا اصلاح آسیبپذیریها بدون نیاز به دخالت انسانی میباشد.
- **تشخیص دیپفیک:** با پیشرفت فناوری دیپفیک، هوش مصنوعی برای شناسایی تصاویر، ویدئوها و فایلهای صوتی جعلی که میتوانند برای تقلب یا انتشار اطلاعات نادرست مورد استفاده قرار گیرند، به کار گرفته میشود.
- **افزایش امنیت فضای ابری:** هوش مصنوعی به صورت مداوم محیط های ابری را برای شناسایی آسیب پذیری ها، تلاشهای دسترسی غیرمجاز و ضعف های پیکربندی اسکن میکند تا امنیت زیرساختهای مبتنی بر فضای ابری حفظ شود.

شکل2:امنیت سایبری

هوش مصنوعی چگونه تلاشهای فیشینگ را شناسایی میکند؟

هوش مصنوعی از تکنیک های پیشرفت های برای تحلیل ایمیل ها، وبسایت ها و رفتار کاربران به منظور کشف تلاشهای فیشینگ استفاده میکند. این روشها شامل موارد ذیل هستند:

۱.پردازش زبان طبیعی: هوش مصنوعی محتوای ایمیل ها را بررسی میکند تا کلمات مشکوک، اشتباهات گرامری، درخواست های فوری یا لینکهای فریبنده که شبیه الگوهای شناخته شده فیشینگ هستند را شناسایی نماید.

۲.تحلیل رفتاری: هوش مصنوعی رفتار کاربران را در طول زمان مطالعه میکند و هرگونه فعالیت غیرعادی نظیر ورود از مکان های ناشناخته یا کلیک بر روی لینکهای نامتعارف را تشخیص میدهد.

۳.بررسی لینکها و دامنه ها: هوش مصنوعی لینک های وب موجود در ایمیل ها را با پایگاه داده سایتهای فیشینگ مقایسه نموده و بررسی میکند که آیا شباهتی به دامنههای معتبر دارند یا خیر.

۴.تشخیص تصویر: ایمیلهای فیشینگ اغلب دارای لوگوها و برندهای جعلی هستند. هوش مصنوعی قادر به تحلیل تصاویر به منظور تشخیص تغییرات اعمال شده و یا استفاده نادرست از آنها میباشد.

۵.تحلیل متاداده ایمیل: هوش مصنوعی اطلاعات مربوط به هدر ایمیل، آدرس فرستنده و مسیر ارسال را بررسی میکند تا ایمیلهای جعلی را شناسایی نماید.

۶.یادگیری ماشین برای شناسایی الگوها: هوش مصنوعی با تجزیه و تحلیل حملات فیشینگ پیشین، به طور مداوم یاد میگیرد تا توانایی شناسایی تهدیدات جدید را بهبود بخشد.

۷.هشدار به کاربران و دفاع خودکار: سیستم های امنیتی مبتنی بر هوش مصنوعی میتوانند پیش از کلیک کاربران بر روی لینکهای مشکوک، هشدار دهند یا حتی ایمیلهای جعلی را به طور کامل مسدود نمایند.

سیستم امنیتی چیست؟

سیستم امنیتی مجموعه ای از ابزارها، فناوری ها و فرآیندهایی است که برای محافظت از داده ها، شبکه ها، دستگاه ها و زیر ساخت های دیجیتال در برابر تهدیدات سایبری، دسترسیهای غیرمجاز و حملات طراحی شده است .این سیستم ها در محیط های مختلف نظیر سازمان ها، بانک ها، مراکز دولتی و حتی خانه های هوشمند مورد استفاده قرار میگیرند.

اجزای اصلی یک سیستم امنیتی:

- احراز هویت و کنترل دسترسی: تأیید هویت کاربران و تعیین سطح دسترسی آنها به داده ها.
- رمزگذاری دادهها: تبدیل اطلاعات به فرم های غیرقابل خواندن به منظور جلوگیری از سرقت داده ها.
- سیستمهای تشخیص نفوذ شناسایی و جلوگیری از حملات سایبری.
- دیوارهای آتش فیلتر نمودن ترافیک شبکه و جلوگیری از ورود تهدیدات خارجی.
- هوش مصنوعی و یادگیری ماشین: تحلیل رفتارهای مشکوک و شناسایی تهدیدات سایبری در زمان واقعی.
- پایش و نظارت امنیتی: رصد دائمی فعالیتهای شبکه به منظور کشف هرگونه ناهنجاری.
- مدیریت ریسک و پاسخ به تهدیدات: برنامه ریزی برای مقابله با حملات و کاهش آسیب های احتمالی.

سیستم های امنیتی دیجیتال به طور مداوم در حال پیشرفت هستند تا بتوانند با تهدیدات نوظهور مقابله نمایند.

نتیجه گیری

هوش مصنوعی به عنوان یک فناوری پیشرفته، نقش مهمی در افزایش امنیت سایبری و کشف نفوذ به سیستمهای امنیتی ایفا مینماید. این فناوری با بهرهگیری از الگوریتمهای یادگیری ماشین، تحلیل ناهنجاریها، پردازش بیدرنگ دادهها و همکاری با سیستمهای امنیتی دیگر، قادر به شناسایی تهدیدات سایبری در زمان واقعی و انجام اقدامات پیشگیرانه میباشد.

کاربردهای هوش مصنوعی در شناسایی تهدیدات فیشینگ، تحلیل رفتارهای غیرعادی، شناسایی بدافزارهای جدید، خودکار سازی پاسخ به حملات و افزایش امنیت فضای ابری نشاندهنده توانایی بالای این فناوری در کاهش خطرات سایبری است. همچنین ،ترکیب هوش مصنوعی با سایر تکنیک های امنیتی نظیر رمزگذاری داده ها، احراز هویت چندمرحله ای و مدیریت ریسک میتواند لایه محافظتی قدرتمندی در برابر حملات سایبری ایجاد نماید.

با توجه به پیشرفت روزافزون تهدیدات سایبری، بهره گیری از هوش مصنوعی در حوزه امنیت دیجیتال نه تنها یک ضرورت، بلکه یک انتخاب استراتژیک محسوب میگردد. سازمانها باید سرمایه گذاری در سیستم های امنیتی هوش مصنوعی را افزایش داده، مدلهای امنیتی را به روزرسانی نموده و به توسعه فناوریهای پیشرفته برای مقابله با تهدیدات نوظهور بپردازند.

در آینده، نقش هوش مصنوعی در امنیت سایبری بیش از پیش گسترش خواهد یافت و این فناوری میتواند با شناسایی سریعتر تهدیدات، پیشبینی حملات و خودکارسازی دفاع سایبری، امنیت دیجیتال را به سطحی بالاتر ارتقا دهد.

مراجع

[1] Determining the effective factors on evaluation the cyber defense power of the Army of the Islamic Republic of Iran Mohammad Ghasemi 1 Davod Azar 2 Vahid Sajadi 115-140.

[2] The pattern of threats of new technologies of the Islamic Republic of Iran Army's ground forces vahid Riazi 1 Esmaeil Biabany 2 .. 58-77.

[3]طراحی الگوی مفهومی توسعه اکوسیستم کسب و کارهای دیجیتالی مبتنی بر مطالعات علم سنجی .155-133 :(68)فصلنامه انجمن علوم مدیریت ایران 17

[4] بررسی کاربرد هوش مصنوعی در آموزش و توسعه منابع انسانی حمید قربانی جمشید عطایی فر

[5] بررسی آثار سیاست‌های توسعهٔ فناوری‌های نوین و هوش مصنوعی در گسترش راهبردهای سیاسی کلان با رویکرد سیاست‌های کلی نظام شریف زاده زهرا ,میرکوشش امیرهوشنگ ,حسینی محمد مهدی: 24-47