عنوان مقاله : نقش هوش مصنوعی در تقویت دفاع سایبری: شبیه‌سازی تهدیدات و راهکارهای پیشرفته شناسایی

نویسنده : امیرمسعود صادقیان

وابستگی سازمانی نویسنده : دانشگاه پیام نور

چکیده

امروزه تهدیدات سایبری یکی از بزرگ‌ترین چالش‌ها در دنیای دیجیتال به شمار می‌روند و سیستم‌های سنتی امنیتی قادر به مقابله کامل با تهدیدات پیچیده و نوظهور نیستند. به همین دلیل، استفاده از هوش مصنوعی (AI) در امنیت سایبری به عنوان یک راه‌حل نوین در حال گسترش است. این مقاله به بررسی کاربردهای هوش مصنوعی در شناسایی و مقابله با تهدیدات سایبری، از جمله تهدیدات ناشناخته(Zero-Day Threats) ، نفوذهای شبکه‌ای و حملات فیشینگ می‌پردازد. همچنین، چالش‌ها و محدودیت‌های استفاده از این فناوری در مقابله با تهدیدات پیچیده بررسی می‌شود. نتایج تحقیق نشان می‌دهند که هوش مصنوعی می‌تواند در شناسایی تهدیدات به طور قابل توجهی مؤثر باشد، اما نیاز به داده‌های با کیفیت، هزینه‌های بالا و تخصص فنی از جمله محدودیت‌های مهم این فناوری هستند. در نهایت، پیشنهاداتی برای بهبود امنیت سایبری با استفاده از هوش مصنوعی ارائه می‌شود.

واژگان کلیدی: هوش مصنوعی، امنیت سایبری، یادگیری ماشین، تهدیدات سایبری، شناسایی نفوذ

مقدمه

امنیت سایبری به عنوان یکی از ارکان اساسی در دنیای دیجیتال امروز شناخته می‌شود و تهدیدات سایبری در سال‌های اخیر پیچیده‌تر و گسترده‌تر شده‌اند. در این میان، استفاده از هوش مصنوعی به عنوان یک راهکار پیشرفته در مقابله با تهدیدات سایبری مطرح شده است. هوش مصنوعی، به ویژه یادگیری ماشین و یادگیری عمیق، می‌تواند به سیستم‌ها کمک کند تا تهدیدات جدید و ناشناخته را شناسایی کرده و از شبکه‌ها و داده‌ها محافظت کنند. در این مقاله، به بررسی روش‌های مختلف استفاده از هوش مصنوعی در امنیت سایبری، کاربردهای آن، و چالش‌های پیش روی این فناوری پرداخته می‌شود.

روش‌های استفاده از هوش مصنوعی در امنیت سایبری

۱ .شناسایی تهدیدات ناشناخته (Zero-Day Threats)

تهدیدات روز صفر (Zero-Day Threats) به تهدیداتی گفته می‌شود که پیش از شناسایی و ایجاد راه‌حل‌های مقابله، به سیستم وارد می‌شوند. این حملات می‌توانند از نقص‌های امنیتی ناشناخته‌ای بهره‌برداری کنند که هیچ سیستم یا نرم‌افزاری هنوز از آن آگاه نیست. در اینجا هوش مصنوعی نقش بسیار مهمی ایفا می‌کند. سیستم‌های مبتنی بر هوش مصنوعی، به‌ویژه الگوریتم‌های یادگیری ماشین و یادگیری عمیق، قادر به شبیه‌سازی و پیش‌بینی تهدیدات جدید و ناشناخته هستند. این سیستم‌ها به‌طور مداوم از داده‌های تاریخی و الگوهای موجود در ترافیک شبکه برای شناسایی رفتارهای غیرمعمول و تهدیدات روز صفر استفاده می‌کنند. به این ترتیب، هوش مصنوعی می‌تواند حملاتی که هنوز به‌طور عمومی شناخته نشده‌اند را پیش‌بینی و شبیه‌سازی کرده و قبل از وقوع واقعی آن‌ها اقدامات حفاظتی را پیشنهاد دهد.

۲ .تشخیص نفوذ و دفاع خودکار

سیستم‌های تشخیص نفوذ (IDS) مبتنی بر هوش مصنوعی به‌طور پیوسته و به صورت بلادرنگ، ترافیک شبکه و فعالیت‌های سیستم را بررسی کرده و حملات یا نفوذهای احتمالی را شبیه‌سازی می‌کنند. این سیستم‌ها از یادگیری ماشینی برای یادگیری الگوهای عادی و غیرعادی در ترافیک شبکه استفاده می‌کنند. هرگونه انحراف از این الگوها می‌تواند به عنوان یک تهدید یا حمله شبیه‌سازی و شناسایی شود. در صورت شناسایی تهدید، این سیستم‌ها قادر به انجام واکنش‌های خودکار برای جلوگیری از نفوذ یا کاهش آسیب‌ها هستند، مانند قطع دسترسی مهاجم یا فیلتر کردن بسته‌های مشکوک. استفاده از هوش مصنوعی در این سیستم‌ها باعث می‌شود که تهدیدات پیچیده و ناشناخته نیز به‌سرعت شناسایی و مهار شوند

۳ .پیش‌بینی حملات و جلوگیری از آسیب‌ها

یکی دیگر از کاربردهای هوش مصنوعی در امنیت سایبری، پیش‌بینی حملات سایبری است. با تحلیل داده‌های ترافیک شبکه، رفتار کاربران و الگوهای معمول در سیستم، هوش مصنوعی می‌تواند حملات احتمالی را شبیه‌سازی کرده و پیش‌بینی‌هایی دقیق از تهدیدات آتی ارائه دهد. به‌این‌ترتیب، سازمان‌ها قادر خواهند بود قبل از وقوع حمله واقعی، اقدامات پیشگیرانه انجام دهند و از بروز آسیب‌های مالی یا اطلاعاتی جلوگیری کنند. این پیش‌بینی‌ها به‌ویژه در تشخیص حملات DDoS (حمله انکار سرویس توزیع‌شده) و حملات ویروس‌ها و بدافزارها بسیار مفید است.

۴ .شناسایی حملات فیشینگ

حملات فیشینگ یکی از رایج‌ترین روش‌های حمله در دنیای دیجیتال هستند که از طریق ایمیل‌ها یا پیام‌های جعلی تلاش دارند تا اطلاعات حساس کاربران مانند نام کاربری، کلمه عبور یا اطلاعات بانکی را به‌دست آورند. هوش مصنوعی با استفاده از تکنیک‌های یادگیری ماشین می‌تواند به شناسایی این حملات بپردازد. این سیستم‌ها از الگوریتم‌های پردازش زبان طبیعی (NLP) برای تحلیل محتوا و شبیه‌سازی ویژگی‌های پیام‌ها استفاده می‌کنند تا ایمیل‌ها یا پیام‌های مشکوک را شناسایی کنند. علاوه بر این، هوش مصنوعی می‌تواند با تحلیل الگوهای رفتاری کاربران در محیط‌های آنلاین، به شناسایی و مسدودسازی حملات فیشینگ قبل از وقوع آن‌ها بپردازد.

۵ .تحلیل رفتار کاربران و شناسایی فعالیت‌های مشکوک

هوش مصنوعی به ویژه در تحلیل رفتار کاربران و شناسایی فعالیت‌های مشکوک می‌تواند به شدت مفید باشد. سیستم‌های مبتنی بر هوش مصنوعی از الگوریتم‌های یادگیری ماشین برای تجزیه و تحلیل الگوهای رفتاری کاربران در سیستم‌های مختلف (مانند شبکه‌های اجتماعی، وب‌سایت‌ها و سیستم‌های داخلی سازمان) استفاده می‌کنند. این سیستم‌ها به‌طور مداوم رفتارهای کاربران را پایش می‌کنند و هرگونه انحراف از الگوهای عادی، مانند دسترسی به منابع حساس یا ورود به سیستم از موقعیت‌های جغرافیایی غیرمعمول، را شناسایی می‌کنند. این نوع از تحلیل می‌تواند به شناسایی حملات داخلی (مانند حملات توسط کارکنان سازمان) یا دسترسی‌های غیرمجاز کمک کند.

۶ .دفاع در برابر بدافزارها (Malware) و ویروس‌ها

یکی دیگر از کاربردهای هوش مصنوعی در امنیت سایبری، مقابله با بدافزارها و ویروس‌ها است. سیستم‌های AI می‌توانند با استفاده از تحلیل رفتار و ویژگی‌های اجرایی فایل‌ها و برنامه‌ها، به شناسایی بدافزارهایی بپردازند که قادر به تغییر شکل یا پنهان شدن در سیستم‌ها هستند. این سیستم‌ها می‌توانند به صورت بلادرنگ فعالیت‌های مشکوک را شبیه‌سازی و شناسایی کرده و با ارائه واکنش‌های فوری (مانند قرنطینه فایل‌های آلوده یا توقف برنامه‌های مشکوک) از گسترش بدافزار جلوگیری کنند.

۷ .بررسی و تحلیل امنیت در محیط‌های ابری(Cloud Security)

با گسترش استفاده از فضای ابری برای ذخیره‌سازی و پردازش داده‌ها، امنیت این محیط‌ها نیز تبدیل به یک چالش اساسی شده است. هوش مصنوعی می‌تواند با بررسی الگوهای دسترسی، ترافیک شبکه و رفتار کاربران در محیط‌های ابری، تهدیدات امنیتی مانند دسترسی‌های غیرمجاز یا حملات توزیع‌شده به سرویس‌ها (DDoS) را شبیه‌سازی و شناسایی کند. علاوه بر این، هوش مصنوعی می‌تواند به طور مداوم امنیت محیط‌های ابری را بررسی کرده و نقاط ضعف احتمالی را شناسایی کرده و اقدامات پیشگیرانه پیشنهاد دهد.

۸ .مدیریت و پاسخ به تهدیدات (Threat Hunting)

هوش مصنوعی می‌تواند در فرآیند تهدیدیابی (Threat Hunting) به کار رود. در این فرآیند، تیم‌های امنیتی به طور فعال به دنبال تهدیدات پنهان و حملات احتمالی در شبکه می‌گردند. هوش مصنوعی با تجزیه و تحلیل حجم عظیم داده‌های شبکه، می‌تواند به شناسایی ناهنجاری‌ها و الگوهای مشکوک که احتمالاً نشان‌دهنده حملات در حال وقوع هستند، کمک کند. این سیستم‌ها می‌توانند به شناسایی حملات پیچیده و پیشرفته مانند Advanced Persistent Threats (APT) کمک کنند که ممکن است برای مدت طولانی در شبکه باقی بمانند.

۹ .تقویت امنیت در زمان‌های بحران (Incident Response)

در زمان بروز بحران‌های امنیتی مانند حملات سایبری یا نفوذهای شبکه، هوش مصنوعی می‌تواند به تیم‌های امنیتی کمک کند تا واکنش سریع و مؤثری داشته باشند. سیستم‌های مبتنی بر هوش مصنوعی قادرند به طور خودکار شواهد حمله را جمع‌آوری و تحلیل کنند و به

شناسایی مسیر نفوذ و نحوه انجام حمله بپردازند. این اطلاعات به تیم‌های امنیتی کمک می‌کند تا تصمیمات بهتری بگیرند و اقدامات فوری برای جلوگیری از گسترش حمله انجام دهند.

۱۰ .مدیریت آسیب‌پذیری‌ها (Vulnerability Management)

هوش مصنوعی می‌تواند در شناسایی و مدیریت آسیب‌پذیری‌های نرم‌افزارها و سیستم‌ها به کار رود. این سیستم‌ها می‌توانند به طور خودکار آسیب‌پذیری‌های شناخته‌شده در نرم‌افزارها را شناسایی کرده و به سازمان‌ها پیشنهاد دهند که اصلاحات امنیتی (پچ‌ها) را به سرعت پیاده‌سازی کنند. هوش مصنوعی همچنین می‌تواند به تحلیل الگوهای حملات علیه آسیب‌پذیری‌ها و پیش‌بینی تهدیدات احتمالی بپردازد، تا اقدامات پیشگیرانه به‌موقع انجام گیرد.

چالش‌ها و محدودیت‌ها در استفاده از هوش مصنوعی در امنیت سایبری

۱ .نیاز به داده‌های با کیفیت

یکی از بزرگ‌ترین چالش‌ها در استفاده از هوش مصنوعی در امنیت سایبری، نیاز به داده‌های با کیفیت بالا است. الگوریتم‌های هوش مصنوعی به داده‌های دقیق و جامع برای شبیه‌سازی تهدیدات و شناسایی حملات نیاز دارند. داده‌های ناقص یا نادرست می‌تواند دقت سیستم‌ها را کاهش دهد و منجر به شناسایی نادرست تهدیدات یا هشدارهای کاذب شود. همچنین، حجم بالای داده‌ها ممکن است باعث بروز مشکلاتی در پردازش و تحلیل شود، که به نوبه خود عملکرد سیستم‌های AI را تحت تأثیر قرار خواهد داد.

۲ .حملات به سیستم‌های هوش مصنوعی

سیستم‌های هوش مصنوعی خود نیز در معرض حملات قرار دارند. مهاجمان ممکن است تلاش کنند تا با حملات تزریقی داده (Data Injection) یا تغییر در داده‌های آموزشی مدل‌های هوش مصنوعی، آن‌ها را فریب دهند. این حملات می‌توانند باعث شوند که مدل‌های هوش مصنوعی به اشتباه تهدیدات غیرموجود را شناسایی کنند یا تهدیدات واقعی را نادیده بگیرند. به همین دلیل، محافظت از سیستم‌های هوش مصنوعی در برابر حملات، به‌ویژه در حوزه امنیت سایبری، اهمیت زیادی دارد.

۳ .هزینه‌ها و پیچیدگی‌ها

پیاده‌سازی و نگهداری سیستم‌های هوش مصنوعی در زمینه امنیت سایبری، به دلیل نیاز به سخت‌افزار قوی، نرم‌افزارهای پیشرفته، و نیروی انسانی متخصص، ممکن است هزینه‌های بالایی به همراه داشته باشد. این هزینه‌ها می‌تواند برای بسیاری از سازمان‌ها، به‌ویژه کسب‌وکارهای کوچک و متوسط، چالشی جدی ایجاد کند. علاوه بر این، پیچیدگی‌های فنی در پیاده‌سازی این سیستم‌ها ممکن است نیاز به زمان و منابع قابل‌توجهی برای آموزش و پشتیبانی مستمر داشته باشد.

۴ .محدودیت‌های فنی و نیاز به تخصص

برای پیاده‌سازی و استفاده مؤثر از هوش مصنوعی در امنیت سایبری، نیاز به تخصص‌های فنی و کارشناسان با تجربه در حوزه‌های مختلف هوش مصنوعی، یادگیری ماشین و یادگیری عمیق وجود دارد. طراحی و نگهداری مدل‌های پیچیده AI برای شناسایی تهدیدات و تحلیل داده‌ها نیازمند دانش فنی بالا و توانایی حل مسائل پیچیده است. کمبود متخصصان این حوزه می‌تواند به عنوان یک مانع بزرگ در توسعه و پیاده‌سازی موفق این فناوری‌ها در بخش امنیت سایبری عمل کند.

۵ .هشدارهای کاذب (False Positives)

یکی از چالش‌های رایج در استفاده از هوش مصنوعی در امنیت سایبری، تعداد بالای هشدارهای کاذب است. سیستم‌های هوش مصنوعی ممکن است رفتارهای غیرمعمول را شبیه به تهدیدات امنیتی شبیه‌سازی کرده و هشدارهای نادرستی ایجاد کنند. این امر می‌تواند باعث شود که کارشناسان امنیتی زمان زیادی را صرف بررسی هشدارهای بی‌اهمیت کنند و از شناسایی تهدیدات واقعی غافل شوند. بهبود دقت الگوریتم‌ها برای کاهش هشدارهای کاذب یک چالش بزرگ است.

۶ .دستکاری مدل‌های هوش مصنوعی

حملات به سیستم‌های هوش مصنوعی از طریق تکنیک‌هایی مانند حملات تزریقی داده (Data Poisoning) یا حملات تغییر ویژگی‌ها (Feature Manipulation) می‌تواند مدل‌های هوش مصنوعی را فریب دهد. این نوع حملات می‌توانند منجر به اشتباهات جدی در شناسایی تهدیدات و در نتیجه از دست دادن امنیت سیستم شوند. مقابله با این حملات و طراحی مدل‌های هوش مصنوعی مقاوم در برابر دستکاری‌ها نیازمند تلاش‌های مستمر است.

۷ .انتقال هوش مصنوعی به سیستم‌های جدید

پیاده‌سازی سیستم‌های هوش مصنوعی در امنیت سایبری باید به‌طور مستمر به‌روز و سازگار با تهدیدات جدید باشد. تهدیدات و تکنیک‌های حمله به سرعت تغییر می‌کنند و مدل‌های هوش مصنوعی باید قادر باشند که با این تغییرات سازگار شوند. به همین دلیل، به‌روزرسانی مداوم مدل‌ها و نگهداری از آن‌ها در برابر تهدیدات جدید از اهمیت بالایی برخوردار است.

در نهایت، استفاده از هوش مصنوعی در امنیت سایبری، اگرچه چالش‌هایی دارد، اما می‌تواند به‌طور قابل توجهی توانایی‌های دفاعی سازمان‌ها را تقویت کرده و از حملات پیچیده و نوظهور جلوگیری کند

پلتفرم‌های هوش مصنوعی در مبارزه با تهدیدات سابیری : کاربردها و مزایا

۱. Darktrace

Darktraceیکی از پیشرفته‌ترین سیستم‌های امنیت سایبری مبتنی بر هوش مصنوعی است که از الگوریتم‌های یادگیری ماشینی برای شناسایی تهدیدات و رفتارهای غیرعادی در شبکه‌ها، فضای ابری و سیستم‌های اینترنت اشیاء (IoT) استفاده می‌کند. این پلتفرم توانایی شناسایی تهدیدات سایبری به صورت خودکار و بدون نیاز به دخالت انسانی دارد. به‌طور خاص، Darktrace از مفهوم "هوش مصنوعی خودآموز" استفاده می‌کند که به این سیستم امکان می‌دهد رفتارهای طبیعی شبکه را بیاموزد و به محض شناسایی هرگونه انحراف از این رفتارها، اقدامات امنیتی لازم را انجام دهد. این فناوری به‌ویژه برای سازمان‌ها با حجم بالای داده‌ها و شبکه‌های پیچیده مفید است.

۲. CrowdStrike

CrowdStrike یکی از پیشرفته‌ترین پلتفرم‌های امنیتی سایبری است که از هوش مصنوعی و یادگیری ماشینی برای تشخیص، تجزیه‌وتحلیل و مقابله با تهدیدات سایبری استفاده می‌کند. این سیستم به‌ویژه در شناسایی و جلوگیری از حملات پیچیده و تهدیدات پیشرفته به خوبی عمل می‌کند CrowdStrike .یک راه‌حل "Endpoint Protection" ارائه می‌دهد که به‌صورت متمرکز تمامی

دستگاه‌ها و نقطه‌های ورودی به شبکه سازمان را تحت نظارت قرار می‌دهد. با استفاده از مدل‌های هوش مصنوعی، این پلتفرم می‌تواند الگوهای حملات سایبری را شبیه‌سازی و شناسایی کند و با استفاده از واکنش‌های خودکار، تهدیدات را در مراحل اولیه متوقف کند.

۳. IBM Watson for Cyber Security

IBM Watson for Cyber Security یکی از راه‌حل‌های برتر برای تحلیل تهدیدات سایبری است که با استفاده از قابلیت‌های هوش مصنوعی خود به شناسایی و تحلیل داده‌های امنیتی کمک می‌کند. این سیستم از الگوریتم‌های یادگیری ماشین برای تحلیل و پردازش داده‌های امنیتی در مقیاس‌های بزرگ استفاده می‌کند و می‌تواند تهدیدات را با سرعت بالا شناسایی کند .IBM Watson در واقع به تیم‌های امنیتی کمک می‌کند تا از طریق تحلیل‌های پیشرفته، تهدیدات پیچیده را شبیه‌سازی کنند و به آن‌ها اطلاعات دقیقی برای مقابله با حملات ارائه دهد. از دیگر ویژگی‌های این سیستم، توانایی پردازش زبان طبیعی است که امکان تعامل مستقیم با متخصصان امنیتی را فراهم می‌آورد.

۴. Vectra AI

Vectra AIیک پلتفرم پیشرفته امنیتی است که از هوش مصنوعی برای شناسایی و تحلیل تهدیدات سایبری در شبکه‌های پیچیده استفاده می‌کند. این سیستم به‌ویژه برای شناسایی حملات پیشرفته و تهدیدات ناشناخته کاربرد دارد Vectra AI .با استفاده از مدل‌های یادگیری ماشینی قادر است رفتارهای مخرب در شبکه را شبیه‌سازی و شناسایی کند و به تیم‌های امنیتی این امکان را می‌دهد که تهدیدات را در مراحل ابتدایی شناسایی و از گسترش آن‌ها جلوگیری کنند. این سیستم می‌تواند در محیط‌های ابری، دیتاسنترها و شبکه‌های سازمانی به‌طور مؤثر عمل کند.

۵. Fortinet

Fortinet یکی از برجسته‌ترین ارائه‌دهندگان راه‌حل‌های امنیت سایبری است که از هوش مصنوعی برای تشخیص تهدیدات و محافظت از شبکه‌های سازمانی استفاده می‌کند. Fortinet با استفاده از مدل‌های یادگیری ماشینی و تحلیل‌های رفتارشناسی، قادر است تهدیدات سایبری را در زمان واقعی شناسایی و مسدود کند. این سیستم به‌ویژه برای شبکه‌های بزرگ و پیچیده طراحی شده است و می‌تواند در مقیاس‌های گسترده به نظارت بر ترافیک شبکه، شناسایی حملات و جلوگیری از نفوذهای سایبری کمک کند. Fortinet همچنین با ارائه راه‌حل‌های امنیتی در سطح دستگاه‌ها (Endpoint)، شبکه‌ها و فضای ابری، امکان محافظت جامع از تمامی بخش‌های سازمان را فراهم می‌آورد.

روش تحقیق

این مقاله به روش تحقیق کیفی و تحلیلی پرداخته است و در آن، منابع مختلف علمی و تحقیقاتی در زمینه هوش مصنوعی و امنیت سایبری مورد بررسی قرار گرفته‌اند. همچنین، از تحلیل مقالات و کتاب‌های معتبر در این زمینه برای شناسایی کاربردها، مزایا و چالش‌های استفاده از AI در مقابله با تهدیدات سایبری بهره‌برداری شده است.

بحث و نتیجه‌گیری

استفاده از هوش مصنوعی در امنیت سایبری می‌تواند تغییرات چشمگیری در شناسایی تهدیدات و مقابله با آن‌ها ایجاد کند. روش‌هایی مانند شبیه‌سازی تهدیدات، پیش‌بینی حملات و دفاع خودکار از جمله قابلیت‌های منحصر به فرد AI در این حوزه هستند. با این حال،

چالش‌هایی همچون نیاز به داده‌های با کیفیت، حملات به سیستم‌های AI و هزینه‌های بالای پیاده‌سازی، همچنان بر سر راه این فناوری وجود دارند.

-تقویت دسترسی به داده‌های با کیفیت برای آموزش مدل‌های هوش مصنوعی

-افزایش سرمایه‌گذاری در تحقیق و توسعه سیستم‌های امنیتی مبتنی برAI

-برگزاری دوره‌های آموزشی برای متخصصان امنیت سایبری در زمینه هوش مصنوعی

-توسعه روش‌های دفاعی ترکیبی که از فناوری‌های سنتی و نوین به‌طور همزمان بهره‌برداری کنند

منابع

وب‌سایت رسمی Darktrace:
- لینک: [https://darktrace.com]
- توضیحات: اطلاعات مربوط به فناوری هوش مصنوعی و کاربردهای آن در امنیت سایبری.

وب‌سایت رسمی CrowdStrike:
- لینک: [https://www.crowdstrike.com]
- توضیحات: اطلاعات درباره پلتفرم‌های امنیتی مبتنی بر هوش مصنوعی و یادگیری ماشینی برای شناسایی و مقابله با تهدیدات سایبری.

وب‌سایت رسمی IBM(IBM Watson for Cyber Security) :
- لینک: [https://www.ibm.com/security]
- توضیحات: استفاده از تحلیل‌های مبتنی بر هوش مصنوعی برای شناسایی تهدیدات و حفاظت از اطلاعات.

وب‌سایت رسمی Vectra AI:
- لینک: [https://www.vectra.ai]
- توضیحات: پلتفرم امنیتی که با استفاده از هوش مصنوعی تهدیدات شبکه را شناسایی و تحلیل می‌کند.

وب‌سایت رسمی Fortinet:
- لینک: [https://www.fortinet.com]
- توضیحات: راهکارهای امنیت سایبری مبتنی بر هوش مصنوعی برای شناسایی تهدیدات و مدیریت امنیت در شبکه‌های بزرگ.

Amor, N. B., & Manogaran, G. (2020). *Artificial Intelligence and Machine Learning in Cybersecurity: Principles, Methods and Applications*. Elsevier.

Zhang, Y., & Lee, H. (2018). *Machine Learning for Cybersecurity: Applications, Challenges, and Opportunities*. Springer.

Chen, M., Mao, S., & Liu, Y. (2014). *Big Data: A Survey*. Mobile Networks and Applications, 19(2), 171-209.

Sommer, R., & Paxson, V. (2010). *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection*. IEEE Symposium on Security and Privacy.

Shu, Q., & Liao, X. (2021). *Artificial Intelligence in Cyber Security: A Survey of Techniques, Applications, and Future Directions*. Journal of Computer Science and Technology, 36(4), 757-788.

Buczak, A. L., & Guven, E. (2016). *A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection*. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

The Role of Artificial Intelligence in Strengthening Cyber Defense: Threat Simulation and Advanced Detection Solutions

First Author Name and Surname: Amir Masoud Sadeghian

Affiliation of the Author: Payame Noor University

Abstract

Today, cyber threats are considered one of the biggest challenges in the digital world, and traditional security systems are not capable of fully addressing complex and emerging threats. As a result, the use of Artificial Intelligence (AI) in cybersecurity is rapidly expanding as an innovative solution. This paper examines the applications of AI in identifying and mitigating cyber threats, including unknown threats (Zero-Day Threats), network intrusions, and phishing attacks. Additionally, the challenges and limitations of using this technology to counter complex threats are explored. The findings suggest that AI can be significantly effective in threat detection, but the need for high-quality data, high costs, and technical expertise are important limitations of this technology. Finally, suggestions for improving cybersecurity using AI are provided.

Keywords: Artificial Intelligence, Cybersecurity, Machine Learning, Cyber Threats, Intrusion Detection