مروری بر راهکارهای هوش مصنوعی در بهینه سازی امنیت کسب و کار الکترونیک و امنیت سایبری

مهدی میزانی

کارشناسی ارشد مدیریت فناوری اطلاعات دانشگاه آزاد اسلامی واحد تهران مرکزی، تهران، ایران

حمیدرضا آزادی‌فر

کارشناسی ارشد مدیریت فناوری اطلاعات دانشگاه آزاد اسلامی واحد تهران مرکزی، تهران، ایران

علیرضا خوشنویس راد

کارشناسی ارشد مدیریت فناوری اطلاعات دانشگاه آزاد اسلامی واحد تهران مرکزی، تهران، ایران

محمد نمدی پور

کارشناسی ارشد مدیریت فناوری اطلاعات دانشگاه آزاد اسلامی واحد تهران مرکزی، تهران، ایران

چکیده

امروزه با گسترش فضای دیجیتال به تمام جنبه‌های زندگی و محیط کسب‌وکار توجه و نگرانی‌ها در زمینه امنیت سایبری و امنیت کسب‌وکار الکترونیک بیش از پیش مورد توجه قرار گرفته است. وجود امنیت در فضای سایبری و کسب‌وکار الکترونیک یکی از عوامل مهم جهت جلب اعتماد مصرف‌کنندگان و تمایل بیشتر آنان برای استفاده از خدمات و محصولات دیجیتال است. تهدیدات و ترفندهای نفوذ و تخریب روز به روز پیچیده‌تر شده و تامین امنیت سایبری در حال حاضر با استفاده از روشهای سابق امکانپذیر نیست. هوش مصنوعی به عنوان یک فناوری قدرتمند به عنوان یک ابزار نوین برای ارائه روشهای جدید مقابله با تهدیدات سایبری مورد توجه متخصصان امنیت قرار گرفته است. ما در این تحقیق، جدیدترین مقالات و پژوهش‌های ارائه شده در زمینه راهکارهای ارائه شده بوسیله هوش مصنوعی در زمینه امنیت سایبری و روشهای مقابله با تهدیدات را مرور کرده‌ایم. این تحقیق نشان داد که استفاده از روشهای هیبریدی و ترکیب روشهای بدیع توسط هوش مصنوعی و ارائه الگوریتم‌های ترکیبی برای بالا بردن سرعت و دقت تشخیص و شناسایی تهدیدات و مقابله با آنها بسیار مورد توجه محققان در سالهای اخیر بوده است. همچنین توجه به تهدیدات بالقوه در استفاده از اینترنت موبایل و ضرورت ارائه روشهای هوشمند جهت تقویت امنیت آن از اهمیت بالایی برخوردار است.

واژگان کلیدی: هوش مصنوعی، یادگیری ماشین، یادگیری عمیق، امنیت کسب و کار الکترونیک، امنیت سایبری.

مقدمه

امنیت تبادلات الکترونیک یکی از مهم‌ترین جنبه‌های امنیت سایبری در کسب‌وکارهای الکترونیک محسوب می‌شود. با توجه به افزایش روز افزون تبادلات الکترونیک از طریق اینترنت در بخش تجارت، حفظ امنیت این تبادلات و جلوگیری از دسترسی غیرمجاز به اطلاعات محرمانه از اهمیت بالایی برخوردار است (Saini and Rao, 2020). با این حال، رشد تجارت الکترونیک متاثر از عدم اعتماد کاربران در اشتراک‌گذاری اطلاعات مالی و شماره‌های کارت اعتباری خود از طریق اینترنت می‌باشد (Ulbricht and Jahnke, 2018). با ادامه پیشرفت تحول دیجیتال، سازمان‌ها به طور فزاینده‌ای از مزایایی که فناوری‌های مدرن ارائه می‌دهند آگاه می‌شوند. با این حال، با پذیرش بیشتر فناوری، خطر تهدیدات و حملات امنیت سایبری بیشتر می‌شود. بنابراین، نیاز به اقدام پیشرفته‌تری برای محافظت در برابر تهدیدات دائمی در حال تحول وجود دارد (Jada and Mayayise, 2023). بنابراین، برای حفظ و ارتقای اعتماد مشتریان و افزایش نرخ فروش، بازاریابی و سودآوری، رعایت استانداردهای امنیتی و محافظت از اطلاعات شخصی و مالی کاربران از اهمیت بالایی برخوردار است (Rehman and Coggin, 2019). با گسترش فناوری‌های نوین مانند ابرداده‌ها، اینترنت اشیا و محاسبات ابری، حجم زیادی از اطلاعات و داده‌های حساس در معرض سرقت و تخریب قرار گرفته است (Jingguo et al, 2020). از سوی دیگر، رشد چشمگیر تجارت الکترونیک و وابستگی کسب‌وکارها به سیستم‌های اطلاعاتی، فرصت‌های بیشتری را برای حملات سایبری فراهم کرده است (Saini and Rao, 2020). طبق آمارهای منتشر شده، هزینه‌های ناشی از حملات و تهدیدات سایبری سالانه ۶۰۰ میلیارد دلار در سطح جهانی و ۳۰۰ میلیارد دلار در سطح آمریکا برآورد می‌شود (Zhong et al, 2019). بنابراین، تضمین امنیت سایبری سازمان‌ها و حفظ اطلاعات شرکت‌ها در برابر دسترسی غیرمجاز، از وظایف مهم مدیریت و فراتر از آن یک مزیت رقابتی محسوب می‌شود. سرمایه‌گذاری در زیرساخت‌های امنیت سایبری می‌تواند اعتماد مشتریان را جلب کند و آسیب‌پذیری کسب‌وکار در برابر تهدیدات را به حداقل برساند (Jang-Jaccard and Nepal, 2014). طی سال‌های اخیر حجم زیادی از تحقیقات در مورد فناوری‌ها و راهکارهای جدید برای تأمین امنیت سایبری و حفاظت از زیرساخت‌های حیاتی در بخش کسب وکار صورت گرفته است. در دنیای امروز که عصر دیجیتال و ارتباطات الکترونیک حاکم است، امنیت سایبری به یکی از مهم‌ترین چالش‌های فناوری تبدیل شده است. تهدیدات سایبری روز به روز در حال افزایش و پیچیده‌تر شدن هستند و نیازمند راه‌کارهای مقابله‌ای نوآورانه و پیشرفته می‌باشند (Maji, 2020). هوش مصنوعی به عنوان یکی از ابزارهای قدرتمند در تشخیص و مقابله با تهدیدات سایبری فراهم آمده است. استفاده از یادگیری ماشین و یادگیری عمیق در سیستم‌های امنیت سایبری باعث افزایش قابل توجهی در دقت و سرعت تشخیص و پاسخ‌گویی به تهدیدات شده است (Hassan et al, 2019). با این حال، راه‌اندازی چنین سیستم‌های هوشمندی نیز با چالش‌هایی همراه است. تأمین حجم بالای داده‌های آموزشی معتبر و مدیریت حریم خصوصی اطلاعات کاربران از مهمترین این چالش‌ها هستند (Conneau et al, 2017). با توجه به پیچیدگی‌ها و چالش‌های موجود در تأمین امنیت شبکه‌های رایانه‌ای و فضای سایبر، استفاده از قدرت هوش مصنوعی و یادگیری ماشین می‌تواند کمک قابل توجهی به متخصصان امنیت سایبری کند (Kumar and Singh, 2021). طبق یک گزارش منتشر شده توسط، فارستردر سال ۲۰۱۹، بخش امنیت سایبری بزرگترین بازار هدف برای هوش مصنوعی بوده و پیش‌بینی می‌شود استفاده از هوش مصنوعی در امنیت سایبری تا سال ۲۰۲۵ چند برابر افزایش یابد (Forrester, 2020). فناوری هوش مصنوعی امکان پردازش حجم عظیمی از داده‌ها را فراهم می‌آورد، با سرعت بیشتری تشخیص موارد غیر عادی را میسر می‌سازد و می‌تواند الگوهای مخرب را

در داده‌های آموزش دیده شده شناسایی کند. بنابراین، با توجه به رشد روزافزون تهدیدات و حملات سایبری، امنیت شبکه‌ها و زیرساخت‌های حیاتی در آینده نزدیک بدون بهره‌گیری از قدرت هوش مصنوعی و یادگیری ماشین غیر ممکن به نظر می‌رسد.

عدم حل مسائل مربوط به امنیت سایبری می‌تواند تبعات و پیامدهای منفی متعددی به همراه داشته باشد. برخی از مهم‌ترین پیامدهای ناشی از عدم توجه کافی به مقوله امنیت سایبری به شرح زیر است:

۱- آسیب‌پذیری در برابر حملات سایبری: عدم برنامه‌ریزی و سرمایه‌گذاری در زیرساخت‌های امنیت سایبری، سازمان‌ها را در معرض حملات مخرب قرار می‌دهد که می‌تواند منجر به وقفه در فعالیت‌ها، افشای اطلاعات محرمانه و در نهایت خسارات مالی گردد (Chang and Hsu, 2021).

۲- افول اعتماد عمومی: نشت اطلاعات شخصی کاربران و نقض حریم خصوصی آنها می‌تواند اعتماد عمومی را تضعیف کرده و رغبت مشتریان به استفاده از سرویس‌ها و محصولات را کاهش دهد (Taqi et al, 2020).

۳- زیان‌های مالی: هزینه‌های ناشی از حملات سایبری از جمله هزینه‌های بازیابی داده‌ها و سیستم‌ها، از دست دادن درآمد ناشی از توقف فعالیت‌های کسب‌وکار و هزینه‌های قانونی برای جبران خسارات وارده به مشتریان، سازمان‌ها را با چالش مواجه می‌کنند (Woods and Agrafiotis, 2021).

۴- جریمه‌ها و محدودیت‌های قانونی: عدم رعایت مقررات و استانداردهای امنیت سایبری می‌تواند منجر به تحریم‌ها، جریمه‌ها و محدودیت‌های قانونی از سوی مراجع نظارتی گردد (Te Veide et al, 2021).

از آنجا که حملات سایبری و سرقت هویت به شدت در حال افزایش است، کسب‌وکارهای الکترونیکی نیازمند روش‌های نوینی برای مقابله با این حملات هستند (Yuan et al, 2019). بنابراین، توجه به امنیت سایبری و برنامه‌ریزی‌های مدون جهت کاهش آسیب‌پذیری‌ها و مقابله با تهدیدات سایبری امری ضروری برای بقای کسب‌وکارها در عصر دیجیتال است. هوش مصنوعی یک فناوری قدرتمند است که به تیم‌های امنیت سایبری کمک می‌کند تا وظایف تکراری را خودکار کنند، شناسایی و پاسخ تهدید را تسریع کنند و دقت اقدامات خود را برای تقویت وضعیت امنیتی در برابر مسائل مختلف امنیتی و حملات سایبری بهبود بخشند (Kaur et al, 2023). با این حال، ادبیات و انتشارات اخیر نشان داده‌اند که درباره هک شدن، شکافهای امنیتی، دستکاری داده‌ها، مهندسی اجتماعی و روشهای نوین تهاجمات نگرانی‌های روزافزونی وجود دارند. شیوه‌ها، ویروسها و روشهای مخفی برای دزدیدن اطلاعات و تصاویر شخصی به‌منظور انتشار غیرقانونی آنها، غصب و دزدی هویت در شبکه‌های اجتماعی وجود دارند. جهت تشریح اثر راه‌حلهای کشسان امنیتی و حریم خصوصی می‌توان از روشهایی همچون تعیین استانداردهای جدید، رمزنگاری پیشرفته، بهبود الگوریتم‌های کشف تهاجم، حریم خصوصی شخصی شده و ایزوله کردن ویروسهای مخرب به‌طور مستقل و یا همه آنها با هم برای حداقل‌سازی تهدیدها استفاده نمود. این عمل کاربران را تشویق نموده است تا امنیت و حریم خصوصی چند رسانه‌ای در اینترنت اشیاء، مدنظر قرار دهند. از آگوست ۲۰۱۶، تحقیقاتی وجود داشته است که فرآیندهای پیچیده بازبینی را به انجام رساندند. متخصصان حوزه‌های امنیت و حریم خصوصی با تیزبینی مشغول فعالیت شدند تا توصیه نامه‌ای برای آنها فراهم آورند (اکبری و براتی، ۱۴۰۱).

روش تحقیق

در این پژوهش، ما به دنبال بررسی جدیدترین تحقیقات و مقالات ارائه شده در پایگاه‌های علمی بودیم تا بتوانیم از آخرین وضعیت و رویکرد محققان در زمینه استفاده از هوش مصنوعی در امنیت سایبری آگاه شویم. بدین منظور از پایگاه های علمی Science Direct و IEEE و همچنین برای بررسی تحقیقات و مقالات داخلی از پایگاه علمی مرکز اطلاعات جهاد دانشگاهی استفاده شده است. مقالات با استفاده از ترکیب کلیدواژه‌های هوش مصنوعی، یادگیری ماشین، امنیت سایبری و امنیت کسب و کار جمع‌آوری و پس از غربال‌گری اولیه انتخاب شدند. در این میان مقالاتی که برای بررسی آن با محدودیت دسترسی مواجه شدیم به ناچار حذف شدند.

یافته ها

در (Djenna et al, 2023) پژوهشی جهت شناسایی و تجزیه و تحلیل بدافزارها با استفاده از هوش مصنوعی انجام شده است که در آن با استفاده از روش‌های یادگیری عمیق و رویکردهای هیوریستیک به تجزیه و تحلیل دقیق بدافزارها پرداخته است. نتایج این تحقیق نشان می دهد که استفاده از روش‌های ترکیبی یادگیری عمیق از جمله روشهای مبتنی بر رفتار و روش‌هایی که رویکرد اکتشافی برای شناسایی و طبقه‌بندی بدافزار دارند عملکرد بهتری نسبت به روش‌های یادگیری عمیق استاتیک خواهند داشت.

در (Ali et al, 2023) مزایا و معایب استفاده از هوش مصنوعی در امنیت سایبری مورد بررسی قرار گرفته است و این نتیجه حاصل شده است که مزایای استفاده از هوش مصنوعی در امنیت سایبری شامل شناسایی نرم‌افزارهای مخرب و تهدیدات آنلاین، کاهش خطرات امنیتی، تسریع و افزایش دقت در تشخیص تهدیدات می‌باشد و معایب استفاده از هوش مصنوعی در امنیت سایبری شامل قابلیت کنترل و سوء استفاده از آن به عنوان یک ابزار نظامی، مشکلات در تشخیص تهدیدات پیچیده و نیاز به حضور انسان به جهت اعمال خلاقیت و ابداع در برخورد با تهدیدات است.

در (Qazi et al, 2023) در یک تحقیق در زمینه آزمون یک روش جدید برای تشخیص نفوذ در شبکه اعلام کردند که تهدیدات مخرب به طور مداوم ظهور و تکامل می‌یابند و شبکه به یک راه حل امنیتی بسیار پیشرفته نیاز دارد. آنان دریافتند که استفاده از یادگیری عمیق برای شناسایی ترافیک مخرب، تشخیص تغییرات مختلف در ترافیک را امکان‌پذیر می‌کند و با جلوگیری از ورود آن به سیستم باعث بهبود عملکرد شبکه‌ها می‌شود. برای این منظور در پژوهش انجام شده از یک روش ترکیبی مبتنی بر یادگیری عمیق با استفاده از شبکه عصبی تکرار شونده استفاده شد که نتایج آزمایش نشان داد عملکرد این روش از نظر دقت در سطح بهتری قرار دارد.

در (Kaur et al, 2023) پتانسیل هوش مصنوعی برای بهبود امنیت سایبری در زمینه‌های مختلف مورد بررسی قرار گرفته است و تکنیک‌های مختلف هوش مصنوعی که در حوزه امنیت سایبری استفاده شده ارزیابی شده است و نتایج این پژوهش نشان داد که باید توجه بیشتری به جمع‌آوری و نمایش داده‌های تاریخی مربوط به عملکردهای مختلف امنیت سایبری برای اجرای راه حل‌های علمی امنیت سایبری مبتنی بر هوش مصنوعی شود.

در (Pingale and Sutar, 2022) یادگیری عمیق ترکیبی مبتنی بر بهینه‌سازی نهنگ رمورا و استفاده از ویژگیهای سی‌ان‌ان برای تشخیص نفوذ در سیستم، مورد بررسی و تحقیق قرار گرفته بود. در این روش داده‌های ورودی از قبل پردازش شده و پس از تایید، تبدیل آنها به داده انجام می‌شود. تبدیل داده‌های از پیش پردازش شده با استفاده از روش هولوآنتروپی انجام می‌شود و در همین

حال الگوریتم بهینه‌سازی پیشنهادی با نام RWO برای آموزش مدل عمقی ترکیبی استفاده می‌شود. این مطالعه نشان داده است که این رویکرد توسعه یافته از مدل‌های موجود بهتر عمل می‌کند.

در (Bishtawi and Alzu'bi, 2022) پژوهشی در زمینه امنیت سایبری برنامه‌های تلفن همراه با استفاده از هوش مصنوعی انجام شده است که در آن نحوه استفاده کاربران از تکنیک‌های هوش مصنوعی برای حفظ امنیت در برنامه‌های تلفن همراه با استفاده از یادگیری ماشین، یادگیری عمیق و شبکه عصبی مورد بررسی قرار گرفته است. در این تحقیق از یک روش شبیه‌سازی در یک معادله ریاضی استفاده می‌شود که می‌تواند مقادیر عظیمی از داده‌ها را برای رسیدن به نتیجه تجزیه و تحلیل کند. این روش نیز بیشتر تمرکز بر شناسایی بدافزارها با دقت بیشتر از روشهای مرسوم امروزی دارد. از آنجایی که یکی از خطرناک‌ترین نقاط ضعف تلفن همراه، آگاهی محدود کاربر نسبت به مسائل امنیت سایبری معرفی می‌شود استفاده از روشهای سریعتر و دقیق‌تر از روشهای مرسوم بسیار حائز اهمیت است زیرا در این تحقیق عنوان شده است که روشهای مرسوم فعلی در برابر تهدیدات پیش‌بینی نشده و جدید، موفقیت چندانی نداشته‌اند ولی فناوری‌های یادگیری عمیق توانسته‌اند نتایج امیدوارکننده‌ای را برای کاربردهای مختلف از جمله امنیت سایبری نشان دهند.

در (Zhang et al, 2022) درباره جدیدترین فناوری‌های هوش مصنوعی در امنیت سایبری تمرکز و اعلام کرده است اگر چه رویکردهای مبتنی بر هوش مصنوعی برای شناسایی و دفاع از حملات و تهدیدات سایبری در مقایسه با استراتژی‌های امنیت سایبری مبتنی بر امضاء دیجیتال پیشرفته‌تر و کارآمدتر است ولی کمبود شفافیت و دشواری تفسیرپذیری تکنیک‌های هوش مصنوعی موجود، اعتماد کاربران انسانی را به مدل‌های مورد استفاده برای دفاع از حملات سایبری کاهش می‌دهد. با توجه به اینکه در شرایط فعلی حملات سایبری به طور فزاینده ای متنوع و پیچیده می‌شود حفظ دقت بالا و امکان درک آن، اعتماد مدیریت نسل بعدی مکانیسم‌های دفاع سایبری را می تواند به وجود بیاورد.

در (Funk, 2022) پیامدهای هوش مصنوعی و امنیت سایبری برای مدیریت کسب‌وکار را بررسی کرده و معتقد است امنیت سایبری و هوش مصنوعی باید برای افزایش آگاهی در زمینه امنیت سایبری در سازمان ها با هم همکاری کنند. مطالعات فانک نشان می‌دهد که وقتی صحبت از هوش مصنوعی و امنیت سایبری می‌شود، کسب‌وکارها باید از پیامدهای بالقوه برای مدیریت و عملیات خود آگاه باشند. با پیچیدگی روزافزون فن‌آوری هوش مصنوعی، مجرمان سایبری راه‌های جدیدی برای بهره‌برداری از آسیب پذیری‌ها در سیستم ها و شبکه‌ها پیدا می‌کنند. به این ترتیب، کسب و کارها باید خطرات مرتبط با هوش مصنوعی را درک کنند. و اقداماتی را برای امنیت سایبری و کاهش خطرات آنها انجام دهند.

در (Zhang et al, 2021) چالش‌ها، فرصت‌ها و پیشرفتهای تحقیقاتی کاربرد هوش مصنوعی در امنیت سایبری در زمینه احراز هویت، دسترسی کاربر، رفتار خطرناک و شناسایی ترافیک غیر عادی شبکه مورد بررسی قرار گرفته است و بر اساس یافته‌ها در خصوص چالش‌ها و محدودیت‌ها، ضمن مطرح کردن اهمیت عامل انسانی در این چرخه، یک مدل مفهومی امنیت سایبری با توجه به هوش انسان در این حلقه را ارائه می کند.

در (Naik et al, 2021) در بررسی جامع، تاثیر تکنیک‌های هوش مصنوعی در تقویت امنیت سایبری مورد تحقیق قرار گرفته است و اثرات کاربرد این فن‌آوری‌ها در امنیت سایبری مرور شده است. در این پژوهش، کاربرد تکنیک‌های هوش مصنوعی در تجزیه و

تحلیل، شناسایی و مبارزه با حملات سایبری مختلف بررسی شده است و اثرات اجرای روش‌های هوش مصنوعی "توزیع شده" طبقه بندی شده مشروط و روش‌های هوش مصنوعی "فشرده" طبقه بندی شده بر روی تهدیدات سایبری مختلف بررسی شده است. علاوه بر این، دامنه و چالش‌های آینده استفاده از چنین تکنیک‌هایی در امنیت سایبری مورد بحث قرار گرفته است و نتایجی از نظر ارزیابی استفاده از پیشرفت‌های مختلف هوش مصنوعی در بهبود امنیت سایبری گرفته شده است.

در (Luka et al, 2021) هوش مصنوعی در مدل‌های کسب‌وکار به عنوان یک ابزاری برای مدیریت ریسک‌های دیجیتال در بازارهای بین المللی مورد بررسی قرا گرفته است و عوامل تعیین کننده اصلی هوش مصنوعی را تجزیه و تحلیل کرده است و روشی که استفاده از هوش مصنوعی در مدل کسب‌وکار می تواند به سازمان در مدیریت ریسک‌های دیجیتال کمک کند را بررسی کرده و راه‌های جدیدی برای تحقیقات آینده پیشنهاد کرده است.

در (Sjdon et al, 2021) درباره چگونگی قابلیت‌های هوش مصنوعی در نوآوری مدل کسب‌وکار از طریق مقیاس‌سازی هوش مصنوعی از طریق فرآیندهای تکاملی و حلقه‌های بازخورد پژوهش انجام شده که یافته‌ها سه مجموعه از قابلیت‌های حیاتی هوش مصنوعی را در زمینه خط تولید داده‌ها، توسعه الگوریتم و دموکراسی‌سازی هوش مصنوعی نشان می‌دهند و برای گسترش این قابلیت‌ها شرکتها باید مدل‌های کسب‌وکار خود را با تمرکز بر ایجاد مشترک مشتری چابک، عملیات تحویل مبتنی بر داده و یکپارچه‌سازی اکوسیستم مقیاس‌پذیر، نوآوری کنند. این تحقیق بینش‌ها را در چارچوبی تکاملی برای مقیاس‌پذیری هوش مصنوعی از طریق نوآوری در مدل کسب و کار ترکیب کرده است تا بر مکانسیم ها و حلقه‌های بازخورد تاکید کند همچنین در مورد اینکه چگونه تولید کنندگان می‌توانند هوش مصنوعی را مقیاس‌بندی کنند بینش‌هایی ارائه داده است.

در (Lima et al, 2020) آنتی‌ویروسی مبتنی بر هوش مصنوعی جهت شناسایی پیشگیرانه بدافزار معرفی و مورد آزمایش قرار گرفته است. این آنتی ویروس می‌تواند نحوه عملکرد یک بدافزار را حتی قبل از اجرای آن توسط کاربر شناسایی کند. روش کار این نرم‌افزار بدین گونه است که ویژگیهای استخراج شده از فایل اجرایی که همان ویژگیهای ورودی شبکه‌های عصبی هستند را در یک معماری ۳۲ بیتی به دو کلاس خوش‌خیم و بدخیم طبقه‌بندی می‌کند و از این روش می‌تواند در کمتر از یک ثانیه با دقت بالای ۹۸ درصد نسبت به شناسایی بدافزارها قبل از اجرای آن اقدام کند. همچنین در کنار بررسی این روش جدید و بررسی سیستمهای عامل موجود، اینگونه نتیجه‌گیری شده است که باید کاربرد شبکه‌های عصبی برای امنیت اطلاعات به منظور اعمال سایر فایل‌های اجرایی سیستم‌های عامل غیر ویندوز هم گسترش داده شود. زیرا دیگر سیستمهای عامل از جمله اندروید که توسط تلفن‌های هوشمند و تبلت‌ها در زندگی روزمره مورد استفاده قرار می‌گیرد در حال حاضر به بدافزارهای زیادی اجازه می‌دهد تا در تعداد زیادی از برنامه ها مخفی شوند که می‌تواند به طور جدی امنیت سیستم را تهدید و کاربر را تحت تاثیر قرار دهد.

در (Shaukat et al, 2020) کاربردهای مدل‌های مختلف یادگیری ماشین در زمینه امنیت سایبری مورد بررسی قرار گرفته است و به این نتیجه رسیده‌اند که در هر تهدید سایبری ویژگیهایی وجود دارد که حتی برای مدل‌های پیشرفته یادگیری ماشین نیز مقابله با آن حملات، دشوار است و ارائه یک توصیه کلی برای همه تهدیدات بر اساس یک مدل، غیر ممکن است در این پژوهش، چندین ابزار محبوب یادگیری ماشین بررسی و تاکید شده است که مجموعه داده برای آموزش و آزمایش مدل‌های یادگیری ماشین بسیار حیاتی است.

در (محمد حسینی و همکاران، ۲۰۲۰) محرک‌های ارائه خدمات سایبری پایدار در دولت با تاکید بر حفظ امنیت با استفاده از هوش مصنوعی مورد بررسی و تحلیل قرار گرفته است با توجه به ابعاد امنیتی به گفته کارشناسان، ۱۲ ارائه کننده با بالاترین پتانسیل ارائه خدمات سایبری را شناسایی و در چهار حوزه اولویت‌بندی کرده‌اند و با در نظر گرفتن دو پارامتر کنش و واکنش، روابط بین محرک‌ها را بررسی کردند در نهایت تلاش کرده‌اند با تجویز رویه مناسب سیستم را به پایداری نزدیک کنند. بر اساس نتایج تحقیق، آنان نتیجه‌گیری کرده‌اند که دولت برای ارائه خدمات سایبری باید میزان اقدام و واکنش سازمان را مدنظر قرار دهد و از تصمیم‌گیری‌های پراکنده که اولویت خاصی ندارد، خودداری کند. در تحقق خدمات سایبری خود باید به بعد امنیتی نیز توجه ویژه‌ای داشته باشد.

در (قاسمی و احمدی، ۱۴۰۱) مدل‌های مناسب بهره‌گیری از فناوری هوش مصنوعی در نظارت کارآمد و شفاف مورد بررسی قرار گرفته است و اعلام کردند که مطالعات نشان می‌دهد به دلیل حجم بالای داده‌ها و ضرورت بهره‌گیری از یک سامانه تحلیلی هوشمند می‌توان میزان خطای نظارتی را نزدیک صفر نمود و به جای نظارت مالی سایر شاخص‌های بهره‌وری، منابع انسانی, نوآوری, تولید و. . . را هم در نظارت مؤثر نماید.

در (حسین‌آبادی و زارع فرد، ۱۴۰۱) کاربرد هوش مصنوعی در نظارت الکترونیک و افزایش شفافیت امور مورد پژوهش و بررسی قرار گرفته است و نتایج بررسی ها نشان دهنده الزام استفاده از قابلیت‌های وسیع و مفید هوش مصنوعی در دولت‌ها و ایجاد نظارت الکترونیکی مبتنی بر هوش مصنوعی جهت کشف فوری, جلوگیری و کاهش فساد اداری است. براساس یافته‌ها ,هوش مصنوعی می‌تواند چهار نقش توصیف کنندگی, تشخیص دهندگی, پیش بینی و تصمیم‌گیری را داشته باشد.

در (امینی، ۱۴۰۱) تحقیقی در زمینه تاثیراخلاق کسب‌وکار (امنیت و حریم خصوصی) بر مشارکت کاربران در راهبرد هم‌آفرینی ارزش در یک مطالعه موردی روی شرکت‌های خرده فروشی آنلاین انجام شده است و نتایج نشان داد که حفظ حریم خصوصی کاربران و حفظ امنیت مشتریان در پلتفرم‌های آنلاین بر میزان مشارکتشان در راهبرد هم‌آفرینی ارزش تأثیر گذاشته است. با توجه به رقابتی که در خرده فروشی‌های آنلاین وجود دارد و لزوم وارد شدن اطلاعات کاربر برای خرید محصولات و خدمات به صورت آنلاین, موضوع امنیت اطلاعات کاربران و حفظ حریم خصوصی بیش از پیش اهمیت یافته و به مدیران خرده‌فروشی پیشنهاد می‌شود که در استفاده از درگاه واریزی و همچنین در حفظ اطلاعات کاربران کوشا باشند.

در (مطیع شیرازی و مصطفوی، ۱۴۰۲) مقاله پژوهشی جهت ارائه یک روش برای تشخیص و تقلیل حملات انکار سرویس در اینترنت اشیاء از طریق شبکه‌های نرم‌افزار محور انجام شده است که در این مقاله راهکاری برای تشخیص و تقلیل حملات DoS توزیع شده (DDoS) در اینترنت اشیاء بر پایه SDN ارائه می‌شود. روش پیشنهادی مبتنی بر معیار آنتروپی و شروع جریان و مطالعه مشخصات جریان است. در این روش با استفاده از دو مؤلفه جدید روی کنترل کننده و در نظر گرفتن پنجره زمانی و محاسبه آنتروپی و نرخ جریان، حمله در شبکه تشخیص داده می‌شود. ارزیابی‌ها نشان می‌دهد که این روش حملات را با دقت بالا شناسایی کرده و اثرات آنها را تقلیل می‌دهد.

بحث و نتیجه‌گیری

امروزه با گسترش فضای دیجیتال به تمام عرصه‌های زندگی و محیط کسب‌وکار توجه و نگرانی‌ها در زمینه امنیت سایبری و امنیت کسب‌وکار الکترونیک بیش از پیش مورد توجه قرار گرفته است. رشد فراگیر استفاده از اپلیکیشن ها و اینترنت تلفن همراه، فضای دیجیتال را در برابر حملات سایبری آسیب‌پذیرتر کرده است. متخصصان امنیت همواره به دنبال جدیدترین روشها برای مقابله با تهدیدها هستند. شیوه‌های قبلی دیگر به مانند گذشته پاسخگوی نیازهای امنیتی نبوده و سیستم های امنیتی به دنبال روشهای جدید با کارآیی بیشتر در زمینه امنیت سایبری هستند. هوش مصنوعی به عنوان یک فناوری قدرتمند به تیم‌های امنیت سایبری امکان می‌دهد تا با استفاده از روشهای یادگیری ماشین و یادگیری عمیق، کارهای تکرار شونده را خودکار کرده و علاوه بر امکان تشخیص و پاسخ سریع‌تر به تهدیدات بطور گسترده‌ای در زمینه های تشخیص نفوذ، تشخیص بدافزار و هرزنامه عملکرد بهتر و دقیق‌تری داشته باشند. در تحقیقات اخیر، مشخص شد که تمرکز بر روی سرعت تشخیص تهدیدات و شناسایی آن در مراحل ابتدایی از اهمیت زیادی برخوردار است. شناسایی سریع بدافزارها و حملات نفوذ به شبکه قبل از اجرای فایل‌های اجرایی و یا حتی قبل از پردازش در سیستم، مورد توجه بوده است همچنین در پژوهش‌های بررسی شده، رویکرد فعلی تحقیقات انجام شده استفاده از روشهای ترکیبی مختلف برای پیدا کردن راه‌حل‌ها و روشهای جدید در پیدا کردن الگوریتم‌های شناسایی با استفاده از هوش مصنوعی جهت بالا بردن سرعت و همچنین دقت تشخیص و شناسایی حملات است.

منابع

قاسمی، سیداحمد، و حاتمی، علی، ۱۴۰۱، ارائه مدل مناسب بهره گیری از فناوری هوش مصنوعی در نظارت کارآمد و شفاف. همایش ملی ارتقای شفافیت.

حسین آبادی، سعید، و زارع فرد، مصطفی، ۱۴۰۱، کاربرد هوش مصنوعی در نظارت الکترونیک و افزایش شفافیت امور. همایش ملی ارتقای شفافیت.

اکبری، مهدی، و براتی، حمید، ۱۴۰۱، مروری بر روش های حفظ حریم خصوصی در اینترنت اشیاء. کنفرانس بین المللی مطالعات بین رشته ای در مدیریت و مهندسی.

امینی، حسین،۱۴۰۱، بررسی تاثیر اخلاق کسب و کار (امنیت و حریم خصوصی) بر مشارکت کاربران در راهبرد هم آفرینی ارزش (مورد مطالعه: شرکت های خرده فروشی آنلاین). کنفرانس بین المللی مطالعات بین رشته ای در مدیریت و مهندسی.

مطیع شیرازی، فاطمه و مصطفوی، سیداکبر، ۱۴۰۲، ارائه یک روش جهت تشخیص و تقلیل حملات انکار سرویس در اینترنت اشیا از طریق شبکه‌های نرمافزار محور، نشریه مهندسی برق و مهندسی کامپیوتر ایران.

Djenna A, Bouridane A, Rubab S, Marou IM. Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation. *Symmetry*. 2023; 15(3):677. https://doi.org/10.3390/sym15030677

Qazi, E.U.H.; Faheem, M.H.; Zia, T. HDLNIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System. *Appl. Sci.* **2023**, *13*, 4921. https://doi.org/10.3390/app13084921

de Lima, S.M.L., Silva, H.K.d.L., Luz, J.H.d.S. *et al.* Artificial intelligence-based antivirus in order to detect malware preventively. *Prog Artif Intell* **10**, 1–22 (2021). https://doi.org/10.1007/s13748-020-00220-4

Subhash V. Pingale, Sanjay R. Sutar, Remora whale optimization-based hybrid deep learning for network intrusion detection using CNN features, Expert Systems with Applications, Volume 210, 2022, 118476, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2022.118476.

T. Bishtawi and R. Alzu'bi, "Cyber Security of Mobile Applications Using Artificial Intelligence," *2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI)*, Zarqa, Jordan, 2022, pp. 1-6, doi: 10.1109/EICEEAI56378.2022.10050484.

Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar, Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion, Volume 97,2023, 101804, ISSN 1566-2535, https://doi.org/10.1016/j.inffus.2023.101804.

Zhang, Zhibo & Al Hamadi, Hussam & Damiani, Ernesto & Yeun, Chan & Taher, Dr. Fatma. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. 10.48550/arXiv.2208.14937.

Zhang, Z., Ning, H., Shi, F. *et al.* Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artif Intell Rev* **55**, 1029–1053 (2022). https://doi.org/10.1007/s10462-021-09976-0

A. Ali et al., "The Effect of Artificial Intelligence on Cybersecurity," 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2023, pp. 1-7, doi: 10.1109/ICBATS57792.2023.10111151

An overview of artificial intelligence solutions in optimizing E-Business security and cyber security

Mahdi Mizani

Islamic Azad University, Central Tehran Branch

Hamidreza Azadifar

Islamic Azad University, Central Tehran Branch

Alireza khoshnevis Raad

Islamic Azad University, Central Tehran Branch

Mohammad Namadipour

Islamic Azad University, Central Tehran Branch

1-1-

Abstract

Today, with the expansion of the digital space to all aspects of life and business environment, attention and concerns in the field of cyber security and electronic business security have been given more attention than before. The existence of security in electronic business is one of the important factors to gain the trust of consumers and their desire to use digital services and products. Artificial intelligence as a powerful technology as a new tool to provide new methods of dealing with cyber threats has been noticed by security experts. In this research, we have reviewed the latest articles and research presented in the field of solutions provided by artificial intelligence in the field of cyber security and methods of dealing with threats. This research showed that the use of hybrid methods and the combination of innovative methods by artificial intelligence and the provision of combined algorithms to increase the speed and accuracy of detecting and identifying threats and dealing with them have been of great interest to researchers in recent years. Also, paying attention to the potential threats in the use of mobile internet and the need to provide smart methods to strengthen its security is of great importance.

Keywords: Artificial intelligence, Machine learning, Cyber security, Deep learning, E-Business security.