نقش هوش مصنوعی در تقویت امنیت شبکه با رویکرد دفاع در عمق جهت شناسایی و پیشگیری از تهدیدات سایبری

نویسنده : عباس رضایی

رشته : کارشناسی مهندسی نرم افزار

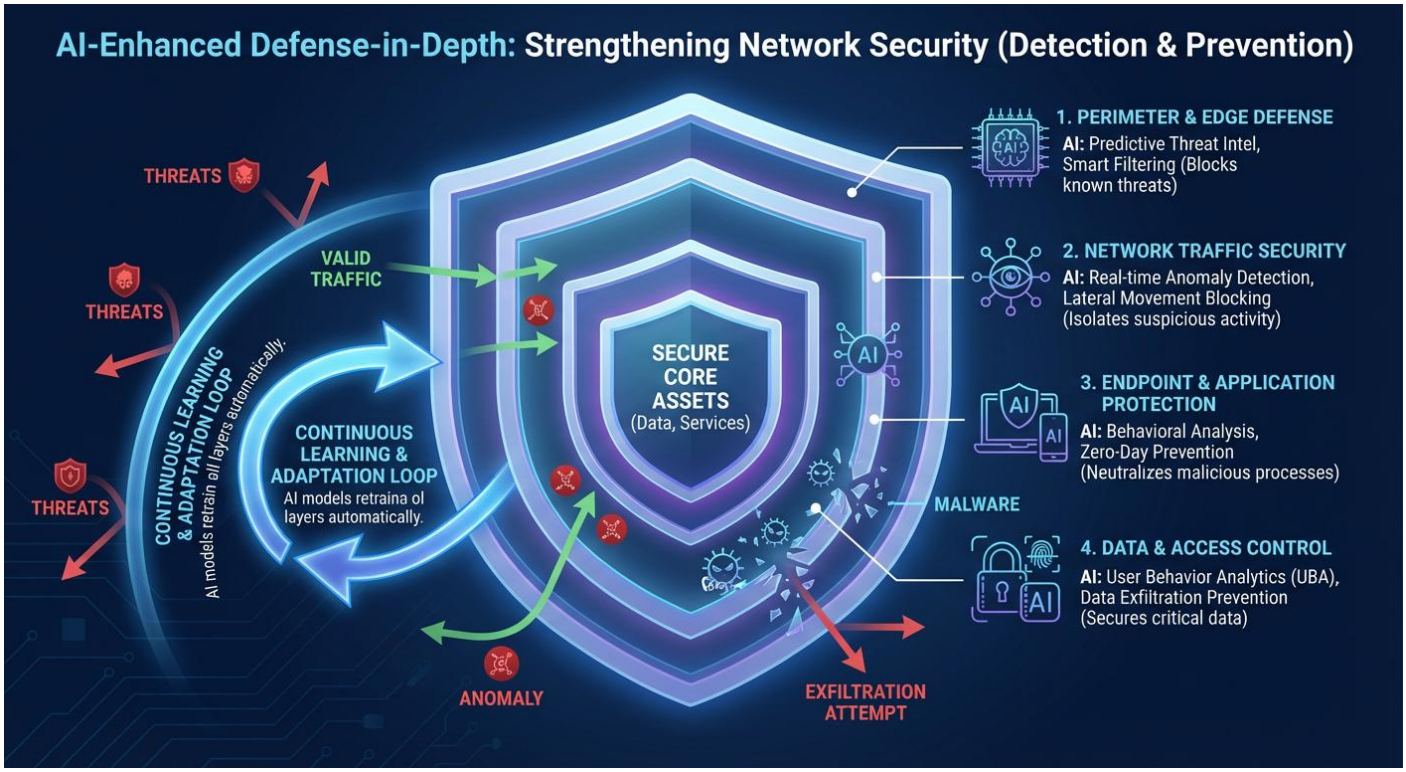
چکیده

با توسعه روزافزون فناوری های اطلاعاتی و گسترش استفاده از شبکه های کامپیوتری در سازمان ها، مسئله امنیت سایبری به یکی از چالش های اساسی دنیای دیجیتال تبدیل شده است.امروزه حجم، تنوع و پیچیدگی حملات سایبری به گونه ای افزایش یافته که روش های سنتی امنیت شبکه، که عمدتاً مبتنی بر قوانین ثابت و امضاهای از پیش تعریف شده هستند، دیگر پاسخگوی نیازهای امنیتی سازمان ها نیستند. تهدیداتی مانند بدافزارهای پیشرفته، حملات روز صفر، نفوذهای هدفمند و حملات مهندسی اجتماعی، نیاز به رویکردهای هوشمند و پویا را بیش از پیش نمایان کرده اند.

در این میان، رویکرد دفاع در عمق به عنوان یک استراتژی لایه ای، با ایجاد چندین سطح امنیتی، تلاش می کند احتمال نفوذ و خسارت را کاهش دهد. با این حال، پیشرفت تهدیدات سایبری نشان می دهد که این رویکرد نیز بدون استفاده از فناوری های نوین، کارایی لازم را نخواهد داشت. هوش مصنوعی با قابلیت هایی نظیر یادگیری ماشین، تحلیل رفتار، شناسایی الگوهای غیرعادی و واکنش خودکار، توانسته است نقش مهمی در تقویت دفاع در عمق ایفا کند.

این مقاله به بررسی نقش هوش مصنوعی در ارتقای امنیت شبکه مبتنی بر دفاع در عمق می پردازد و تمرکز آن بر سه لایه کلیدی امنیت مرزی، امنیت شبکه داخلی و تحلیل رفتار و پیش بینی تهدیدات است. نتایج بررسی ها

نشان می دهد که ترکیب هوش مصنوعی با دفاع در عمق می تواند امنیت شبکه را از حالت واکنشی به حالت پیشگیرانه و هوشمند تبدیل کند.



کلمات کلیدی

هوش مصنوعی، امنیت سایبری، دفاع در عمق، یادگیری ماشین، یادگیری عمیق، تحلیل رفتار شبکه، پیش بینی تهدیدات، امنیت شبکه

---

۱ .مقدمه

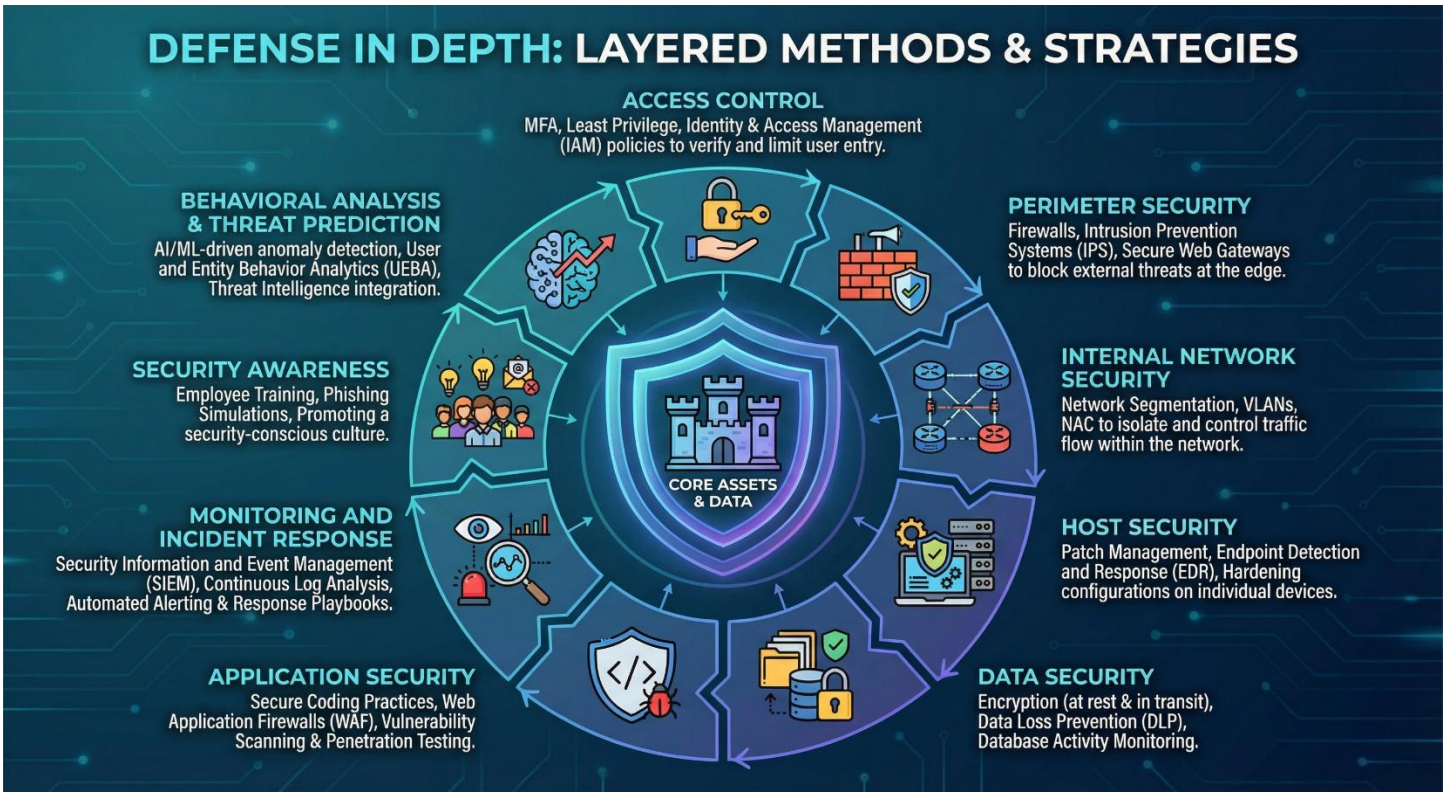
با رشد سریع فناوری اطلاعات و ارتباطات، شبکه های کامپیوتری به زیرساخت اصلی بسیاری از فعالیت های سازمانی، اقتصادی و حتی اجتماعی تبدیل شده اند. سازمان ها برای ذخیره، پردازش و انتقال اطلاعات حیاتی

خود به شدت به شبکه ها وابسته هستند. این وابستگی گسترده، در کنار مزایای فراوان، خطرات امنیتی متعددی را نیز به همراه داشته است.

در سال های اخیر، تهدیدات سایبری نه تنها از نظر تعداد، بلکه از نظر پیچیدگی نیز افزایش یافته اند. مهاجمان امروزی از تکنیک های پیشرفته ای مانند بدافزارهای هوشمند، حملات چند مرحله ای، تهدیدات مداوم پیشرفته و حملات روز صفر استفاده می کنند. این نوع حملات اغلب قادرند از سد سیستم های امنیتی سنتی عبور کرده و خسارات جبران ناپذیری به سازمان ها وارد کنند.

روش های سنتی امنیت شبکه، نظیر فایروال ها و سیستم های تشخیص نفوذ مبتنی بر امضا، معمولاً تنها قادر به شناسایی تهدیدات شناخته شده هستند و در برابر تهدیدات جدید عملکرد ضعیفی دارند. به همین دلیل، استفاده از رویکردهای چندلایه مانند دفاع در عمق به عنوان یک راهکار اساسی مطرح شده است.

دفاع در عمق با ایجاد لایه های متوالی امنیتی، تلاش می کند حتی در صورت نفوذ مهاجم از یک لایه، لایه های بعدی مانع پیشروی او شوند. با این حال، اثربخشی این رویکرد بدون بهره گیری از فناوری های هوشمند محدود خواهد بود. در این راستا، هوش مصنوعی با توانایی تحلیل داده های حجیم، یادگیری مداوم و تصمیم گیری خودکار، می تواند نقش کلیدی در ارتقای امنیت شبکه ایفا کند. هدف این مقاله بررسی این نقش و تأثیر آن در تقویت دفاع در عمق شبکه است.



---

۲ .امنیت مرزی (Perimeter Security)

امنیت مرزی یکی از اولین و مهم ترین لایه های دفاع در عمق در هر شبکه ای است. در این لایه، هدف اصلی این است که قبل از ورود هرگونه تهدید یا نفوذ به شبکه داخلی، آن را شناسایی و متوقف کنیم. روش های سنتی امنیت مرزی شامل فایروال ها، لیست های کنترل دسترسی و سیستم های تشخیص نفوذ بوده اند، اما با گسترش تهدیدات مدرن، این ابزارها دیگر به تنهایی کافی نیستند. حملاتی مثل بدافزارهای پیشرفته، حملات روز صفر و تهدیدات مداوم پیشرفته (APT) می توانند به راحتی از سد روش های قدیمی عبور کنند. زیرا این ابزارها معمولاً مبتنی بر امضا یا قوانین ثابت هستند. در مقابل هوش مصنوعی توانسته امنیت مرزی را وارد مرحله ای کاملاً جدید کند. مرحله ای که در آن سیستم ها توانایی یادگیری، تحلیل و تصمیم گیری هوشمندانه دارند.

هوش مصنوعی می تواند با تحلیل لحظه ای ترافیک شبکه الگوهای نامعمول را شناسایی کند. برخلاف فایروال های سنتی که فقط بر اساس قوانین ثابت عمل می کنند، الگوریتم های یادگیری ماشین میتوانند تشخیص دهند که آیا رفتار یک بسته یا جریان ترافیک شبیه رفتارهای عادی شبکه هست یا خیر. این ویژگی باعث می شود تهدیدات ناشناخته که هنوز امضای امنیتی برای آن ها وجود ندارد، پیش از رسیدن به لایه های بعدی شناسایی و مسدود شوند. برای مثال در بسیاری از سازمان ها، سیستم های AI محور می توانند حملات DDoS را با تحلیل الگوهای ترافیک تشخیص دهند و به صورت خودکار اقداماتی مانند محدودسازی یا مسدودسازی ترافیک مشکوک را انجام دهند.

یکی دیگر از مزیت های هوش مصنوعی در امنیت مرزی، کاهش سطح هشدارهای اشتباه است. ابزار های سنتی IDS اغلب هشدارهای نادرست زیادی تولید می کنند که باعث خستگی و بی توجهی تیم امنیتی می شود. هوش مصنوعی با یادگیری رفتار عادی شبکه می تواند تنها موارد واقعی و خطرناک را گزارش کند و این موضوع بهره وری تیم امنیتی را به شدت افزایش می دهد. براساس نتایج پژوهش های جدید استفاده از مدل های هوش مصنوعی در IDS/IPS باعث شده میزان هشدارهای اشتباه تا ۵۰ درصد کاهش پیدا کند.

همچنین سیستم های مبتنی بر هوش مصنوعی قادرند در برابر حملات پیچیده تر مانند Evasion یا Polymorphic Malware مقاومت بیشتری نشان دهند. این نوع حملات سعی می‌کنند خود را شبیه ترافیک عادی نشان دهند تا سیستم های سنتی را فریب دهند. اما مدل های یادگیری عمیق (Deep Learning) با تحلیل ویژگی های پنهان رفتار ترافیک می توانند چنین فعالیت هایی را شناسایی کنند، حتی اگر ظاهر آن ها تغییر کرده باشد.

قابلیت واکنش خودکار یکی دیگر از ویژگی هایی است که هوش مصنوعی به امنیت مرزی اضافه کرده است. در گذشته تشخیص حمله ممکن بود توسط IDS انجام شود اما پاسخ دهی به آن نیازمند دخالت انسانی بود. امروزه سیستم های هوشمند می توانند بلافاصله پس از تشخیص خطر، عملاً جلوی حمله را بگیرند. این نوع واکنش سریع در حملاتی که در چند ثانیه می توانند خسارت ایجاد کنند، بسیار حیاتی است. در مجموع، هوش مصنوعی باعث شده امنیت مرزی از یک سیستم ثابت و وابسته به قوانین به یک ساختار پویا ، یادگیرنده و بسیار دقیق تبدیل شود. این فناوری نه تنها توانایی شناسایی تهدیدات شناخته شده را افزایش داده، بلکه در مقابله با تهدیدات ناشناخته و پیچیده نیز عملکردی بسیار بهتر ارائه می دهد. بنابراین ترکیب هوش مصنوعی با لایه Perimeter Security یکی از مهم ترین گام ها در تقویت دفاع در عمق و ایجاد شبکه ای امن تر محسوب می شود.

---

۳ .امنیت شبکه داخلی(Internal Network Security)

امنیت شبکه داخلی لایه ای است که تمرکز آن بر فعالیت هایی است که پس از ورود ترافیک به داخل شبکه انجام می شود. برخلاف تصور رایج، بسیاری از تهدیدات اصلی در داخل شبکه اتفاق می افتند، زیرا مهاجمان پس از عبور از امنیت مرزی سعی می کنند به صورت جانبی (Lateral Movement) حرکت کرده و به منابع حیاتی دسترسی پیدا کنند. علاوه بر این، تهدیدات داخلی مانند کارمندان ناراضی، سوء استفاده از دسترسی ها و رفتارهای غیرعادی کاربران نیز از جمله خطراتی هستند که امنیت داخلی را بسیار مهم می کنند. روش های سنتی در این لایه اغلب توانایی

تشخیص حرکات مشکوک را ندارند، زیرا تغییرات رفتاری را بررسی نمی کنند. اما با ورود هوش مصنوعی، امنیت شبکه داخلی دچار تحول اساسی شده است.

یکی از مهم ترین کاربردهای هوش مصنوعی در این لایه، تشخیص حرکات جانبی مهاجمان است. معمولاً مهاجم پس از نفوذ اولیه تلاش می کند از یک سیستم به سیستم دیگر منتقل شود و داده های بیشتری جمع آوری کند. مدل های AI با تحلیل رفتار معمول سیستم ها و کاربران می توانند متوجه شوند که چه زمانی این رفتارها از حالت طبیعی خارج شده اند. به عنوان مثال، اگر یک کارمند معمولاً فقط به یک سرور خاص دسترسی دارد اما ناگهان شروع به اسکن شبکه یا دسترسی به فایل های محرمانه کند، سیستم های مبتنی بر هوش مصنوعی این رفتار را غیرعادی تشخیص می دهند.

یکی دیگر از مزایای هوش مصنوعی در امنیت داخلی، توانایی تحلیل حجم بالای داده ها است. در شبکه های بزرگ روزانه میلیون ها رویداد ثبت می شود که بررسی دستی آن ها غیرممکن است. با این حال، مدل های یادگیری ماشین می توانند این داده ها را پردازش کرده، الگوهای روزمره را یاد بگیرند و تنها موارد مشکوک را برای بررسی به تیم امنیتی گزارش کنند. این کار باعث می شود تیم امنیتی بتواند بدون اتلاف وقت روی موارد واقعی تمرکز کند.

هوش مصنوعی همچنین در تشخیص رفتار کاربران نقش مهمی دارد. سیستم های تحلیلی معروف به UBA یا UEBA می توانند پروفایل رفتاری برای هر کاربر ایجاد کنند و هرگونه انحراف را شناسایی کنند. این کار در جلوگیری از سرقت حساب کاربری، سوء استفاده از دسترسی ها و جلوگیری از تهدیدات داخلی بسیار مؤثر است.

در کنار این موارد، هوش مصنوعی می تواند رخدادهای امنیتی را با هم مرتبط کرده و تصویر کلی تری از وضعیت شبکه ارائه دهد. برای مثال، اگر از چند نقطه شبکه فعالیت های کوچک و کم اهمیت ثبت شود، شاید سیستم های سنتی هیچ یک را به عنوان تهدید تلقی نکنند، اما هوش مصنوعی می تواند این فعالیت ها را مرتبط کرده و نتیجه بگیرد که احتمال یک حمله گسترده وجود دارد.

باید گفت هوش مصنوعی نقش بزرگی در افزایش سرعت واکنش امنیتی دارد. هنگامی که یک رفتار مشکوک تشخیص داده می شود، سیستم می تواند بلافاصله اقداماتی مانند قطع دسترسی، قرنطینه کردن دستگاه، یا هشدار به مدیریت شبکه را انجام دهد. این واکنش سریع باعث جلوگیری از گسترش حملات در داخل شبکه می شود.

به طور کلی، هوش مصنوعی امنیت شبکه داخلی را از یک فرآیند واکنشی و محدود به یک سیستم هوشمند، پیش بینی کننده و دقیق تبدیل کرده است. این تحول باعث شده لایه امنیت داخلی نقش بسیار مؤثری در دفاع در عمق ایفا کند و در برابر تهدیدات پیچیده امروزی ایستادگی بهتری داشته باشد.

---

۴ .تحلیل رفتار و پیش بینی تهدیدات (Behavioral Analysis & Threat Prediction)

تحلیل رفتار و پیش بینی تهدیدات یکی از هوشمندترین و پیشرفته ترین لایه های دفاع در عمق است. برخلاف لایه های سنتی که بیشتر واکنشی عمل می کنند، این لایه با کمک هوش مصنوعی می تواند تهدیدات را حتی قبل از وقوع شناسایی کند. این ویژگی باعث شده امنیت شبکه از حالت «پاسخ به حمله» به سمت «پیش بینی و جلوگیری از حمله» حرکت کند. امروزه بسیاری از سازمان ها از سیستم های هوشمند تحلیل رفتار برای تشخیص فعالیت های غیرعادی و بررسی الگوهای

مشکوک استفاده می کنند، زیرا روش های سنتی قادر به تحلیل چنین حجم بزرگی از داده ها نیستند.

یکی از مهم ترین کاربرد های هوش مصنوعی در این حوزه، ایجاد پروفایل رفتاری برای کاربران و سیستم ها است. مدل های یادگیری ماشین با بررسی رفتار روزمره هر کاربر یا دستگاه، مانند زمان ورود، نوع فعالیت ها، میزان دسترسی، و حجم داده های منتقل شده، یک الگوی رفتاری عادی ایجاد می کنند. هر انحراف از این الگو می تواند نشانه یک تهدید باشد. برای مثال، اگر کارمندی که همیشه در ساعات اداری وارد سیستم می شود، ناگهان نیمه شب شروع به دانلود حجم زیادی از فایل ها کند، سیستم سریع و بلافاصله هشدار می دهد.

تحلیل رفتار نه تنها برای کاربران، بلکه برای دستگاه ها، سرورها و حتی برنامه ها نیز کاربرد دارد. مثلاً اگر یک سرور شروع به ایجاد ارتباط با آدرس های ناشناس کند، یا حجم ترافیک آن به طور غیرعادی افزایش یابد، سیستم های هوش مصنوعی این فعالیت ها را غیرمنطقی تشخیص می دهند.

بخش مهم دیگری از این لایه، پیش بینی تهدیدات است. مدل های مبتنی بر هوش مصنوعی می توانند با تحلیل داده های گذشته، رفتار فعلی و روند های امنیتی، احتمال وقوع حملات را محاسبه کنند. این قابلیت به سازمان ها کمک می‌کند قبل از وقوع حادثه اقدامات لازم را انجام دهند. برای نمونه، اگر مدل های هوشمند تشخیص دهند که الگوهای رفتاری چند کاربر به رفتارهای مشکوک شبیه شده، ممکن است احتمال حمله داخلی یا سرقت اطلاعات را پیش بینی کنند.

هوش مصنوعی همچنین نقش مهمی در تشخیص تهدیدات ناشناخته (Zero-Day) دارد. تهدیدات روز صفر معمولاً هیچ امضای شناخته شده ای ندارند و ابزارهای سنتی نمی توانند آن ها را تشخیص دهند. اما مدل های یادگیری عمیق با تحلیل ویژگی های رفتاری و الگوهای مشابه، می توانند

احتمال وجود یک تهدید جدید را شناسایی کنند، حتی اگر هیچ داده ای از گذشته درباره آن وجود نداشته باشد.

---

۵ .نتیجه گیری

در این مقاله نقش هوش مصنوعی در تقویت دفاع در عمق شبکه مورد بررسی قرار گرفت. نتایج نشان داد که هوش مصنوعی می تواند کارایی لایه های امنیت مرزی، امنیت شبکه داخلی و تحلیل رفتار را به‌طور چشمگیری افزایش دهد. این فناوری با افزایش دقت شناسایی تهدیدات، کاهش هشدارهای اشتباه و تسریع واکنش امنیتی، امنیت شبکه را از حالت واکنشی به حالت پیشگیرانه تبدیل می کند. در نهایت، ترکیب هوش مصنوعی با رویکرد دفاع در عمق، راهکاری مؤثر و قابل اعتماد برای مقابله با تهدیدات پیچیده سایبری در دنیای امروز محسوب می شود.

---

۶ .منابع

https://ijsra.net/sites/default/files/IJSRA-2024-2161.pdf

https://www.irejournals.com/formatedpaper/1706249.pdf

https://catalog.lib.kyushu-u.ac.jp/opac_download_md/6793674/p1133-1139.pdf

https://journal.pandawan.id/itee/article/view/428/381

https://www.researchgate.net/profile/Carlos-Merlano-Porras/publication/386621772_Enhancing_Cyber_Security_through_Artificial_Intelligence_and_Machine_Learning_A_Literature_Review/links/6758526805bf5b3e924c303a/Enhancing-Cyber-Security-through-Artificial-Intelligence-and-Machine-Learning-A-Literature-Review.pdf

https://www.researchgate.net/profile/Georgi-Tsochev/publication/323919777_Increasing_the_level_of_network_and_information_security_using_artificial_intelligence/links/5c331bf5a6fdccd6b598b393/Increasing-the-level-of-network-and-information-security-using-artificial-intelligence.pdf

---

https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2023.1200390/full

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9172062

https://www.researchgate.net/profile/Bilal-Zafer/publication/392657246_Next-Gen_Cybersecurity_Integrating_Artificial_Intelligence_with_Behavioral_Analytics_for_Threat_Prediction/links/684c2ee326f43051a5806fde/Next-Gen-Cybersecurity-Integrating-Artificial-Intelligence-with-Behavioral-Analytics-for-Threat-Prediction.pdf

https://d197for5662m48.cloudfront.net/documents/publicationstatus/90291/preprint_pdf/c12f4b6dfcb0ece3a42a357ad2203fac.pdf

https://d1wqtxts1xzle7.cloudfront.net/102883869/IJAERS_08_may_2023-libre.pdf?1685595510=&response-content-disposition=inline%3B+filename%3DEnhancing_cybersecurity_The_power_of_art.pdf&Expires=1765479225&Signature=XXIYvDS6gU7SUvLXtwcwncJf7nI~fx0HRnTub16vbX7teSQL8D~bPCbcbVcVgFjDA9FW3Bqk5jK7TTe-~p4TynNu5ccIh-cQs7-BQcNLDSzl~OV70N~rZg2FTX1DsW4~qvl6B0RDbHIp8qIpaxzOl2MCptegdYUldcVUl~nqWKOQal~H8onDSCTD6mzFOn1mWlHYPOQXQrlKeOzgU8jVmbyBKxNkQ6bteXob2PQg9HbINr-SoAZ2kGNjCKVFDiipiiJTeE5Sorq1FcmpFWGSrAmL7tv~bZkP9BYOjXVE3npb-m4M4JSdO7~BB895YLGzAVntDL4pTxo-YC6TLdLhRQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA