نهمین کنفرانس ملی مباحث نوین در کامپیوتر و فناوری اطلاعات
9th National Conference on Advanced Topics in Computer and Information Technology
۲۰ آذر ماه ۱۴۰۴

نقش هوش مصنوعی جهت حفظ امنیت در صنایع مختلف

داریوش غنی‌زاده حصار

چکیده : با گسترش روزافزون فناوری‌های دیجیتال و تحول به سمت صنعت ۴.۰، حجم داده‌های تولید شده در صنایع مختلف به شدت افزایش یافته است. این انفجار داده‌ای، چالش‌های جدیدی را در زمینه حفظ محرمانگی، یکپارچگی و در دسترس بودن اطلاعات ایجاد کرده است. روش‌های سنتی امنیت سایبری که بر پایه قوانین از پیش تعیین شده و پاسخ‌های واکنشی استوار هستند، دیگر توانایی مقابله با تهدیدات پیچیده، پویا و در مقیاس بزرگ را ندارند. در این راستا، هوش مصنوعی (AI) به عنوان یک توانمندساز کلیدی، با ارائه قابلیت‌های تحلیل پیشرفته، یادگیری ماشین و تشخیص الگو، نقش حیاتی در پیشگیری، شناسایی و پاسخ به تهدیدات امنیتی ایفا می‌کند. این مقاله به بررسی نقش هوش مصنوعی در حفظ امنیت اطلاعات در صنایع مختلف از جمله مالی، بهداشتی، انرژی و تولید می‌پردازد. همچنین، چالش‌های مرتبط با حریم خصوصی، سوگیری الگوریتم‌ها و حملاتبدافزاری (Adversarial) مورد بحث قرار گرفته و راهکارهایی برای پیاده‌سازی ایمن و کارآمد هوش مصنوعی در زیرساخت‌های حیاتی ارائه می‌شود. یافته‌ها نشان می‌دهد که اگرچه هوش مصنوعی خطر امنیتی را به طور کامل حذف نمی‌کند، اما با کاهش زمان تشخیص و پاسخ به تهدیدات (MTTD و MTTR) و افزایش دقت در شناسایی ناهنجاری‌ها، سطح کلی امنیت اطلاعات را به طور قابل توجهی ارتقا می‌دهد.

کلمات کلیدی: هوش مصنوعی- امنیت- اطلاعات- صنایع

۱ - مقدمه

در دهه اخیر، منظر تهدیدات سایبری دستخوش تغییرات بنیادین شده است. حملات سایبری از حالت‌های ساده و مبتنی بر ویروس‌های کلاسیک، به سمت حملات هدفمند، چندمرحله‌ای و مبتنی بر هوش مصنوعی تکامل یافته‌اند. بدافزارهای نسل جدید قادر به تغییر ساختار خود برای فرار از تشخیص آنتی‌ویروس‌های سنتی هستند و حملات روز صفر (Zero-day) بدون نشانه‌های شناخته شده قبلی رخ می‌دهند. در چنین محیطی، صنایع مختلف با حجم عظیمی از داده‌های حساس روبرو هستند که حفاظت از آن‌ها نه تنها یک نیاز تجاری، بلکه الزامی قانونی و اخلاقی است. صنایع مالی با تراکنش‌های لحظه‌ای، صنایع بهداشتی با پرونده‌های پزشکی محرمانه، صنایع انرژی با زیرساخت‌های حیاتی و صنایع تولیدی با نقشه‌های صنعتی و مالکیت فکری، همگی در معرض خطرات جدی قرار دارند. امنیت اطلاعات بر سه اصل محرمانگی، یکپارچگی و در دسترس بودن استوار است. هوش مصنوعی با توانایی پردازش سریع داده‌های ساختاریافته و غیرساختاریافته، امکان نظارت مستمر و بلادرنگ بر این سه اصل را فراهم می‌کند. برخلاف روش‌های سنتی که نیازمند ورود دستی اپراتورهای انسانی برای تحلیل لاگ‌ها و رویدادها هستند، سیستم‌های مبتنی بر هوش مصنوعی می‌توانند الگوهای پیچیده و ناهنجاری‌های ظریف را در کسری از ثانیه شناسایی کنند. در عصر دیجیتال، صنایع مختلف با حجم عظیمی از داده‌ها، سامانه‌های متصل و تهدیدات امنیتی پیچیده روبه‌رو هستند. در این میان، هوش مصنوعی به‌عنوان یکی از فناوری‌های تحول‌آفرین،

توانسته است نقش مهمی در شناسایی، پیش‌بینی و مقابله با تهدیدات ایفا کند. این مقاله با هدف بررسی عمیق این نقش‌ها، نحوه ادغام هوش مصنوعی در استراتژی‌های امنیت سایبری صنایع مختلف و همچنین ملاحظات اخلاقی و فنی مرتبط با آن تدوین شده است[۲و۱].

۲ – امنیت اطلاعات

با توجه ویژگی‌های عصر امروزی که عصر اطلاعات نیز نامیده شده است مهمترین سرمایه برای هر فرد و یا سازمان اطلاعات است به همین جهت در این عصر، امنیت اطلاعات جزء یکی از مهمترین مسائل امروزی گشته است. امنیت اطلاعات در واقع محافظت از اطلاعات در برابر طیف وسیعی از تهدیدات شامل دسترسی، کاربرد، افشاء، قطع، تغییر یا انهدام غیرمجاز اطلاعات است که با هدف تضمین استمرار فعالیت‌های کاری، به حداقل رساندن ریسک‌های کاری و به حداکثر رساندن میزان بازده سرمایه‌گذاری‌ها و فرصت‌ها صورت می‌پذیرد. طبق این دیدگاه، امنیت اطلاعات، تأثیر مثبت و دراماتیکی بر سازمان دارد. همچنین امنیت اطلاعات، کنترلی برای تضمین تداوم حفاظت از دارایی‌های سازمان از آسیب یا از دست دادن معنا شده است. به عبارت دیگر امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن خطر افشای اطلاعات در بخش‌های غیرمجاز اشاره دارد. امنیت اطلاعات مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری و علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیر مجاز است. افزایش وابستگی صنایع به سامانه‌های دیجیتال، شبکه‌های ارتباطی و زیرساخت‌های هوشمند باعث شده است که امنیت به یکی از مهم‌ترین دغدغه‌های سازمان‌ها تبدیل شود. حملات سایبری، نفوذ به شبکه‌ها، دستکاری داده‌ها و اختلال در سامانه‌های صنعتی می‌توانند خسارات مالی، عملیاتی و حتی انسانی گسترده‌ای ایجاد کنند. در چنین شرایطی، روش‌های سنتی امنیتی که بیشتر بر شناسایی تهدیدات شناخته‌شده تکیه دارند، برای مقابله با تهدیدات نوین کافی نیستند.

هوش مصنوعی با توانایی یادگیری از داده‌ها، شناسایی رفتارهای غیرعادی و واکنش سریع، به‌عنوان راهکاری مؤثر برای ارتقای امنیت در صنایع مختلف مطرح شده است[۳].

۳ – هوش مصنوعی

هوش مصنوعی در امنیت سایبری از زیرمجموعه‌های مختلفی بهره می‌برد که مهم‌ترین آن‌ها یادگیری ماشین[1]، یادگیری عمیق[2] و پردازش زبان طبیعی (NLP) است. یادگیری ماشین به سیستم‌ها اجازه می‌دهد تا از داده‌های تاریخی آموزش ببینند و بدون برنامه‌نویسی صریح، قوانین تشخیص تهدید را استخراج کنند. الگوریتم‌های نظارت‌شده[3] برای طبقه‌بندی ترافیک شبکه به عنوان مخرب یا سالم استفاده می‌شوند، در حالی که الگوریتم‌های نظارت‌نشده[4] برای شناسایی انحرافات از رفتار نرمال[5] به کار می‌روند. یادگیری عمیق، با استفاده از شبکه‌های عصبی چندلایه، قادر به تحلیل داده‌های پیچیده و غیرخطی است که برای شناسایی بدافزارهای مبتنی بر کد یا الگوهای پیچیده حمله بسیار کارآمد است. همچنین، پردازش زبان طبیعی برای تحلیل محتوا، شناسایی حملات مهندسی اجتماعی از طریق ایمیل‌های فیشینگ و بررسی متون گزارش‌های امنیتی استفاده می‌شود. یک مفهوم کلیدی دیگر در این حوزه، امنیت شناختی[6] است که بر ادغام بینش‌های انسانی و توانایی‌های ماشین برای تصمیم‌گیری سریع‌تر و دقیق‌تر تمرکز دارد. در این پارادایم، هوش مصنوعی نه به عنوان جایگزین انسان، بلکه به عنوان یک دستیار هوشمند عمل می‌کند که بار کاری تیم‌های امنیتی را کاهش داده و تمرکز آن‌ها را بر روی تهدیدات پیچیده‌تر ممکن می‌سازد. هوش مصنوعی مجموعه‌ای از روش‌ها و الگوریتم‌هاست که به سیستم‌ها امکان می‌دهد از داده‌ها یاد بگیرند، الگوها را تشخیص دهند و تصمیم‌گیری کنند. در حوزه امنیت، فناوری‌هایی مانند یادگیری ماشین و یادگیری عمیق بیشترین کاربرد را دارند. این روش‌ها می‌توانند رفتار عادی سیستم را مدل‌سازی کنند و در صورت مشاهده انحراف از الگوی معمول، آن را به‌عنوان تهدید احتمالی شناسایی نمایند. یکی از

[1] Machine Learning
[2] Deep Learning
[3] Supervised Learning
[4] Unsupervised Learning
[5] Anomaly Detection
[6] Cognitive Security

مهم‌ترین مزیت‌های این رویکرد، توانایی آن در تشخیص تهدیدات ناشناخته و حملات پیچیده است؛ تهدیداتی که در روش‌های مبتنی بر امضا معمولاً قابل شناسایی نیستند. به همین دلیل، AI در سال‌های اخیر به یکی از ارکان اصلی امنیت مدرن تبدیل شده است[۴].

استفاده از هوش مصنوعی در امنیت مزایای قابل توجهی دارد. نخست اینکه این فناوری قادر است حجم عظیمی از داده‌ها را در زمان کوتاه تحلیل کند و تهدیدات را سریع‌تر از روش‌های انسانی شناسایی نماید. دوم اینکه AI می‌تواند الگوهای پنهان و پیچیده را کشف کند؛ الگوهایی که ممکن است از دید تحلیل‌گران انسانی پنهان بمانند. سوم، قابلیت یادگیری مداوم باعث می‌شود که دقت سیستم در طول زمان افزایش یابد. علاوه بر این، امکان خودکارسازی بخشی از فرایندهای پاسخ به حادثه وجود دارد که این امر موجب کاهش بار کاری تیم‌های امنیتی و افزایش سرعت واکنش می‌شود. در نتیجه، AI می‌تواند هم سطح امنیت را ارتقا دهد و هم هزینه‌های عملیاتی را کاهش دهد[۵].

۴ – کاربردهای هوش مصنوعی در صنایع مختلف

در صنایع تولیدی، هوش مصنوعی به پایش لحظه‌ای تجهیزات و فرایندها کمک می‌کند و می‌تواند نشانه‌های خرابی، دستکاری یا رفتار غیرعادی را شناسایی کند. این موضوع نه‌تنها امنیت را افزایش می‌دهد، بلکه بهره‌وری و تداوم تولید را نیز بهبود می‌بخشد[۶و۷].

- **صنعت مالی و بانکداری**

صنعت مالی یکی از پیشگامان استفاده از هوش مصنوعی در امنیت است. در این بخش، تمرکز اصلی بر روی تشخیص تقلب در تراکنش‌های مالی[۷] و شناسایی پولشویی (AML) است. سیستم‌های هوش مصنوعی با تحلیل رفتار لحظه‌ای کاربر، موقعیت جغرافیایی، مقدار تراکنش و الگوهای خرید، می‌توانند تراکنش‌های مشکوک را در کسری از ثانیه مسدود کنند. برخلاف روش‌های قانون‌محور سنتی که نرخ خطای مثبت بالا[۸] دارند و منجر به آزار مشتریان می‌شوند، مدل‌های یادگیری عمیق با یادگیری مداوم از رفتارهای جدید، دقت بسیار بالاتری دارند. علاوه بر این، هوش مصنوعی در امنیت هویت دیجیتال[۹] و احراز هویت بیومتریک (مانند تشخیص چهره و الگوی ضربان قلب از طریق وبکم) نقش مهمی ایفا می‌کند. در بازارهای مالی، سیستم‌های الگوریتمی با نظارت بر نوسانات بازار و شناسایی الگوهای معامله‌گری غیرعادی، از دستکاری بازار و حملات هکری به پلتفرم‌های معاملاتی جلوگیری می‌کنند.

- **صنعت بهداشت و درمان**

در صنعت بهداشت، داده‌های بیمارانی پرونده‌های الکترونیک سلامت (EHR) از حساس‌ترین داده‌ها محسوب می‌شوند. نشت این داده‌ها می‌تواند منجر به اختلاس هویت، بیمه یا حتی خطرات جانی شود. هوش مصنوعی در اینجا برای محافظت از حریم خصوصی داده‌ها و ایمن‌سازی شبکه‌های بیمارستانی استفاده می‌شود. تکنیک‌هایی مانند یادگیری فدرال[۱۰] اجازه می‌دهند تا مدل‌های هوش مصنوعی بدون انتقال داده‌های خام بیمار به سرورهای مرکزی، آموزش ببینند و thus حریم خصوصی را حفظ کنند. همچنین، سیستم‌های تشخیص نفوذ مبتنی بر هوش مصنوعی با تحلیل ترافیک شبکه تجهیزات پزشکی متصل به اینترنت (IoMT)، از دسترسی غیرمجاز به دستگاه‌های حیاتی مانند پمپ‌های انسولین یا دستگاه‌های ضربان‌ساز قلب جلوگیری می‌کنند. شناسایی زودهنگام حملات ansomware که می‌تواند خدمات درمانی را فلج کند، از دیگر کاربردهای حیاتی این فناوری در این صنعت است.

- **صنعت انرژی و زیرساخت‌های حیاتی**

زیرساخت‌های انرژی، از جمله نیروگاه‌ها و شبکه‌های توزیع برق، اهداف اصلی حملات سایبری پیشرفته (APT) هستند. هوش مصنوعی در این بخش برای نظارت بر سیستم‌های کنترل صنعتی (ICS) و سیستم‌های کنترل نظارتی و جمع‌آوری داده (SCADA) استفاده می‌شود. این سیستم‌ها با پایش مداوم پارامترهای فیزیکی و دیجیتال، هرگونه انحراف غیرعادی را که می‌تواند نشانه‌ای از تلاش برای دستکاری فرآیندها باشد، شناسایی می‌کنند. برای مثال، تغییر ناگهانی در فشار لوله‌ها یا ولتاژ شبکه که با الگوهای طبیعی همخوانی ندارد، توسط الگوریتم‌های یادگیری

[7] Fraud Detection
[8] False Positive
[9] Digital Identity
[10] Federated Learning

ماشین به عنوان یک تهدید بالقوه طبقه‌بندی می‌شود. علاوه بر این، هوش مصنوعی در مدیریت ریسک زنجیره تأمین انرژی و شناسایی آسیب‌پذیری‌های نرم‌افزاری در تجهیزات قدیمی صنعتی نقش کلیدی دارد.

- **صنعت تولید و زنجیره تأمین**

در صنایع تولیدی، مالکیت فکری و نقشه‌های صنعتی ارزشمندترین دارایی‌ها هستند. هوش مصنوعی با استفاده از تکنیک‌های شناسایی ناهنجاری در دسترسی به فایل‌ها و شبکه‌های داخلی، از سرقت داده‌های حساس جلوگیری می‌کند. سیستم‌های کنترل دسترسی مبتنی بر هوش مصنوعی[11] رفتار کارکنان را تحلیل می‌کنند و اگر کارمندی شروع به دانلود حجم زیادی از فایل‌های محرمانه در ساعات غیرمجاز کند، دسترسی او را به صورت خودکار قطع می‌کند. همچنین، در زنجیره تأمین، هوش مصنوعی با تحلیل داده‌های از منابع متعدد، ریسک‌های امنیتی مرتبط با تامین‌کنندگان ثالث را ارزیابی کرده و از طریق‌های نفوذ احتمالی در زنجیره تأمین را شناسایی می‌کند.

۵ – چالش‌ها و تهدیدات نوظهور

با وجود مزایای فراوان، استفاده از هوش مصنوعی در امنیت بدون چالش نیست[۸و۹].

- **حملات خصمانه[12]**

یکی از بزرگترین چالش‌های هوش مصنوعی در امنیت، حملات خصمانه است. مهاجمان با ایجاد ورودی‌های خاص و دستکاری شده (مانند تصاویری که با چشم انسان عادی به نظر سالم می‌رسند اما مدل‌های بینایی ماشین را گمراه می‌کنند)، می‌توانند سیستم‌های تشخیص نفوذ مبتنی بر هوش مصنوعی را فریب دهند. این حملات می‌توانند منجر به رد مثبت کاذب (مشخص کردن ترافیک مخرب به عنوان سالم) یا رد منفی کاذب (نادیده گرفتن ترافیک مخرب) شوند. مقابله با این حملات نیازمند توسعه مدل‌های مقاوم[13] و استفاده از تکنیک‌های آموزشی است که در آن مدل‌ها همزمان با داده‌های واقعی و داده‌های مصنوعی تولید شده توسط مهاجمان آموزش می‌بینند.

- **حریم خصوصی و حریم داده‌ها**

استفاده از هوش مصنوعی نیازمند حجم عظیمی از داده‌هاست که این امر نگرانی‌های جدی درباره حریم خصوصی ایجاد می‌کند. جمع‌آوری داده‌های رفتاری کاربران برای آموزش مدل‌های تشخیص ناهنجاری ممکن است با قوانین حفاظت از داده‌ها مانند GDPR مغایرت داشته باشد. علاوه بر این، اگر مدل‌های آموزش دیده به درستی محافظت نشوند، مهاجمان ممکن است با حمله عضویت[14] به اطلاعات حسیمی از داده‌های آموزشی دسترسی پیدا کنند. بنابراین، پیاده‌سازی اصول «حریم خصوصی از طریق طراحی[15] و استفاده از تکنیک‌هایی مانند همسان‌سازی داده‌ها[16] و رمزنگاری هم‌تراز[17] ضروری است.

- **جعبه سیاه و قابل تفسیر نبودن مدل‌ها**

بسیاری از مدل‌های پیشرفته یادگیری عمیق به عنوان «جعبه سیاه» عمل می‌کنند، به این معنی که فرآیند تصمیم‌گیری آن‌ها برای انسان قابل درک نیست. در محیط‌های امنیتی که نیاز به پاسخگویی و توضیح اقدامات (مانند مسدود کردن یک IP یا بستن یک حساب کاربری) وجود دارد، عدم قابلیت تفسیرپذیری[18] یک مشکل بزرگ است. اگر یک سیستم هوش مصنوعی اشتباهاً یک کاربر قانونی را به عنوان تهدید شناسایی کند، تیم‌های امنیتی باید بتوانند دلیل این تصمیم را سریعاً بررسی و رفع کنند. توسعه مدل‌های هوش مصنوعی قابل تفسیر (XAI) برای رفع این چالش ضروری است.

- **کمبود نیروی انسانی متخصص**

با وجود پتانسیل بالای هوش مصنوعی، کمبود متخصصانی که هم دانش عمیقی در حوزه امنیت سایبری و هم درک قوی از الگوریتم‌های هوش

[11] UBA - User Behavior Analytics
[12] Adversarial Attacks
[13] Robust Models
[14] Membership Inference Attack
[15] Privacy by Design
[16] Data Anonymization
[17] Homomorphic Encryption
[18] Explainability

مصنوعی داشته باشند، یک مانع بزرگ است. این شکاف مهارتی منجر به پیاده‌سازی نادرست یا غیربهینه سیستم‌های مبتنی بر هوش مصنوعی می‌شود که ممکن است به جای افزایش امنیت، آسیب‌پذیری‌های جدیدی ایجاد کند.

۶ – راهکارها و بهترین شیوه‌های پیاده‌سازی

برای بهره‌برداری مؤثر از هوش مصنوعی در امنیت اطلاعات، سازمان‌ها باید رویکردی چندلایه و استراتژیک اتخاذ کنند[۱۰].

اولاً، ادغام هوش مصنوعی باید با استراتژی کلی امنیت سایبری سازمان همسو باشد. هوش مصنوعی نباید به عنوان یک محصول جادویی مستقل خریداری شود، بلکه باید بخشی از یک اکوسیستم امنیتی یکپارچه[۱۹] باشد که در آن داده‌ها از منابع مختلف جمع‌آوری و تحلیل می‌شوند.

ثانیاً، استفاده از رویکردهای ترکیبی[۲۰] توصیه می‌شود. ترکیب هوش مصنوعی با دانش کارشناسان انسانی[۲۱] می‌تواند دقت سیستم را افزایش دهد. در این مدل، هوش مصنوعی هشدارهای اولیه را تولید کرده و کارشناسان انسانی آن‌ها را بررسی و اعتبارسنجی می‌کنند. این بازخورد انسانی سپس به مدل بازگردانده می‌شود تا مدل در آینده دقیق‌تر عمل کند.

ثالثاً، تمرکز بر امنیت خود هوش مصنوعی[۲۲] حیاتی است. سازمان‌ها باید اطمینان حاصل کنند که مدل‌های هوش مصنوعی خود در برابر دستکاری، تزریق داده و دسترسی غیرمجاز محافظت شده‌اند. این شامل رمزنگاری داده‌های آموزشی، نظارت بر سلامت مدل در طول زمان[۲۳] و اجرای کنترل‌های دسترسی دقیق به زیرساخت‌های هوش مصنوعی است.

رابعاً، سرمایه‌گذاری در آموزش و توسعه مهارت‌های نیروی انسانی ضروری است. کارشناسان امنیت باید با مفاهیم پایه‌ای هوش مصنوعی آشنا شوند تا بتوانند با سیستم‌ها تعامل مؤثر داشته باشند و نتایج آن‌ها را به درستی تفسیر کنند. همچنین، ایجاد فرهنگ سازمانی که در آن امنیت داده‌ها و استفاده مسئولانه از هوش مصنوعی ترویج شود، نقش مهمی در کاهش خطرات انسانی دارد.

۷ – بحث و تحلیل مقایسه‌ای

بررسی تطبیقی روش‌های سنتی و مبتنی بر هوش مصنوعی نشان می‌دهد که روش‌های سنتی در مقابله با تهدیدات شناخته شده کارایی دارند، اما در برابر تهدیدات ناشناخته یا بسیار کند واکنش نشان می‌دهند. در مقابل، روش‌های مبتنی بر هوش مصنوعی در شناسایی الگوهای جدید و پیچیده برتری دارند، اما نیازمند داده‌های باکیفیت و زیرساخت محاسباتی قوی هستند. هزینه‌های اولیه پیاده‌سازی سیستم‌های هوش مصنوعی بالا است، اما بازگشت سرمایه (ROI) از طریق کاهش خسارات ناشی از نقض داده‌ها و کاهش زمان توقف عملیات[۲۴] در بلندمدت بسیار قابل توجه است. همچنین، باید توجه داشت که هوش مصنوعی یک جابجایی در تعادل قدرت سایبری ایجاد کرده است. هم مدافعان و هم مهاجمان از این فناوری استفاده می‌کنند. مهاجمان از هوش مصنوعی برای تولید بدافزارهای پیشرفته، هدف‌گیری دقیق‌تر و خودکارسازی حملات استفاده می‌کنند. بنابراین، دفاع صرفاً کافی نیست؛ بلکه نیاز به یک روی فعال[۲۵] و پیش‌دستانه وجود دارد. این رویکرد شامل جستجوی فعال تهدیدات[۲۶] با کمک هوش مصنوعی، به اشتراک‌گذاری اطلاعات تهدیدات بین صنایع (ISACs) و استفاده از مدل‌های تهدید[۲۷] پیشرفته است.

۸ – نتیجه‌گیری و پیشنهادات آتی

هوش مصنوعی نقش غیرقابل انکاری در تحول امنیت سایبری و حفظ امنیت اطلاعات در صنایع مختلف ایفا می‌کند. این فناوری با ارائه بینش‌های بلادرنگ، خودکارسازی پاسخ به تهدیدات و توانایی مقابله با حجم عظیم داده‌ها، سطح امنیت را به مرحله‌ای فراتر از توانایی روش‌های سنتی ارتقا می‌دهد. با این حال، هوش مصنوعی یک راه‌حل جامع نیست

[19] Security Operations Center - SOC
[20] Hybrid Approaches
[21] Human-in-the-Loop
[22] Securing AI
[23] Model Drift Detection
[24] Downtime
[25] Proactive
[26] Threat Hunting
[27] Threat Modeling

و چالش‌هایی نظیر حملات خصمانه، حریم خصوصی و نیاز به تفسیرپذیری همچنان پابرجاست. بنابراین بررسی‌ها نشان می‌دهد که هوش مصنوعی می‌تواند به‌عنوان یک ابزار راهبردی در حفظ امنیت صنایع مختلف مورد استفاده قرار گیرد. توانایی آن در تحلیل سریع، تشخیص تهدیدات ناشناخته و پشتیبانی از تصمیم‌گیری امنیتی، این فناوری را به یکی از ارکان اصلی امنیت آینده تبدیل کرده است. با این حال، بهره‌برداری موفق از AI مستلزم توجه هم‌زمان به داده‌های باکیفیت، طراحی امن مدل‌ها، نظارت انسانی و سیاست‌گذاری مناسب است. بنابراین، آینده امنیت صنعتی نه در حذف انسان، بلکه در همکاری هوشمندانه میان انسان و هوش مصنوعی شکل خواهد گرفت. این همکاری می‌تواند زمینه‌ساز سامانه‌هایی ایمن‌تر، هوشمندتر و مقاوم‌تر در برابر تهدیدات نوظهور باشد.

پیشنهاد می‌شود سازمان‌ها برای بهره‌برداری حداکثری از پتانسیل‌های هوش مصنوعی، گام‌های زیر را بردارند:

۱) تدوین چارچوب‌های اخلاقی و امنیتی مشخص برای توسعه و استقرار مدل‌های هوش مصنوعی.
۲) سرمایه‌گذاری در زیرساخت‌های داده‌ای باکیفیت و یکپارچه برای آموزش مدل‌های دقیق‌تر.
۳) تقویت همکاری بین بخش‌های فناوری اطلاعات، امنیت سایبری و واحدهای کسب‌وکار برای درک بهتر نیازهای امنیتی.
۴) مشارکت در اکوسیستم‌های به اشتراک‌گذاری اطلاعات تهدیدات برای بهبود مدل‌های تشخیصی مبتنی بر داده‌های جمعی.
۵) انجام ارزیابی‌های منظم امنیتی بر روی خود سیستم‌های هوش مصنوعی برای شناسایی و رفع آسیب‌پذیری‌های آن‌ها.

در نهایت، آینده امنیت اطلاعات در گرو تعادل هوشمندانه بین توانایی‌های ماشین و قضاوت انسانی است. هوش مصنوعی باید به عنوان ابزاری برای توانمندسازی انسان‌ها و نه جایگزین آن‌ها دیده شود تا بتوان در برابر تهدیدات سایبری نوظهور و پیچیده مقاومت پایدار ایجاد کرد.

مراجع

[1] Singh, S., Karimipour, H., HaddadPajouh, H., & Dehghantanha, A. (2020). Artificial intelligence and security of industrial control systems. *Handbook of Big Data Privacy*, 121-164.

[2] Naqvi, S. G., Sheraz, S., Mehmood, I., & Yasin, M. (2023). Cyber-physical systems and artificial intelligence: the role of cyber security, machine learning, threats and benefits to modern economies and industries. *Pakistan Journal of Humanities and Social Sciences*, *11*(2), 1475-1484.

[3] Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial intelligence review*, *54*(5), 3849-3886.

[4] Nair, M. M., Deshmukh, A., & Tyagi, A. K. (2024). Artificial intelligence for cyber security: Current trends and future challenges. *Automated secure computing for next-generation systems*, 83-114.

[5] Waqas, M., Tu, S., Halim, Z., Rehman, S. U., Abbas, G., & Abbas, Z. H. (2022). The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. *Artificial Intelligence Review*, *55*(7), 5215-5261.

[6] Neoaz, N. (2024). Role of artificial intelligence in enhancing information assurance. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(5), 749-758.

[7] Гаврилюк, О., Якушев, О., Петченко, М., Зачосова, Н., Бєлялов, Т., & Козловська, С. (2023). Cyber security and artificial intelligence in the context of ensuring business security in wartime. *Financial and credit activity problems of theory and practice*, *6*(53), 451-459.

[8] Li, J., & Wang, T. (2021, August). Research on the application of artificial intelligence technology in intelligent operation and maintenance of industrial equipment and system. In *Journal of Physics: Conference Series* (Vol. 1992, No. 3, p. 032090). IOP Publishing.

[9] Jagatheesaperumal, S. K., Rahouti, M., Ahmad, K., Al-Fuqaha, A., & Guizani, M. (2021). The duo of artificial intelligence and big data for industry 4.0: Applications, techniques, challenges, and future research directions. *IEEE Internet of Things Journal*, *9*(15), 12861-12885.

[10] Rane, N. (2023). Role of ChatGPT and similar generative artificial intelligence (AI) in construction industry. *Available at SSRN 4598258*.