Quarterly Journal of Defense Technology Engineering Imam Ali University

Autumn 2024, Vol. 39

Original Research

The Role of Artificial Intelligence in Defense Technology Engineering: A New Approach to Cybersecurity

Mohadeseh Dhavamipour Sereshkeh [1*], Amirreza Mahmoudi [2]

[1] PhD student in criminal law and criminology, Lahijan branch, Islamic Azad University, Lahijan

[2] Assistant Professor, Department of Law, Lahijan branch, Islamic Azad University, Lahijan

ARTICLE INFO

Received: 2024.05.09

Accepted: 2024.08.20

Published: 2024.09.13

Keyword:

Cyber warfare

Cyber Defense

Artificial Intelligence in Cyber

Defense Technology Engineering

***Corresponding Author:**

Mohadeseh Dhavamipour Sereshkeh

Email:

mohadesehghavamipour@gmail.com

ABSTRACT

A cyber-attack means unauthorized access to computer systems via the Internet with the aim of dominating critical infrastructure and causing disruption. Attack tools include malicious software and actions of aggressive users that can completely destroy advanced infrastructure and paralyze even the strongest countries. Defending against these attacks, especially in dynamic and complex networks, are difficult using traditional algorithms. In the meantime, advanced artificial intelligence technologies, with their flexibility and learning capabilities, offer new solutions to counter these threats. This article analyzes artificial intelligence methods in cyber defense and introduces intelligent techniques such as artificial neural networks and expert systems as effective tools in engineering defense technology. The findings show that many challenges related to cyber security can only be solved through artificial intelligence. In addition, examples of real-world cyber–attacks are examined to illustrate the importance of advanced technologies in cyber defense.

فصل نامه مهندسی فناوری‌های دفاعی دانشگاه افسری امام علی (ع)

پاییز ۱۴۰۳ ، دوره ۳۹



مقاله پژوهشی

نقش هوش مصنوعی در مهندسی فناوری دفاعی: رویکردی نوین به امنیت سایبری

محدثه قوامی‌پور سرشکه [۱*]، امیررضا محمودی [۲]

۱- دانشجوی دکتری حقوق کیفری و جرم شناسی، واحد لاهیجان، دانشگاه آزاد اسلای، لاهیجان

۲- استادیار گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلای، لاهیجان

اطلاعات مقاله

دریافت مقاله: ۱۴۰۳/۱۰/۱۹

پذیرش مقاله: ۱۴۰۳/۰۶/۳۰

انتشار مقاله: ۱۴۰۳/۰۹/۲۳

کلید واژگان:

هوش مصنوعی

مهندسی فناوری دفاعی

امنیت سایبری

شبکه‌های عصبی مصنوعی

دفاع سایبری

نویسنده مسئول*

محدثه قوامی‌پور سرشکه

پست الکترونیکی:

mohadesehghavamipour@gmail.com

چکیده

حمله سایبری به معنای دسترسی غیرمجاز به سیستم‌های رایانه‌ای از طریق اینترنت با هدف تسلط بر زیرساخت‌های حیاتی و ایجاد اختلال است. ابزارهای حمله شامل نرم‌افزارهای مخرب و اقدامات کاربران مهاجم است که می‌توانند زیرساخت‌های پیشرفته را به‌طور کامل نابود کنند و حتی قوی‌ترین کشورها را فلج نمایند. دفاع در برابر این حملات، به‌ویژه در شبکه‌های پویا و پیچیده، با استفاده از الگوریتم‌های سنتی دشوار است. در این میان، فناوری‌های پیشرفته هوش مصنوعی، با انعطاف‌پذیری و قابلیت یادگیری خود، راهکارهای نوینی برای مقابله با این تهدیدات ارائه می‌دهند.این مقاله به تحلیل روش‌های هوش مصنوعی در دفاع سایبری پرداخته و تکنیک‌های هوشمندی مانند شبکه‌های عصبی مصنوعی و سیستم‌های خبره را به‌عنوان ابزارهای مؤثر در مهندسی فناوری دفاعی معرفی می‌کند. یافته‌ها نشان می‌دهند که بسیاری از چالش‌های مرتبط با امنیت سایبری تنها از طریق هوش مصنوعی قابل حل هستند. علاوه بر این، نمونه‌هایی از حملات سایبری واقعی در جهان بررسی شده تا اهمیت فناوری‌های پیشرفته در دفاع سایبری روشن شود.

۱.مقدمه

در عصر اطلاعات که امروزه در آن زندگی می‌کنیم، مفاهیمی مانند دولت الکترونیک، امضای الکترونیک و تجارت الکترونیک به‌طور مکرر مورد بحث قرار می‌گیرند. به دلیل افزایش سرعت و بهره‌وری و همچنین سهولت استفاده، بسیاری از اطلاعات به محیط‌های الکترونیکی منتقل شده‌اند. با این حال، مشاهده شده است که دستیابی دیگران به اطلاعات شخصی یا سازمانی مهم، می‌تواند خسارات مادی و معنوی به بار آورد. به همین دلیل، در پروژه‌هایی نظیر دولت الکترونیک و سازمان‌های الکترونیک، امنیت در بالاترین سطح خود به‌عنوان یک هدف ملی تعیین شده و اقدامات حقوقی و فناوری در این زمینه اتخاذ شده است.(Sağıroğlu & Alkan, 2005, p. 85)

در دنیایی که بسیاری از فعالیت‌ها در فضای مجازی انجام می‌شود، نادیده گرفتن مفهوم جنگ سایبری امکان‌پذیر نیست. جنگ سایبری به معنای دسترسی غیرمجاز، مخفیانه و نامرئی به سیستم‌های تحت کنترل رایانه‌ای دشمن از طریق اینترنت با هدف تضعیف روحیه و روان آن‌ها است. هدف اصلی این نوع حملات، سرقت، تغییر، نابودی یا هدایت نادرست اطلاعات است. (Sundaram, 1996, p. 4)سناریوهای جنگ سایبری که زمانی شبیه تئوری‌های توطئه یا افسانه به نظر می‌رسیدند، اکنون به واقعیت تبدیل شده‌اند.

حملات سایبری که از طریق اینترنت انجام می‌شوند، به تهدیدی جدی تبدیل شده‌اند. جنگ، پس از زمین، هوا، دریا و فضا، اکنون به دنیای مجازی منتقل شده است. فعالیت‌های انجام‌شده در فضای مجازی تحت عناوینی نظیر حمله سایبری، سلاح‌های سایبری، جنگ سایبری و دفاع سایبری طبقه‌بندی می‌شوند. دشمنان در این جنگ‌ها بی‌حرکت، غیرقابل‌دسترس و ناشناخته هستند و این امر باعث می‌شود حملات سایبری خطرناک‌تر از حملات فیزیکی باشند. افزایش حملاتی که برای از کار انداختن، سرقت، نابودی، یا سوءاستفاده از نرم‌افزارها و کدهای سیستم‌های رایانه‌ای انجام می‌شوند، نشان‌دهنده اهمیت روزافزون دفاع سایبری است.

این مقاله به دنبال پاسخگویی به این سوال است که سیستم های هوش مصنوعی به چه صورت می توانند در برابر حملات سایبری موفق عمل کنند و به نوعی دفاع با هوش مصنوعی در برابر جنگ سایبری به چه شکل می باشد. هدف این مقاله تبیین راهکارهای هوش مصنوعی در دفاع از حملات سایبری می باشد. این مقاله در قالب نظری و با روش توصیفی تحلیلی هوش مصنوعی، دفاع سایبری، جنگ دیجیتال و ... را مورد بررسی قرار خواهد داد.

۱. دفاع سایبری

با گسترش اینترنت و امکانات ارتباطی، سیستم‌های بیشتری در معرض حمله قرار گرفته‌اند. بخش عمده‌ای از این حملات با بهره‌گیری از نقص‌ها یا کاستی‌های موجود در سیستم‌ها انجام می‌شود. برای

مقابله با این حملات دو راهکار وجود دارد:

- ایجاد یک سیستم و محیط کاملاً امن؛
- شناسایی حملات و اتخاذ اقدامات لازم.

راهکار اول در عمل غیرممکن است. دلایل این امر عبارتند از:

- ضعف‌های موجود در سیستم‌های عامل معمولاً ابتدا توسط مهاجمان شناسایی می‌شوند و تا زمان اتخاذ اقدامات پیشگیرانه از این ضعف‌ها استفاده می‌کنند؛
- برخی از قوانین ساختاری پروتکل‌های انتقال داده می‌توانند برای اهداف حمله مورد استفاده قرار گیرند؛
- روش‌های رمزنگاری و کلیدهای آن‌ها ممکن است شکسته شوند یا کاربران رمز عبور خود را فراموش کنند؛ (Sundaram, 1996, p. 6)
- حتی اگر امنیت در برابر تهدیدات خارجی تضمین شود، امکان سوءاستفاده داخلی وجود دارد؛
- کاهش سطح دسترسی کاربران برای افزایش امنیت ممکن است کارایی آن‌ها را کاهش دهد.

افرادی که قصد دارند سیستم‌های خود را ایمن نگه دارند، معمولاً تا زمان وقوع حمله در وضعیت انتظار باقی می‌مانند و تلاش می‌کنند حمله را به‌سرعت شناسایی کنند. این همان وظیفه دفاع سایبری است. بدون اطلاع از منبع یا پورت حمله، مقابله با آن امکان‌پذیر نیست.

تکنیک‌های دفاع سایبری مبتنی بر هوش مصنوعی با استفاده از اطلاعات جمع‌آوری‌شده و ذخیره‌شده به‌طور دقیق، قابلیت شناسایی زودهنگام حملات را دارند. این تکنیک‌ها همچنین می‌توانند حملاتی که پیش‌تر با آن‌ها مواجه نشده‌اند را شناسایی کنند. این ویژگی، هوش مصنوعی را به ابزاری جذاب در دفاع سایبری تبدیل کرده است. (Sağıroğlu & Alkan, 2005, p. 67)

۲. هوش مصنوعی

هنگامی که صحبت از هوش مصنوعی می‌شود، نخستین تصوری که به ذهن خطور می‌کند، توانایی ماشین در تفکر شبیه به انسان، تقلید رفتار انسانی، یا حتی شبیه‌سازی یک مغز انسانی است. در واقع، ایده شخصی‌سازی رایانه‌ها در ذهن تداعی می‌شود. اما آنچه در پژوهش حاضر درباره هوش مصنوعی مدنظر قرار دارد، بررسی ساختار الگوریتمی است که برای حل مسائل مختلف از آن بهره می‌برد و ارتباط آن با منطق حل مسئله انسانی است. به‌طور کلی، هوش مصنوعی به عنوان توانایی یک رایانه یا دستگاهی که توسط رایانه کنترل می‌شود، تعریف می‌شود که وظایفی مرتبط با فرآیندهای ذهنی

پیشرفته، مانند استدلال، استخراج معنا، تعمیم‌دادن و یادگیری از تجربیات گذشته را که به‌طور معمول مختص انسان است، انجام دهد. (Kalaycı, 2016, p. 4) اگر بخواهیم تعریفی جامع ارائه دهیم، هدف از هوش مصنوعی ایجاد سیستم‌های رایانه‌ای است که رفتارهایی شبیه انسان داشته باشند.

آنچه در مفهوم هوش مصنوعی اهمیت دارد، اطلاعات است. توانایی استخراج نتایج از اطلاعات و اتصال این نتایج به دلایل منطقی، نمونه‌ای از قابلیت تفکر هوش مصنوعی محسوب می‌شود. به طور طبیعی، در این فرایند انتظار می‌رود که هوش مصنوعی به جای تکیه بر داده‌های خام، بر دانش سطح بالاتری متمرکز شود. این سیستم‌ها اطلاعات را ترکیب می‌کنند، تحلیل می‌کنند، به نتیجه می‌رسند و نتایج خود را بر پایه دلایل منطقی ارائه می‌دهند.

تاریخچه هوش مصنوعی به قدمت علم رایانه مدرن بازمی‌گردد. آلن متیسون تورینگ، که به عنوان پدر علم رایانه شناخته می‌شود، با مطرح کردن پرسش «آیا ماشین‌ها می‌توانند فکر کنند؟» زمینه را برای بحث درباره هوش ماشینی باز کرد. اگر بخواهیم به مثالی از تفکر شبیه انسان توسط هوش مصنوعی اشاره کنیم، می‌توانیم تولید هوش مصنوعی **دیپ بلو**[1] را ذکر کنیم که موفق شد قهرمان شطرنج روسیه، کاسپاروف را شکست دهد. (Kalaycı, 2016, p. 3) در روزهای ابتدایی رایانه‌ها، تصور اینکه یک هوش مصنوعی بتواند با بازی شطرنج، قهرمان جهان را شکست دهد، تقریباً غیرممکن به نظر می‌رسید. اما این امر محقق شد و سه دلیل اصلی برای آن وجود دارد:

- قدرت پردازش بالا،
- طراحی یک الگوریتم مناسب،
- وجود پایگاه‌های داده حاوی تمامی اطلاعات ممکن درباره شطرنج.

در حقیقت، مسئله شطرنج به دلیل ماهیت خاص خود که به هوش مصنوعی محدود مربوط می‌شود، قابل حل بود. اما برای مسائل دیگر، مانند ترجمه زبان، نیاز به هوش مصنوعی عمومی جنرال است. در دهه ۱۹۶۰ و به‌ویژه پس از کارهای ساختاری نوام چامسکی در حوزه زبان‌شناسی، پیش‌بینی می‌شد که مشکل ترجمه زبان‌های طبیعی به‌زودی حل شود. با اینکه در برخی برنامه‌های خاص، مانند زبان‌شناسی هوش مصنوعی گوگل، موفقیت‌هایی حاصل شده است، هنوز ترجمه زبان‌های طبیعی به‌صورت کامل امکان‌پذیر نشده است. علت این امر، نیاز به اطلاعات گسترده در همه زمینه‌های مرتبط با فعالیت‌های انسانی و ضرورت برخورداری از هوش مصنوعی عمومی برای مدیریت چنین اطلاعاتی است. (Kalaycı, 2016, p. 4)

۳. ضرورت استفاده از هوش مصنوعی در دفاع سایبری

---

[1] Deep Blue

برای شروع، لازم است به **ویروس کنفیکر**[۱] اشاره کنم. تأثیرات این ویروس بر شبکه‌های نظامی و پلیسی اروپا شامل موارد زیر بود:

- در تاریخ ۱۵ ژانویه ۲۰۰۹، این ویروس به شبکه رایانه‌ای نیروی دریایی فرانسه نفوذ کرد. این شبکه به‌منظور جلوگیری از گسترش ویروس به دیگر رایانه‌ها، قرنطینه شد.
- وزارت دفاع انگلستان اعلام کرد که برخی از سیستم‌های اصلی و رایانه‌های رومیزی آن آلوده شده‌اند.
- ویروس به دفاتر اداری، تعدادی از کشتی‌های جنگی سلطنتی و زیردریایی‌های نیروی دریایی سلطنتی گسترش یافت. همچنین در بیمارستان‌های شهر شفیلد، ویروس در بیش از ۸۰۰ رایانه گزارش شد.
- در آلمان، حدود ۱۰۰ رایانه متعلق به بوندس‌ور (نیروهای مسلح جمهوری فدرال آلمان) آلوده شد.
- در ژانویه ۲۰۱۰، ویروس به شبکه پلیس منچستر نفوذ کرد که به‌عنوان یک اقدام احتیاطی، ارتباط رایانه‌های پلیس ملی به مدت سه روز قطع شد. در این مدت، مأموران مجبور شدند بازرسی‌های معمول را با وسایل نقلیه و افراد به صورت دستی انجام دهند. (Shankarapani et al., 2010, p. 2504)

برای مقابله با این حملات سایبری رو به افزایش، توسعه تدابیر تکنولوژیکی ضروری است. هدف از این تدابیر، حفاظت از اطلاعات به‌عنوان یک دارایی مهم در برابر تهدیدها و حملات سایبری است. اما دفاع در برابر سلاح‌های سایبری هوشمند، تنها با استفاده از نرم‌افزارهای هوشمند امکان‌پذیر است.

برای جلوگیری از تکرار حوادثی مانند ویروس مذکور، تغییرات فوری در دفاع سایبری موردنیاز است. روش‌های جدید دفاعی، نیازمند محیط‌های امن، آگاهی جامع از موقعیت، واکنش‌های بسیار خودکار به حملات شبکه‌ای و استفاده گسترده از ابزارهای مبتنی بر دانش و روش‌های هوش مصنوعی است.(Sundaram, 1996, p. 3-7)

برای درک این مسئله کافی است نگاهی دقیق‌تر به فضای سایبری بیندازیم. هوش مصنوعی در عملیات سایبری ضروری است، زیرا می‌تواند به سرعت به شرایط اینترنتی واکنش نشان دهد. هوش مصنوعی به دلیل سرعت واکنش بالا، تحلیل دقیق رویدادها و توانایی اتخاذ تصمیمات مناسب در فضای سایبری، نقشی کلیدی ایفا می‌کند. در یک محیط سایبری کارآمد، مقابله با حملات به کمک

---

[۱] Conficker

الگوریتم‌های سنتی بسیار دشوار است؛ چرا که تهدیدهای جدید به‌طور مداوم ظاهر می‌شوند. این امر لزوم استفاده از روش‌های هوش مصنوعی را برجسته می‌کند.

۴. سیستم‌های هوشمند مورد استفاده در دفاع سایبری

روش‌های تشخیص نفوذ که برای شناسایی حملات به سیستم‌های رایانه‌ای یا شبکه‌ها طراحی شده‌اند، علیرغم توانایی بالا در شناسایی بسیاری از حملات، قادر به شناسایی تعداد زیادی از حملات ناشناخته و جدید نیستند. این ضعف منجر به خسارات جدی به سیستم‌ها می‌شود و نیاز به افزایش دقت در شناسایی تهدیدات جدید را نشان می‌دهد. برای پاسخ به این نیاز و تضمین امنیت اطلاعات و رایانه‌ها در مواجهه با حملات متغیر و پیچیده، روش‌های هوش مصنوعی برای بهبود عملکرد دفاع سایبری در توسعه آن ها به‌کار گرفته شده است. قابلیت‌های برجسته تکنیک‌های هوش مصنوعی شامل یادگیری سریع، ارائه راه‌حل برای مسائل پیچیده و ریاضیاتی، و تعمیم مناسب است که استفاده از این رویکردها در دفاع سایبری را به‌شدت توجیه می‌کند.

با ورود رویکردهای هوشمند، روش‌های تشخیص ناهنجاری[۱] مورد توجه بیشتری قرار گرفته‌اند. این رویکردها توانایی شناسایی تهدیدات جدید را به‌طور قابل‌توجهی افزایش داده‌اند. از اهداف اصلی پژوهشگران هوش مصنوعی همواره توسعه سیستم‌هایی بوده است که مانند انسان فکر و رفتار کنند. با درک دشواری این هدف، تمرکز تحقیقات به طراحی سیستم‌هایی که به‌طور منطقی فکر و عمل می‌کنند تغییر یافت.

هوش مصنوعی در حل مسائل دشوار یا غیرممکن با روش‌های سنتی نقش مهمی ایفا می‌کند. از جمله تکنیک‌های هوش مصنوعی که در این زمینه استفاده می‌شوند عبارتند از: شبکه‌های عصبی مصنوعی[۲]، سیستم‌های خبره[۳]، عوامل هوشمند[۴]، الگوریتم‌های ژنتیک[۵]، منطق فازی[۶]، جستجو[۷] و یادگیری[۸].

الف. شبکه‌های عصبی مصنوعی

استفاده از **رویکردهای هوشمند** در دفاع سایبری نشان داده است که می‌توان از روش‌های هوشمند متنوعی استفاده کرد. از میان این تکنیک‌ها، شبکه‌های عصبی مصنوعی به دلیل نتایج

---

[۱] Anomaly Detection
[۲] Neural Nets
[۳] Expert Systems
[۴] Intelligent Agents
[۵] Genetic Algorithms
[۶] Fuzzy Logic
[۷] Search
[۸] Learning

موفقیت‌آمیز، بیشترین کاربرد را داشته‌اند. (Wassmer & Fikus, 2003, p. 1-14; Cannady, 1998, p. 443-456) شبکه‌های عصبی مصنوعی سیستم‌هایی رایانه‌ای هستند که بر مبنای اصول کارکرد سلول‌های مغز انسان طراحی شده‌اند و شامل ورودی‌ها و خروجی‌هایی هستند که به‌شدت با یکدیگر در تعامل‌اند.

تاریخچه شبکه‌های عصبی مصنوعی به پرسپترون[۱]، که توسط فرانک روزنبلات در سال ۱۹۵۷ معرفی شد، بازمی‌گردد. (Rosenblatt, 1957) پرسپترون‌های محدود قادر به یادگیری و حل مسائل جالب بودند. اما شبکه‌های عصبی مصنوعی از تعداد زیادی نورون مصنوعی تشکیل می‌شوند که امکان یادگیری و تصمیم‌گیری به‌صورت موازی را فراهم می‌کنند.

ویژگی متمایز این سیستم‌ها سرعت پردازش بالای آن‌هاست. شبکه‌های عصبی مصنوعی برای مدل‌سازی یادگیری، تشخیص الگو، طبقه‌بندی و انتخاب پاسخ به اقدامات مناسب به کار گرفته می‌شوند.(Klein et al., 2010) این سیستم‌ها قابلیت استفاده در سخت‌افزار و نرم‌افزار را دارند. شبکه‌های عصبی مصنوعی به راحتی در تشخیص و پیشگیری از نفوذ قابل استفاده هستند. پیشنهاداتی برای استفاده از آنها در تشخیص حملات (Iftikhar & Alghamdi, 2009, p. 229) ، تشخیص ویروس‌های کامپیوتری(Stopel et al., 2006, p. 2362) ، تشخیص هرزنامه‌ها (Wu, 2009, p. 4321)، تشخیص زامبی‌ها(Salvador et al., 2009) ، طبقه‌بندی بدافزارها (Shankarapani et al., 2010, p. 2504)و تحقیقات قانونی (Fei et al., 2006, p. 33) ارائه شده است.

یکی از دلایل محبوبیت شبکه‌های عصبی مصنوعی در دفاع سایبری، سرعت بالای آن هنگام استفاده در سخت‌افزار یا پردازنده گرافیکی است. پیشرفت‌های جدیدی در تکنولوژی شبکه‌های عصبی وجود دارد. شبکه‌های عصبی نسل سوم که نورون‌های بیولوژیکی را واقعی‌تر شبیه‌سازی می‌کنند و فرصت‌های کاربردی بیشتری را فراهم می‌آورند.

ب: سیستم های خبره

سیستم‌های خبره را می‌توان سیستم‌هایی دانست که امکان حل مسائل پیچیده‌ای که تنها یک متخصص انسانی می‌تواند حل کند را با کامپیوتر فراهم می‌کنند. سیستم‌های خبره یک برنامه هوش مصنوعی هستند. به طور کلی از الگوریتم استفاده نمی‌کنند و دانش مهم‌تر از پایگاه داده است. سیستم‌های خبره بدون تردید پرکاربردترین ابزارهای هوش مصنوعی هستند. یک سیستم خبره نرم‌افزاری است که برای یافتن پاسخ به سوالات در حوزه‌های کاربردی که توسط کاربر یا نرم‌افزار نشان داده می‌شود، استفاده می‌شود. این سیستم‌ها می‌توانند مستقیماً در تشخیص‌های پزشکی، امور مالی یا حوزه سایبری برای پشتیبانی تصمیم‌گیری استفاده شوند. (Kivimaa et al., 2009, p. 280)

---

[۱] Perceptron

انواع مختلفی از سیستم‌های خبره از سیستم‌های تشخیصی فنی کوچک تا سیستم‌های ترکیبی بزرگ و پیچیده برای حل مسائل پیچیده وجود دارد. به عنوان یک مفهوم، یک سیستم خبره شامل پایگاه دانشی است که دانش تخصصی مربوط به یک حوزه کاربردی خاص در آن ذخیره می‌شود. علاوه بر پایگاه دانش، یک موتور استنتاج که بر اساس این دانش پاسخ تولید می‌کند و همچنین اطلاعات اضافی در مورد یک وضعیت خاص را شامل می‌شود. پایگاه دانش خالی و موتور نتیجه‌گیری با هم پوسته سیستم خبره نامیده می‌شوند که باید قبل از استفاده با دانش پر شود. پوسته سیستم خبره باید با نرم‌افزاری برای افزودن دانش به پایگاه دانش پشتیبانی شود و می‌تواند با برنامه‌هایی برای تعامل کاربر و سایر برنامه‌های قابل استفاده در سیستم خبره ترکیبی پشتیبانی شود. سیستم‌های مبتنی بر قاعده، ترافیک سیستم را بررسی کرده و قوانینی ایجاد می‌کنند و رفتارها در طول تشخیص حمله بر اساس قوانین تعیین شده طبقه‌بندی می‌شوند. (Ilgun et al., 1995, p. 181) با این حال، مفید بودن یک سیستم خبره اساساً نه به شکل نمایش دانش، بلکه به کیفیت دانش موجود در پایگاه دانش سیستم بستگی دارد. (Kivimaa et al., 2009, p. 279) این سیستم خبره انتخاب سطح امنیتی را به میزان قابل توجهی تسهیل می‌کند و برای استفاده بهینه از منابع محدود راهنمایی می‌کند. با استفاده از سیستم‌های خبره می‌توان حملات را در مراحل اولیه تشخیص داد. (Anderson et al., 1995; Lunt & Jagannathan, 1988, p. 59).

پ. عامل‌های هوشمند

از دیدگاه علوم کامپیوتر، کلمه هوشمند به معنای انجام هر عملیات توسط یک عامل با استفاده از ابتکارات خاص است. به عنوان مثال، یک نماینده غیر هوشمند در هر مرحله و هر عملیات از کاربر سؤال می‌پرسد، در حالی که در نماینده هوشمند می‌توان از یک ساختار خودمختار صحبت کرد. عامل‌های هوشمند، اجزای نرم‌افزاری هستند که دارای ویژگی‌های رفتار هوشمند هستند که آنها را خاص می‌کند. یک عامل دارای ویژگی‌هایی مانند درک زبان ارتباطی عامل، واکنش‌پذیری (تصمیم‌گیری و عمل)، توانایی برنامه‌ریزی، تحرک و توانایی انعکاس است.

به طور خلاصه اگر بخواهم در مورد نوع حمله‌ای به نام "DDoS" توضیح دهم، درخواست‌های دسترسی جعلی بیش از حد پاسخگویی به یک سایت یا سرور ارسال می‌شود. در نتیجه، سایت نمی‌تواند به درخواست‌های سرور پاسخ دهد و خود را خاموش می‌کند. پس از برخی راه‌حل‌های قانونی و همچنین مشکلات تجاری، باید امکان توسعه یک "پلیس سایبری" متشکل از عامل‌های هوشمند متحرک وجود داشته باشد. این امر مستلزم پیاده‌سازی زیرساخت‌های تحرک و ارتباطات برای عامل‌های سایبری خواهد بود. ابزارهای چند عامله می‌توانند فضای سایبری را کاملاً عملیاتی نشان دهند، به عنوان مثال؛ روش‌های تشخیص حمله مبتنی بر شبکه عصبی و چند عامله ترکیبی آزمایش شده‌اند و حملات توسط سیستم‌های مبتنی بر عامل تشخیص داده شده‌اند. (Chatzigiannakis et

al., 2004)

ت. الگوریتم‌های ژنتیک

الگوریتم‌های ژنتیک روشی اکتشافی هستند که بر اساس اصل تولید رشته‌های جدید کروموزوم‌ها برای حل مسائل پیچیده منظم عمل می‌کنند. مجموعه داده‌ها با استفاده از شنودگران ترافیک مانند ''tcpdump''یا ''snort'' جمع‌آوری می‌شوند.(Murali & Rao, 2005, p. 233)

ث. منطق فازی

منطق فازی مکانیسمی برای تفکر، تصمیم‌گیری و نتیجه‌گیری است که امکان تصمیم‌گیری سازگار و صحیح را بر اساس اطلاعات ناقص و نامشخص فراهم می‌کند. تلاش‌های اجرای روش منطق فازی برای توسعه اجزای مختلف حملات سایبری در سال‌های ۲۰۰۰ آغاز شد. با موتور تشخیص نفوذ فازی که از این مطالعات نشأت گرفت، منطق فازی پس از پردازش داده‌های هوش مصنوعی برای تشخیص حملات استفاده شد.(Dickerson & Dickerson, 2000, p. 301)

ج. جستجو

جستجو یک روش جهانی است. در حالی که می‌تواند در تمام شرایط حل مسئله اعمال شود، روش‌های دیگر ممکن است در حل مسئله قابل اجرا نباشند. درخت‌های جستجوی و/یا، جستجوی آلفا-بتا، جستجوی مین-ماکس و جستجوی تصادفی به طور گسترده در نرم‌افزارهای بازی استفاده می‌شوند و برای تصمیم‌گیری در دفاع سایبری مفید هستند.

چ. یادگیری

یادگیری به معنای توسعه یک سیستم دانش با گسترش یا سازماندهی مجدد پایگاه دانش، یا بهبود موتور استنتاج است. (Norvig & Russell, 2000) این یکی از جالب‌ترین مسائل هوش مصنوعی است که تحت تحقیقات گسترده قرار دارد. یادگیری ماشین شامل روش‌های محاسباتی برای کسب دانش جدید، مهارت‌های جدید و سازماندهی دانش موجود است.

مشکلات یادگیری از یادگیری پارامتریک که به معنای یادگیری مقادیر برخی پارامترهاست، تا اشکال پیچیده یادگیری نمادین که شامل یادگیری مفاهیم، دستور زبان، توابع و حتی رفتار است، متغیر است. هوش مصنوعی روش‌هایی مانند یادگیری نظارت شده (با یک معلم) و یادگیری بدون نظارت را فراهم می‌کند.

روش دوم به ویژه هنگامی که حجم زیادی از داده‌ها در دسترس است مفید است و در تشخیص نفوذ رایج است زیرا در آن لاگ‌های بزرگی وجود دارد. داده‌کاوی باعث توسعه یادگیری بدون نظارت شده است. اگر بخواهیم به طور خلاصه به داده‌کاوی اشاره کنیم، استخراج دانش برای کشف رویدادهای پنهان در پایگاه داده است. برای یافتن الگوها و روابط بین داده‌ها و استخراج قوانین استفاده می‌شود. به این ترتیب، فعالیت‌های کاربر عادی با استفاده از ردپاهای حساب شناسایی می‌شود. (Lee et al.,

2001, p. 89)

۵. چالش‌های موجود در دفاع سایبری هوشمند

هنگام برنامه‌ریزی تحقیقات آینده، توسعه و اجرای روش‌های هوش مصنوعی در دفاع سایبری برای تمایز اهداف و چشم‌اندازهای بلندمدت بوده است. مدیریت اطلاعات برای جنگ اینترنت‌محور یک کاربرد دشوار است. (Kaster, 2009) تنها مدیریت خودکار اطلاعات می‌تواند برتری تصمیم‌گیری را برای رهبران در ارزیابی سریع وضعیت تضمین کند. سیستم‌های خبره در حال حاضر در بسیاری از برنامه‌ها استفاده می‌شوند، گاهی اوقات در برنامه پنهان هستند، مانند برنامه‌ریزی اقدامات امنیتی. با این حال، می‌توانید عملکرد بهتری از سیستم‌های خبره بگیرید، اگر پایگاه‌های دانش گسترده توسعه یابند.

الف. نمونه‌هایی از حملات سایبری در جهان

در طول جنگ سرد، مشخص شد که روسیه و ایالات متحده فعالیت‌های جاسوسی متقابل انجام می‌دادند. در سال ۱۹۸۲، مسکو شروع به سرقت نرم‌افزاری از یک شرکت در کانادا کرد که برای کنترل خطوط لوله گاز طبیعی استفاده می‌شد. آمریکایی‌ها که متوجه این موضوع شدند، به جای متوقف کردن عملیات، یک ویروس در نرم‌افزار جاسازی کردند. نرم‌افزاری که روس‌ها دزدیده بودند بعد از مدتی توسط ویروس خراب شد، جریان در خطوط لوله را به سطوح غیرعادی افزایش داد و باعث ترکیدن لوله شد. در نتیجه، بزرگترین انفجار (غیرهسته‌ای) قابل مشاهده از فضا تا آن زمان رخ داد. این رویداد به عنوان اولین حمله سایبری در تاریخ ثبت شد. (Cannady, 1998, p. 443-456)

در سال ۲۰۰۳، زمانی که ایالات متحده برنامه‌ریزی برای اشغال عراق را آغاز کرد، هزاران نفر از کارکنان وزارت دفاع عراق درست پیش از حمله، پیامی روی صفحه نمایش رایانه‌های خود از فرماندهی مرکزی ایالات متحده دریافت کردند. در این پیام نوشته شده بود: «به‌زودی ممکن است به عراق حمله کنیم. نمی‌خواهیم به شما آسیبی برسد. اگر نمی‌خواهید به شما صدمه‌ای وارد شود، هنگام شروع جنگ به خانه‌های خود بروید.» بسیاری از افراد، حتی نظامیان، این پیام را جدی گرفته و تانک‌های خود را رها کرده و به خانه‌هایشان بازگشتند. این اقدام باعث شد ایالات متحده به‌راحتی تانک‌های عراق را نابود کند.(Wassmer & Fikus, 2003, p. 1-14)

چین، یکی از کشورهایی است که در زمینه حملات و دفاع سایبری بسیار قدرتمند ارزیابی می‌شود. ادعا شده است که چین تلاش دارد اسرار نظامی ایالات متحده و فناوری‌های پیشرفته اروپا را به دست آورد. گفته می‌شود متخصصان سایبری چین توانسته‌اند به اطلاعات محرمانه شرکت لاکهید مارتین، تولیدکننده تجهیزات نظامی آمریکا، دست یابند و تمامی طرح‌های جنگنده F-35 را سرقت کنند (Cannady, 1998, p. 443-456).

در تاریخ ۶ سپتامبر ۲۰۰۷، جنگنده‌های اسرائیلی ساختمانی را در ۱۲۰ کیلومتری داخل مرز

سوریه با ترکیه بمباران کردند. این ساختمان که گمان می‌رفت یک تأسیسات هسته‌ای باشد، در عرض یک شب به‌طور کامل نابود شد. با این حال، ارتش سوریه تا صبح از این حمله آگاهی نیافت. این در حالی بود که رادارهای پیشرفته‌ای که سوریه از روسیه خریداری کرده بود، باید ورود هواپیماهای اسرائیلی به حریم هوایی را شناسایی می‌کردند.

بررسی‌ها نشان داد که اسرائیل یک نرم‌افزار به سیستم دفاعی سوریه وارد کرده بود که روی نمایشگرهای رادار، همه چیز را طبیعی نشان می‌داد. به این ترتیب، در حالی که هواپیماهای اسرائیلی در حریم هوایی سوریه بودند، مقامات نظامی سوری تصاویری از یک شب آرام و بدون حادثه را مشاهده می‌کردند.(Wassmer & Fikus, 2003, p. 1-14)

ب. نمونه هایی از اقدامات دفاعی در برابر حملات سایبری

امروزه بسیاری از کشورها بودجه‌های ویژه‌ای را به سیستم‌های حمله و دفاع سایبری اختصاص داده و تحقیقات گسترده‌ای در این زمینه انجام می‌دهند. پس از چندین حمله جدی به شبکه‌های محرمانه ایالات متحده، پنتاگون و آژانس امنیت ملی این کشور واحدهایی برای جنگ و اطلاعات سایبری ایجاد کردند. این واحدها متخصصان دفاع سایبری را استخدام و آموزش دادند. بریتانیا نیز مرکزی به نام عملیات دفاع سایبری ایجاد کرده که هزاران جاسوس سایبری را در آن به خدمت گرفته است. هدف این مرکز جلوگیری از افشای اطلاعات محرمانه از طریق حملات سایبری است. همچنین، کره شمالی صدها هکر حرفه‌ای که عمدتاً فارغ‌التحصیلان آکادمی‌های نظامی هستند را به کار گرفته تا توان حمله و دفاع سایبری خود را تقویت کند. ایران نیز دارای ارتشی سایبری است که در زمینه حملات و دفاع سایبری فعالیت می‌کند.(Klein et al., 2010)

۶. تکنیک‌های جدید هوش مصنوعی در دفاع سایبری

در دفاع سایبری، تکنیک‌های جدید هوش مصنوعی مانند یادگیری عمیق[۱]، یادگیری تقویتی[۲]، و یادگیری انتقالی[۳] نقش مهمی در شناسایی و دفع حملات پیچیده ایفا می‌کنند. این روش‌ها با تحلیل داده‌های حجیم، شناسایی الگوهای غیرمعمول و پیش‌بینی رفتارهای مشکوک به امنیت سیستم‌ها کمک می‌کنند. (Arnaud, 2021) در ادامه، هر یک از این تکنیک‌ها و کاربردهای آن‌ها در دفاع سایبری به تفصیل بررسی می‌شود:

یادگیری عمیق یکی از شاخه‌های پیشرفته یادگیری ماشین است که بر استفاده از شبکه‌های عصبی مصنوعی با لایه‌های عمیق برای تحلیل داده‌ها تمرکز دارد. این روش‌ها قادرند ویژگی‌های

---

[۱] Deep Learning

[۲] Reinforcement Learning

[۳] Transfer Learning

پیچیده و پنهان داده‌ها را شناسایی کرده و رفتارهای غیرمعمول را کشف کنند. (Ansari, 2022, 119)

شبکه‌های عصبی عمیق می‌توانند برای شناسایی حملات در شبکه‌های رایانه‌ای به‌کار گرفته شوند. این شبکه‌ها با تحلیل لاگ‌های سیستم و جریان داده‌های شبکه، حملات ناشناخته یا پیشرفته را شناسایی می‌کنند .یادگیری عمیق می‌تواند به‌طور خودکار بدافزارهای ناشناخته را از طریق تحلیل فایل‌ها و رفتارهای نرم‌افزاری شناسایی کند .با استفاده از تکنیک‌های یادگیری عمیق، سیستم‌ها می‌توانند رفتار کاربران را مدل‌سازی کرده و در صورت انحراف از رفتار عادی، هشدار دهند. (Mateus, 2021, 876)

یادگیری تقویتی روشی است که در آن یک عامل از طریق تعامل با محیط و دریافت پاداش یا تنبیه یاد می‌گیرد چگونه تصمیم‌های بهینه بگیرد. در دفاع سایبری، این تکنیک برای تصمیم‌گیری خودکار و بهینه‌سازی واکنش‌ها به تهدیدها کاربرد دارد .عامل‌های یادگیری تقویتی می‌توانند حملات را شناسایی کرده و بهترین پاسخ ممکن را (مانند مسدود کردن ترافیک مخرب) انتخاب کنند .**مدیریت پویا در شبکه :**این روش برای تنظیم خودکار قوانین فایروال و سیستم‌های پیشگیری از نفوذ استفاده می‌شود. .با استفاده از یادگیری تقویتی می‌توان حملات سایبری را شبیه‌سازی کرد تا نقاط ضعف سیستم شناسایی شوند. (Maad, 2023)

یادگیری انتقالی روشی است که از دانش یک مدل که برای حل یک مسئله خاص آموزش دیده است، برای حل مسئله‌ای مشابه استفاده می‌کند. این روش می‌تواند زمان و منابع مورد نیاز برای آموزش مدل‌ها را کاهش دهد و کارایی بالایی در مواجهه با تهدیدات جدید ارائه دهد .مدل‌های از پیش آموزش‌دیده می‌توانند برای شناسایی حملات جدید در حوزه‌های مختلف (مانند شناسایی بدافزار در یک نوع سیستم عامل متفاوت) تطبیق داده شوند. از یادگیری انتقالی می‌توان برای انتقال دانش از یک دامنه (مانند شبکه‌های اجتماعی) به دامنه‌ای دیگر (مانند شبکه‌های نظامی) استفاده کرد. سیستم‌های دفاع سایبری می‌توانند با تغییرات سریع در محیط تطبیق پیدا کنند و نیازی به آموزش مجدد از ابتدا نباشد. (Ansari, 2022, 121)

با ترکیب یادگیری عمیق و تقویتی، می‌توان حملات توزیع‌شده جلوگیری از خدمات را سریع‌تر شناسایی و مسدود کرد. تکنیک‌های یادگیری عمیق و انتقالی می‌توانند برای مدل‌سازی رفتارهای معمول شبکه و شناسایی رفتارهای مشکوک استفاده شوند. با استفاده از یادگیری تقویتی، سیستم‌های دفاعی می‌توانند به‌طور خودکار به تهدیدات پاسخ دهند و قوانین امنیتی را بهینه‌سازی کنند.

تکنیک‌های پیشرفته هوش مصنوعی، به‌ویژه یادگیری عمیق، تقویتی، و انتقالی، توانایی بهبود دفاع سایبری در برابر تهدیدات پیچیده و پویا را دارند. این روش‌ها با افزایش دقت، سرعت و خودکارسازی فرآیندها، به سیستم‌ها کمک می‌کنند تا بهتر با حملات سایبری مقابله کنند. با توجه به پیچیدگی و

تنوع تهدیدات سایبری، استفاده از این تکنیک‌ها به‌عنوان یک ابزار ضروری در امنیت سایبری شناخته می‌شود.

۷. روندهای آینده در جنگ سایبری و دفاع سایبری با تأکید بر مهندسی فناوری دفاعی

تحولات فناوری، نقش کلیدی در شکل‌دهی به آینده جنگ سایبری و دفاع سایبری ایفا می‌کنند. با پیشرفت‌های هوش مصنوعی و محاسبات کوانتومی، قابلیت‌های امنیتی و توانایی‌های حمله در فضای سایبری به سطح جدیدی ارتقا خواهند یافت. این پیشرفت‌ها به‌ویژه در حوزه مهندسی فناوری دفاعی تأثیرات عمیقی خواهند داشت، زیرا توسعه و پیاده‌سازی ابزارهای پیشرفته برای دفاع از زیرساخت‌های حیاتی نظامی، اقتصادی و دولتی ضروری است. در این بخش، روندهای آینده در جنگ سایبری و دفاع سایبری بررسی می‌شود و ارتباط آن‌ها با مهندسی فناوری دفاعی توضیح داده خواهد شد.

هوش مصنوعی عمومی سیستمی است که می‌تواند وظایف مختلف را مشابه انسان انجام دهد. در مهندسی فناوری دفاعی، هوش مصنوعی عمومی می‌تواند به‌عنوان یک ابزار همه‌منظوره برای تحلیل، پیشگیری و پاسخ به تهدیدات سایبری عمل کند. هوش مصنوعی عمومی می‌تواند تهدیدات سایبری ناشناخته و پیچیده را شناسایی کند. به‌عنوان مثال، در سامانه‌های دفاعی نظامی، می‌توان از آن برای تحلیل داده‌های ورودی از سنسورها و شناسایی الگوهای حمله استفاده کرد. در شبکه‌های ارتباطی نظامی، هوش مصنوعی عمومی می‌تواند رفتارهای غیرعادی را به‌سرعت شناسایی کرده و پیشنهادات لازم برای بهبود امنیت ارائه دهد. (Mateus, 2021, 882)

در مهندسی فناوری دفاعی، هوش مصنوعی عمومی می‌تواند سیستم‌هایی طراحی کند که قادر به تصمیم‌گیری‌های خودکار و هوشمند در مواجهه با حملات سایبری باشند. این امر به‌ویژه در سیستم‌های کنترل ترافیک نظامی یا پایگاه‌های موشکی اهمیت دارد. هوش مصنوعی عمومی می‌تواند برای طراحی شبیه‌سازی‌های واقع‌گرایانه از حملات سایبری استفاده شود که در آموزش مهندسان امنیت سایبری و توسعه فناوری‌های دفاعی نقش کلیدی دارد. (Achi, 2021)

محاسبات کوانتومی با استفاده از کیوبیت‌ها، امکان انجام محاسبات بسیار پیچیده را در زمانی کوتاه فراهم می‌کند. در مهندسی فناوری دفاعی، این فناوری می‌تواند امنیت سیستم‌ها را به‌طور بنیادین تغییر دهد. سامانه‌های کوانتومی می‌توانند رمزنگاری‌های غیرقابل نفوذ طراحی کنند. برای مثال، پیام‌های ارسال‌شده در شبکه‌های ارتباطی نظامی می‌توانند با استفاده از رمزنگاری کوانتومی، از رهگیری توسط دشمن جلوگیری کنند. مهندسان دفاعی می‌توانند از محاسبات کوانتومی برای تحلیل و شکستن رمزنگاری‌های متخاصمان استفاده کنند. این امر به ارتش‌ها امکان دسترسی به اطلاعات حساس دشمن را می‌دهد. سامانه‌های کوانتومی می‌توانند شبیه‌سازی‌های پیچیده‌ای از حملات سایبری

انجام دهند و به مهندسان کمک کنند تا نقاط ضعف سیستم‌های موجود را شناسایی و برطرف کنند. با توانایی پردازش سریع، محاسبات کوانتومی می‌توانند حملات پیچیده ای را یا را به‌سرعت شناسایی کرده و اقدامات لازم را پیشنهاد دهند .تلفیق قدرت تحلیل و پیش‌بینی هوش مصنوعی عمومی با سرعت پردازش محاسبات کوانتومی می‌تواند راهکاری انقلابی در مهندسی فناوری دفاعی ارائه دهد. این ترکیب می‌تواند سیستم‌هایی بسازد که قادر به شناسایی و پاسخ‌دهی هم‌زمان به تهدیدات پیچیده سایبری باشند. (Achi, 2021)

ترکیب هوش مصنوعی عمومی و کوانتوم می‌تواند سیستم‌هایی بسازد که به‌طور مداوم وضعیت شبکه را تحلیل کرده و در برابر تهدیدات سایبری جدید واکنش نشان دهند. از این فناوری‌ها می‌توان برای نظارت و حفاظت از زیرساخت‌های حیاتی مانند شبکه‌های برق، آب، و حمل‌ونقل استفاده کرد. این ترکیب می‌تواند در طراحی حملات سایبری هوشمند برای مقابله با دشمنان نیز به کار گرفته شود.

روندهای آینده در جنگ و دفاع سایبری به‌طور مستقیم با پیشرفت‌های هوش مصنوعی و محاسبات کوانتومی مرتبط هستند. در مهندسی فناوری دفاعی، استفاده از این فناوری‌ها می‌تواند به طراحی و پیاده‌سازی سیستم‌های پیشرفته‌ای منجر شود که امنیت ملی و بین‌المللی را بهبود می‌بخشند. با این حال، برای بهره‌گیری از این فناوری‌ها، توجه به چالش‌های اخلاقی، قانونی و زیرساختی نیز ضروری است. کشورهای پیشرو باید در کنار سرمایه‌گذاری در این حوزه‌ها، چارچوب‌های مناسب برای استفاده مسئولانه از این فناوری‌ها طراحی کنند.

نتیجه‌گیری

تحلیل سیستم‌های هوش مصنوعی در دفاع سایبری نشان می‌دهد که استفاده از فناوری‌های پیشرفته به یک نیاز اساسی برای مقابله با تهدیدات سایبری پیچیده تبدیل شده است. با توجه به پویایی و پیچیدگی فضای سایبری، روش‌های سنتی به تنهایی قادر به ارائه امنیت کافی نیستند. هوش مصنوعی، با توانایی‌های خود در یادگیری از داده‌های حجیم، شناسایی الگوهای غیرمعمول و ارائه پاسخ‌های خودکار و هوشمند، انقلابی در دفاع سایبری ایجاد کرده است.

تکنیک‌های مختلفی از جمله یادگیری عمیق، یادگیری تقویتی و یادگیری انتقالی به‌طور گسترده برای شناسایی حملات ناشناخته، پیشگیری از نفوذ و بهینه‌سازی پاسخ‌ها به تهدیدات سایبری به کار گرفته می‌شوند. این تکنیک‌ها توانسته‌اند دقت شناسایی و سرعت واکنش در سیستم‌های دفاعی را بهبود دهند. از سوی دیگر، فناوری‌هایی مانند محاسبات کوانتومی و توسعه هوش مصنوعی عمومی، نویدبخش تحولات آینده در مهندسی فناوری دفاعی هستند.

با این حال، چالش‌هایی از جمله هزینه‌های توسعه، پیچیدگی پیاده‌سازی، و مخاطرات اخلاقی و امنیتی، نیازمند توجه ویژه هستند. بهره‌گیری هوشمندانه از این فناوری‌ها می‌تواند زیرساخت‌های

حیاتی را در برابر حملات محافظت کرده و امنیت جهانی را تقویت کند.

در نهایت، تقویت تحقیقات در حوزه دفاع سایبری، آموزش نیروهای متخصص، و توسعه چارچوب‌های حقوقی و اخلاقی برای استفاده مسئولانه از فناوری‌های پیشرفته از ضروریات است. تنها با یک رویکرد جامع و هماهنگ می‌توان از این فناوری‌ها برای مقابله با تهدیدات سایبری و ایجاد محیطی امن در فضای دیجیتال استفاده کرد.

منابع

1. Achi, A., Kuwunidi Job, G., Shittu, F., Baba Atiku, S., Unimke Aaron, A., & Zahraddeen Yakubu, I. (2021). SEE PROFILE Survey On The Applications Of Artificial Intelligence In Cyber Security. Survey On The Applications Of Artificial Intelligence In Cyber Security Article in International Journal of Scientific & Technology Research. www.ijstr.org.
2. Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The Impact and Limitations of Artificial IntelligenceinCybersecurity:ALiteratureReview.IJARCCE,11(9).https://doi.org/10.17148/ijarcce.2022.11912.
3. Arnaud, Matos, Artificial Intelligence as a Support Tool to Cyber security Activities,(2022), Advanced Research on Information Systems Security, an International Journal (ARIS2Volume 2, No 1, pp 02-12.
4. Cannady, J. (1998). Artificial neural networks for misuse detection. *Proceedings of the 1998 National Information Systems Security Conference (NISSC'98)*, Arlington, VA, 443–456.
5. Chatzigiannakis, V., Androulidakis, G., & Maglaris, B. (2004). A distributed intrusion detection prototype using security agents. *HP OpenView University Association*.
6. Dickerson, J. E., & Dickerson, J. A. (2000). Fuzzy network profiling for intrusion detection. *NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society*, Atlanta, 301–306.
7. Dickerson, J. E., Juslin, J., Koukousoula, O., & Dickerson, J. A. (2001). Fuzzy intrusion detection. *IFSA World Congress and 20th North American Fuzzy Information Processing Society (NAFIPS) International Conference*, Vancouver, British Columbia, 3, 1506–1510.
8. Fei, B., Eloff, J., Olivier, M. S., & Venter, H. (2006). The use of self-organizing maps for anomalous behavior detection in a digital investigation. *Forensic Science International*, 162, 33–37.
9. Iftikhar, B., & Alghamdi, A. S. (2009). Application of artificial neural network in detection of DOS attacks. *Proceedings of the 2nd International Conference on Security of Information and Networks (SIN '09)*, ACM, New York, NY, 229–234.
10. Ilgun, K., Kemmerer, R., & Porras, P. (1995). State Transition Analysis: A Rule-Based Intrusion Detection System. *Software Engineering*, 21(3), 181–199.
11. Kivimaa, J., Ojamaa, A., & Tyugu, E. (2009). Graded Security Expert System. *Lecture Notes in Computer Science*, 5508, 279–286.
12. Lee, K., & Mikhailov, L. (2004). Intelligent intrusion detection system. *Second IEEE International Conference on Intelligent Systems*, 2, 497–502.

13. Lunt, T. F., & Jagannathan, R. (1988). A Prototype Real-Time Intrusion-Detection Expert System. *Proceedings of the IEEE Symposium on Security and Privacy*, 59.
14. Maad M. Mijwil1, Mohammad Aljanabi2,4, ChatGPT)2023) January2023; Accepted January 2023; Available online January 2023.
15. Murali, M., & Rao, P. (2005). A survey on intrusion detection approaches. *First International Conference on Information and Communication Technologies*, IEEE Communications Society Press, 233–240.
16. N. Mateus-Coelho, M. Cruz-Cunha, and P. Silva-Ávila, "Application of the industry 4.0 technologies to Mobile Learning and Health Education Apps," FME Transactions, vol. 49, no. 4, pp. 876–885, 2021.
17. Norvig, P., & Russell, S. (2000). *Artificial Intelligence: Modern Approach*. Prentice Hall.
18. Rosenblatt, F. (1957). The perceptron—a perceiving and recognizing automaton. *Cornell Aeronautical Laboratory Report 85-460-1*.
19. Sağıroğlu, ġ., & Alkan, M. (2005). *Her yönüyle elektronik imza (e-imza)*. Grafiker Yayınları.
20. Salvador, P. (2009). Framework for zombie detection using neural networks. *Fourth International Conference on Internet Monitoring and Protection (ICIMP)*.
21. Shankarapani, M., Kancherla, K., Ramammoorthy, S., Movva, R., & Mukkamala, S. (2010). Kernel machines for malware classification and similarity analysis. *WCCI 2010 IEEE World Congress on Computational Intelligence*, Barcelona, Spain, 2504–2509.
22. Stopel, D., Boger, Z., Moskovitch, R., Shahar, Y., & Elovici, Y. (2006). Application of artificial neural networks techniques to computer worm detection. *International Joint Conference on Neural Networks (IJCNN)*, 2362–2369.
23. Sundaram, A. (1996). An introduction to intrusion detection. *Crossroads: The ACM Student Magazine*, New York, USA, 2(4), 3–7.Tyugu, E. (n.d.). Artificial Intelligence in Cyber Defence. *IEEE Xplore*.
24. Wu, C. H. (2009). Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks. *Expert Systems with Applications*, 36(3), Part 1, 4321–4330.