FRL The Fundamental Researches in Law
The first scientific/specialist publication
Islamic Azad University, Rafsanjan branch
three volume / spring 2024
The Fundamental Research In Law

Artificial intelligence and its impact on cyber security and the right to privacy

Amir reza mahmoodi , Maryambahr kazemi

DateReceived :***20224/3/28*** DateAccepted : ***2024/5/9***

Abstract:

Artificial intelligence has emerged as a key component of cyber security due to its ability to assess security threats in real-time and take appropriate action. Artificial intelligence is now more influential in identifying and stopping attacks that keep businesses on the cutting edge. Identifying and preventing threats is the main role of artificial intelligence in cyber security. If cyber-attacks and attacks are carried out using artificial intelligence algorithms, defense against them requires more advanced technologies, and using them to collect and analyze data may lead to the violation of users› privacy. It may also in some cases not be able to correctly predict how a cyber-attack will be carried out, which can lead to a decrease in cyber security. Research on improving the capabilities of artificial intelligence to detect and prevent cyber-attacks, identify suspicious patterns and behaviors, and implement effective security measures can create significant improvements in cyber security. Also, examining data analysis in order to identify unusual patterns and behaviors of users. It can help in the early detection of cyber-attacks and their prevention, and promoting the use of advanced encryption technologies to protect data and prevent unauthorized access to them can make significant improvements in cyber security. One of the main findings from the research on the impact of artificial intelligence on increasing cyber security and data protection is that the use of artificial intelligence can provide significant improvements in the detection, prevention and management of cyber-attacks, and through big data analysis, identifying suspicious patterns, and implementing security measures. Automating and improving intrusion detection systems can provide significant improvements in cybersecurity and help reduce security risks online.

Keywords: : artificial intelligence, cyber security, data protection, threat detection، Human Rights

پژوهش های بنیادین در حقوق
اولین نشریه علمی/تخصصی حقوق
دانشگاه آزاد اسلامی واحد رفسنجان
شماره سوم /بهار ۱۴۰۳
FRL
پژوهش های بنیادین در حقوق

هوش مصنوعی وتاثیر آن بر امنیت سایبری وحق بر حریم خصوصی

امیر رضا محمودی[۱] ، مریم بحر کاظمی[۲]

تاریخ دریافت: ۱۴۰۳/۱/۹ تاریخ پذیرش :۱۴۰۳/۲/۰۲

چکیده:

هوش مصنوعی به دلیل توانایی آن در ارزیابی تهدیدات امنیتی در زمان واقعی و انجام اقدامات مناسب، به عنوان یک جزء کلیدی امنیت سایبری ظاهر شده است. هوش مصنوعی اکنون تأثیر بیشتری در شناسایی و توقف حملاتی دارد که کسب وکارها را در لبه پیشرفت نگه می دارد. شناسایی و پیشگیری از تهدید، محوراصلی نقش هوش مصنوعی در امنیت سایبری است. اگر تهاجم‌ها و حملات سایبری با استفاده از الگوریتم‌های هوش مصنوعی صورت گیرد، دفاع در برابر آن‌ها نیازمند تکنولوژی‌های پیشرفته‌تری است و استفاده از آن برای جمع‌آوری و تحلیل داده‌ها ممکن است به نقض حریم خصوصی کاربران منجر شود. همچنین ممکن است؛ در برخی موارد نتواند به درستی پیش‌بینی کند که چگونه یک حمله سایبری انجام خواهد شد؛ این مسئله می‌تواند به کاهش امنیت سایبری منجر شود. تحقیقات بر روی ارتقاء توانایی‌های هوش مصنوعی برای تشخیص و پیشگیری از حملات سایبری، شناسایی الگوها و رفتارهای مشکوک و اجرای تدابیر امنیتی مؤثر می‌تواند بهبود قابل توجهی در امنیت سایبری ایجاد کند. همچنین بررسی تجزیه و تحلیل داده‌ها به منظور شناسایی الگوها و رفتارهای غیرعادی کاربران، می‌تواند به تشخیص زودرس حملات سایبری و پیشگیری از آن‌ها کمک کند و ترویج استفاده از فناوری‌های رمزنگاری پیشرفته برای حفاظت از داده‌ها و جلوگیری از دسترسی غیرمجاز به آن‌ها می‌تواند بهبود قابل توجهی در امنیت سایبری ایجاد کند.

یکی از یافته‌های اصلی تحقیقات در زمینه تاثیر هوش مصنوعی بر افزایش امنیت سایبری و حفاظت از داده‌ها این است که هوش مصنوعی می‌تواند؛ بهبود چشمگیری در تشخیص، پیشگیری و مدیریت حملات سایبری فراهم کند و از طریق تحلیل داده‌های بزرگ، شناسایی الگوهای مشکوک، اجرای تدابیر امنیتی خودکار و بهبود سیستم‌های تشخیص نفوذ، بهبود قابل توجهی در امنیت سایبری ایجاد کند و به کاهش خطرات امنیتی حریم خصوصی افراد در فضای آنلاین کمک کند.

واژگان کلیدی: هوش مصنوعی، امنیت سایبری، حفاظت از داده، شناسایی تهدید، حقوق بشر

۱- - امیررضا محمودی،دانشیارگروه تخصصی حقوق ، واحد لاهیجان،دانشگاه آزاد اسلامی ،لاهیجان،ایران.
amirreza.mahmodi@gmail.com
۲- مریم بحرکاظمی،دانشجودکتراگروه حقوق،واحد لاهیجان،دانشگاه آزاد اسلامی،لاهیجان،ایران
gmail.com@Maryambahrekazemi۲۰۱

مقدمه

هوش مصنوعی برای افراد مختلف معانی متفاوتی دارد. از نظر برخی هوش مصنوعی به معنی شکل مصنوعی زندگی است که میتواند انسان ها را هوشمند کند و برای برخی یک تکنولوژی پردازش داده هاست.[۱] پیش بینی می شود هوش مصنوعی در طی حدود یک دهه دیگر به طور عمده در همه سیستم ها و ابزارهای اصلی مدنی نفوذ کند و پایگاه نرم افزاری آنها را ایجاد کند و طی دو تا سه دهه دیگر سبک و سیاق دنیا را دگرگون کند. هنگام در نظر گرفتن حکمرانی، تمرکز نباید فقط بر فناوری باشد، بلکه باید بر ساختارهای اجتماعی پیرامون آن شامل: سازمان ها، افراد و مؤسساتی که آن را ایجاد می کنند، توسعه واستقرار می دهند، استفاده و کنترل می کنند و همچنین افرادی که تحت تأثیر آن قرارمی گیرند؛ مانند شهروندان در رابطه با دولت ها، مصرف کنندگان، کارگران یا حتی کل جامعه نیز متمرکز شود.[۲]

هوش مصنوعی به یک فناوری جدی در مبارزه با جرایم سایبری تبدیل شده است. راه حل های امنیت سایبری مبتنی بر هوش مصنوعی می توانند تهدیدها را در زمان واقعی شناسایی و از آن جلوگیری کنند. این اقدامات می توانند به سازمان ها کمک کنند تا از تهدیدات سایبری در امان بمانند.[۳] جرایم سایبری به سرعت در حال رشد است و اقدامات امنیتی سنتی دیگر برای محافظت در برابر تهدیدات سایبری پیشرفته کافی نیست [۴]. هوش مصنوعی یک فناوری حیاتی برای امنیت سایبری است زیرا می تواند؛ تهدیدات را تجزیه و تحلیل و شناسایی کند، حملات آینده را پیشبینی کند و اقدامات پاسخ را به صورت خودکار انجام دهد. راه حل های امنیت سایبری مبتنی بر هوش مصنوعی می توانند از یادگیری ماشین والگوریتم های یادگیری عمیق برای تجزیه و تحلیل استفاده کنند. امنیت سایبری و حفاظت از داده‌ها از جمله مسائل حیاتی و حساس در دنیای امروز است که با گسترش استفاده از فناوری‌های اطلاعات و ارتباطات، تبادل داده‌ها و اطلاعات حساس در فضای آنلاین رو به افزایش است. این پژوهش می‌تواند بهبود چشمگیری در حفظ امنیت سایبری و جلوگیری از حملات نفوذی و دسترسی غیرمجاز به داده‌ها ایجاد کند. این امر به تدابیر امنیتی بهتر، شناسایی سریع تهدیدات و پاسخگویی سریع‌تر به حملات کمک خواهد کرد. همچنین می‌تواند بهبود در فناوری‌های حفاظت از داده‌ها، رمزنگاری قوی‌تر و مکانیزم‌های خودکار برای تشخیص و جلوگیری از نقض امنیت داده‌ها فراهم کند و استفاده از آن برای تحلیل داده‌های سایبری و شناسایی الگوهای غیرعادی می‌تواند به سازمان‌ها و افراد کمک کند؛ تا تصمیم‌گیری‌های بهتر و سریع‌تر در خصوص امنیت و حفاظت داده‌ها انجام دهند و کاهش خطرات حملات سایبری و پیشگیری از خسارات مالی ناشی از آن‌ها را فراهم کند. هوش مصنوعی اکنون تأثیر بیشتری در شناسایی و توقف حملاتی دارد که کسب وکارهارا در لبه پیشرفت نگه می دارد. شناسایی و پیشگیری از تهدید، محور اصلی نقش هوش مصنوعی در امنیت سایبری است. هوش مصنوعی می تواند روندها و ناهنجاری ها را در ترافیک شبکه و رفتار کاربر که ممکن است؛ نشان دهنده یک حمله سایبری بالقوه از طریق استفاده از الگوریتم های یادگیری ماشینی و تجزیه وتحلیل داده های پیشرفته باشد، شناسایی کند.

در مقاله ای با عنوان به سوی امنیت سایبری مبتنی بر هوش مصنوعی و راه های مبارزه با جرایم سایبری نوشته شده[۵] ، مهم ترین شیوه ها، صحیح ترین روشها و راهبردهای خوب برای جلوگیری از جرایم سایبری در یک محیط دیجیتالی که انتقال داده ها بین دستگاه های

۱- ابوذری، مهرنوش ۱۴۰۱ حقوق و هوش مصنوعی، تهران میزان،ص۱۴.

۲- Srivastava et al، ۲۰۲۱,۱۱

۳- Shamiulla, ۲۰۱۹,۱۸

۴- Mijwi ۲۰۲۳,et al, نقل از

۵- General Data Protection Regulation.

الکترونیکی را به صورت ایمن و بدون حضور نرم افزارهای مخرب تضمین می کند، بررسی می شود. این گزارش به این نتیجه رسیده که رویه های ارائه شده توسط امنیت سایبری ضروری است و باید مراقبت وتوسعه یابد اما در این مقاله شناسایی تهدیدات به وسیله هوش مصنوعی و روند امنیت سایبری به دقت تشریح نشده است .

در مقاله دیگری باعنوان چالش های حفاظت از داده ها در عصرهوش مصنوعی که توسط,۲۰۲۱ نوشته شده است؛ چگونگی استفاده از هوش مصنوعی را از منظر حفاظت از داده ها تشریح کرده، و به ویژه نگرانیهای اصلی حفاظت از داده ها و علاوه بر این نوع خطراتی که هوش مصنوعی برای محافظت از داده ها ایجاد میکند را بیان کرده است. هدف این مقاله ارائه بینشی در مورد رویکرد حفاظت از داده برای هوش مصنوعی است. اما در این مقاله الزامات[1] امنیتی داده های شخصی در استفاده از هوش مصنوعی را مورد بحث قرار نداده و همچنین به بررسی نقاط قوت وضعف استفاده از هوش مصنوعی در حفاظت از داده ها و امنیت سایبری نپرداخته است؛ بلکه در این پژوهش به طور کامل روند امنیت سایبری و کاربرد هوش مصنوعی در حفاظت از داده ها بررسی شده و فقط به شناسایی نقاط قوت وضعف استفاده از هوش مصنوعی در این حوزه می پردازد.

به نظر می رسد؛ استفاده از تکنولوژی هوش مصنوعی می‌تواند بهبود چشمگیری در حفاظت از داده‌ها و افزایش امنیت سایبری ایجاد کند. با توجه به قابلیت‌های پردازش داده، تحلیل الگوها، شناسایی تهدیدات و پاسخگویی سریع به حملات، هوش مصنوعی می‌تواند به صورت خودکار و هوشمند به ارتقاء امنیت سایبری کمک کند.

هدف از این پژوهش تبیین تاثیرات هوش مصنوعی بر حفاظت از داده ها و افزایش امنیت سایبری است بنابراین در این پژوهش عناوینی چون، سیستم هوش مصنوعی، هوش مصنوعی در زمینه حفاظت از داده ها، الزامات امنیتی داده های شخصی در استفاده از هوش مصنوعی، الزامات در استفاده از هوش مصنوعی برای پردازش داده های شخصی، روند امنیت سایبری، هوش مصنوعی در امنیت سایبری و شناسایی تهدید به وسیله هوش مصنوعی مورد مطالعه قرارمی گیرد. در واقع ما به دنبال پاسخگویی به چگونگی تاثیر هوش مصنوعی بر امنیت سایبری و حفاظت از داده ها در حریم خصوصی هستیم.

۱- General Data Protection Regulation.

۱ – سیستم هوش مصنوعی

قدمت هوش مصنوعی به دهه ۱۹۵۰ می رسد و پیشرفت های اخیر فناوری هوش مصنوعی بر رشد نوآوری و اتوماسیون در تولید، تأثیر گذاشته است. علیرغم مزایای ذاتی فناوری های هوش مصنوعی، استفاده ازاین تکنیک ها بحث هایی را در مورد استفاده از آنها به روش های مخرب برانگیخته است[۱] . هوش مصنوعی رشته ای از علوم کامپیوتر است که نظریه ها، روش ها، تکنیک ها و سیستم هایی را برای شبیه سازی و گسترش عقل انسان به ماشین ها توسعه می دهد. هدف هوش مصنوعی اعطای هوش انسانی به ماشین هاست. ماهیت هوش مصنوعی مبتنی بر زمینه ای است که هوش انسانی را می توان با دقت توصیف کرد و امکان تکرار آن توسط ماشین ها ویا نرم افزار را فراهم کرد. اصطلاح «هوش مصنوعی» به طور بالقوه طیف گسترده ای از فناوری را در بر می گیرد، اما معمولاً به سیستم هایی اطلاق می شود که دستورالعمل های از پیش برنامه ریزی شده را دنبال نمی کنند و در عوض خودشان یاد می گیرند. یکی از پیامدهای یادگیری و برنامه ریزی نشدن این می باشد که ممکن است مشخص نگردد سیستم چگونه به تصمیم گیری می رسد. این سیستم در یک «جعبه سیاه» عمل می کند و یک سیستم غیرقابل نفوذ است[۲] .هنگامی که کار نرم افزار مورد استفاده برای عملکرد یک سیستم را نمی توان به راحتی ارزیابی یا بررسی کرد، خطاهای سیستم می توانند تا زمانی که باعث ایجاد مشکلات جدی یا آسیب های بیش از حد به طرف های درگیر شوند؛ بدون توجه و کشف نشده باقی بمانند[۳] . همچنین ممکن است؛ عواقب آن محدود به هزینه های بررسی و تعمیر خطاهای نرم افزاری نباشد، زیرا گاهی اوقات جبران خسارات غیرممکن است. خطا در یک الگوریتم ممکن است از داده های ورودی ناشی شود، زمانی که جزئیات مربوط به مجموعه داده شناسایی نشود[۴] . سیستم هوش مصنوعی ممکن است در یک محیط توسعه یافته کاملاً کار کند اما در دنیای واقعی غیرقابل پیش بینی یا غیرقابل اعتماد می شود. این موضوع نگرانی های حقوقی زیادی را ایجاد می کند. الگوریتم اساسی هستند.ممکن است اتخاذ تصمیماتی باشد که مغرضانه یاتبعیض آمیز و ناقض الزامات عادلانه گس چشم انداز تهدید شامل چندین عنصر است. مهاجمان به دنبال انواع مختلفی از آسیب پذیری ها برای راه اندازی حملات خود هستند که این حملات شامل پیچیدگی و تهدیدات مداوم پیشرفته، اقدامات مخرب در فضای سایبری و کسب درآمد از جرایم سایبری است. جامعه امنیت سایبری باید بداند که چگونه می توان از هوش مصنوعی برای حملات سایبری استفاده کرد و نقاط ضعف آن را برای اجرای اقدامات دفاعی شناسایی کرد[۵]. هوش مصنوعی می‌تواند در ارتقای حقوق بشر و آزادی‌های اساسی نقش مثبتی داشته باشد اما در عین حال، ممکن است منجر به نقض آنان نیز شود. بنابراین، لازم است قوانین و مقررات مناسب برای استفاده از هوش مصنوعی در جامعه تدوین شود تا حقوق

۱- -Revilla,۲۰۱۶,۳۰ Vietnam ۳۰ years after Doi Moi: Achievements And Challenges', Zeitschrift für Wirtschaftsgeographie.Retrievedfrom:https://www.researchgate.net/publication/۳۰۹۴۴۹۷۷۹_Vietnam_۳۰_years_after_Doi_Moi_Achievements_and_challenges [accessed ۱۲ December ۲۰۲۲

۲- Yoshua,۲۰۱۳,۲۳ Deep Learning of Representations: Looking Forward' in Dediu A., Martín-Vide C., Mitkov R., and Truthe B. (eds.), Statistical Language and Speech Processing: First International Conference,

Kaloudi۲۰۲۰,۵۳ Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things, ۱)۱). https://doi.org/۱۰,۱۰۰۷/s٤-۰۰۰۰۱-۰۲۰-٤۳۹۲٦

۳- - Novikov ,۲۰۱۹ How AI can be applied to cyberattacks. Retrieved Novemb. ۲۰۱۹ ,۲۵.

۴- مصطفوی اردبیلی وهمکاران ،۱۴۰۱، ص۴۹.

۵- REGULATION (EU) ۲۰۱٦

یعنی از جهت اینکه شرکت را طرف دعوی قرار دهند یا مدیران را دچار سردرگمی هستند. حال در این صورت وقتی مدیران در مقام نماینده موارد مقرر شده قانونی و قراردادی فیمابین خود و شرکت را رعایت کرده باشند؛ چنین عقدی صحیح و نافذ خواهد بود. لذا شخص ثالث علیه شرکت طرح دعوی خواهد کرد در غیر این صورت ماهیت عقد فضولی خواهد بود و امکان مراجعه به شرکت نیست. البته همیشه اینگونه نیست. یعنی بعضاً قانون برای حمایت حقوق اشخاص ثالث اقدام می کند و حتی در صورت عدم رعایت موازین قانونی از سوی مدیران، شخص ثالث می‌تواند همچنان به شرکت مراجعه نماید. به هر ترتیب با بررسی ماهیت عقود منعقد شده از سوی مدیران با اشخاص ثالث تکلیف اشخاص ثالث مشخص خواهد شد تا به چه شخص یا اشخاصی جهت احقاق حق خود مراجعه نمایند و در صورت فضولی بودن عقد و عدم رعایت موازین از سوی مدیر، مسئولیت مدیر در قبال اشخاص ثالث و همچنین شرکت نیز مشخص خواهد گردید.

۲ – هوش مصنوعی در زمینه حفاظت از داده ها

مقررات پارلمان اروپا و شورای مقررات عمومی حفاظت از داده ها؛ که از این پس به عنوان نامیده می شود؛ به معنای هرگونه اطلاعات مربوط به یک شخص حقیقی شناسایی شده یا قابل شناسایی است. [۱]. علاوه بر این، مقررات حفاظت از داده ها ی عمومی صراحتاً مدت نمایه سازی را در ماده ٤ مشخص می کند. به نظر می رسد فناوری قادر به استنباط ویژگی های شخصی خاص بر اساس داده هایی است که به طور آنی به آن مربوط نمی شود[۲] . به همین دلیل، بسیار مهم است که داده های مورد استفاده به عنوان مبنای الگوریتم یادگیری مناسب باشد تا از تحریف، سوگیری و تبعیض جلوگیری شود. با وجود این واقعیت که پردازش دسته های خاصی از داده های شخصی (مانند نژاد، عقاید سیاسی، اعتقادات مذهبی، عضویت در اتحادیه های کارگری و پردازش داده های ژنتیکی، داده های بیومتریک به منظور شناسایی منحصربه فردیک شخص حقیقی، داده های مربوط به سلامتی جنسی و ...) بر اساس ماده ۹ مقررات حفاظت از داده ها ی عمومی ممنوع است، الگوریتم ها می توانند این اطلاعات را از طریق داده های دیگر با رعایت مرزهای حریم خصوصی استخراج کنند.[۳] طبق ماده ۲۲ مقررات حفاظت از داده های عمومی موضوع داده ها این حق را خواهد داشت که تنها بر اساس پردازش خودکار، از جمله نمایه سازی، تحت تصمیم گیری قرار نگیرد. بنابراین افراد ممکن است به هر نوع پردازش داده های .خود که بدون نظارت یا دخالت انسانی انجام می شود؛ اعتراض کنند

مطابق با مواد۱۵–۱۳ مقررات حفاظت از داده ها ی عمومی مربوط به اطلاعات ودسترسی به داده های شخصی، کلیه سازمان هایی که قصد دارند داده ها را در الگوریتمی قرار دهند که پس از آن تصمیمی در مورد یک فرد اتخاذ می کند، موظف اند به فرد اطلاع دهند که در چنین مواردی پردازش صورت خواهد گرفت. بر اساس مفاد مقررات حفاظت از داده های عمومی، تصمیم گیری فردی خودکار تحت ممنوعیت کامل نیست، برخی ازاستثنائات در ماده ۲۲ (بند۲) تعیین شده است: «این نوع تصمیم گیری برای انعقاد یا اجرای قرارداد بین طرفین ضروری است. موضوع داده و یک کنترل کننده داده؛ توسط قانون اتحادیه یا کشور عضو، مجاز است. همچنین رضایت صریح موضوع داده به تصمیم گیری خودکار داده شده است. داده کاوی می تواند برای ایجاد پروفایل های دیجیتالی مورد استفاده قرار گیرد و اجازه می دهد تا تصمیمات اساسی بدون اطلاع افراد گرفته شود[٤]. اگر داده های حاصل جنبه شخصی فرد را نادرست نشان دهند، یا داده ها رفتارهای فرد را بیش از حد غیر واقعی نشان دهند، چنین داده هایی تا حد زیادی از انتظارات شخص برای حفظ حریم خصوصی تجاوز می کنند؛ همچنین .تصمیمات خودکار، ارزیابی معقول دیگران از فردرامخدوش می کند[٥]

۱-REGULATION (EU) ۲۰۱٦

۲- todoli-signes۲۰۱۸,۳۳ A., Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection, June ۲۰۱۸ ,۳۰, in:Transfer: European Review of Labour and Research, ,(٤) ۲٥ ۲۰۱۹ ,۱۷-۱. (Retrieved from https://ssrn.com/abstract=۲۰۲۱ .۰۱ .۱٥ – ۳۳۱٦٦٦٦.)

۳- -ISHII,۲۰۱۹,٥۳۳ Comparative legal study on privacy and personal data protection for robots equipped with rtificial intelligence: looking at functional and technological aspects, in: AI & Society, ۲۰۱۹ ,٥۳۳-٥۰۹ ,۳٤.

۴- -Hildebrandt,۲۰۱۰,۲۲ The Challenges of Ambient Law and Legal Protection in the Profiling Era,in: Modern Law Review,٤٦۰-٤۲۸ ,(۳) ۷۳, May ۲۰۱۰ ,۷. (Retrieved from https://onlinelibrary.wiley.com/doi/full/۱۰,۱۱۱۱/j.۲۲۳۰,۲۰۱۰,۰۰۸۰٦-۱٤٦۸.x – ۲۰۲۱ .۰۲ .۱۸.)

۳ – حقوق حفظ حریم خصوصی و حفاظت از داده ها

بر اساس ماده ۷و ۸ منشور حقوق اساسی اتحادیه اروپا هرکس حق دارد از اطلاعات شخصی مربوط به خود محافظت کند. چنین داده هایی باید به طور منصفانه برای اهداف مشخص و بر اساس رضایت شخص مربوطه یا هر مبنای قانونی دیگری که توسط قانون تعیین شده است؛ پردازش شود. همچنین هر کس حق دارد به داده هایی که در مورد او جمع آوری شده است؛ دسترسی داشته باشد و حق اصلاح آن را دارد. حریم خصوصی یک حق اساسی است که برای کرامت انسانی ضروری است و امروزه بسیاری از دولتها و مناطق، حق اساسی برای حفاظت از داده ها را به رسمیت می شناسند.

حفاظت از داده ها در درجه اول محافظت از هر گونه اطلاعات شخصی مربوط به شخص است که این موضوع، ارتباط نزدیکی باحق حریم خصوصی دارد و حتی میتواند بخشی از حق حریم خصوصی در سیستم حقوق بشر سازمان ملل باشد[۱]. سیستم های هوش مصنوعی اغلب از طریق دسترسی و تجزیه و تحلیل مجموعه های کلان آموزش داده می شوند. داده ها به منظور ایجاد مکانیسم های بازخورد و ارائه کالیبراسیون و اصلاح مستمر جمع آوری میشوند. این مجموعه داده ها با حفظ حقوق حریم خصوصی و حفاظت از داده ها تداخل دارد و همچنین تجزیه و تحلیل داده ها با استفاده از سیستمهای هوش مصنوعی ممکن است اطلاعات خصوصی افراد را نشان دهد. اطلاعاتی که به عنوان اطلاعات محافظت شده واجد شرایط هستند و باید به عنوان اطلاعات حساس تلقی شوند. حتی اگر از مجموعه داده های بزرگی که از اطلاعات در دسترس عموم تغذیه می شوند مشتق شده باشند. نمونه دیگری از خط باریک، بین داده های عمومی و خصوصی افزایش استفاده از برنامه های نظارت بر رسانه های اجتماعی دولتی است که در آن سازمانهای مجری قانون مجموعه ای از اطلاعات رسانه های اجتماعی را جمع آوری می کنند و آنها را به برنامه های مبتنی بر هوش مصنوعی برای شناسایی تهدیدات ادعایی .می رسانند

حق اطلاعات و حق دسترسی با همکاری کار می کنند تا به افراد اجازه دهند اطلاعاتی در مورد داده هایی که یک نهاد در حال جمع آوری آن است؛ به دست بیاورند که چگونه آنها را جمع آوری می کند و چگونه از آن استفاده خواهد کرد .این حقوق، آگاهی عمومی را در مورد وجود سیستم های هوش مصنوعی و نقشی که ایفا می کنند، افزایش می دهند. علاوه بر این، چنین حقوقی به افراد اجازه می دهند تا آسیب های حقوق بشری احتمالی را کشف و درک کنند و موجب شفافیت بیشتر در مورد .نحوه استفاده از هوش مصنوعی شوند

حق اصلاح به افراد این امکان را میدهد تا در صورت نادرست یا ناقص بودن اطلاعات خود، که توسط یک شخص ثالث نگهداری می شود، آنها را اصلاح کنند. این حق میتواند به کاهش تأثیر نرخ خطا در .سیستمهای هوش مصنوعی کمک کند

حق محدود کردن پردازش به افراد این امکان را میدهد که از یک نهاد درخواست کنند تا استفاده از اطلاعات شخصی را متوقف کند یا استفاده از آنها را محدود کند. این حقوق می تواند برای توقف موقت استفاده از یک سیستم هوش مصنوعی مورد بحث یا برای تحت فشار قرار دادن یک نهاد برای .استفاده مسئولانه تر از سیستم هوش مصنوعی مورد استفاده قرار گیرد[۲]

۱- Masse۲۰۱۸,۱۱.

۲- Gerke, S., Minssen, T., & Cohen, G. (۲۰۲۰). Ethical and legal challenges of artificial intelligence-driven healthcare. In A. Bohr & K. Memarzadeh (Eds.), Artificial Intelligence in Healthcare (pp. ۳۳٦–۲۹٥). Academic Press. ISBN: ۹۷۸۰۱۲۸۱۸٤۳۸۷. https://doi.org/۱۰,۱۰۱٦/B٥-۷,۰۰۰۱۲-۸۱۸٤۳۸-۱۲-۰-۹۷۸

مهم نیست که سیستم های هوش مصنوعی چقدر دقیق تولید می شوند، باید تلاش کنیم تا مطمئن شویم که ارزش های آن ها با ارزش های ما همسو هستند تا هر گونه عارضه ای که از یک ابرهوش ممکن است ساطع شود تا حد امکان کاهش یابد. این که امروزه مشکل همسویی ارزش باید حل شود، توسط اصول راهنمای سازمان ملل در مورد تجارت و حقوق بشر که برای ادغام حقوق بشر در تصمیمات تجاری ایجاد شده است نیز اشاره شده است [۱]. هر جا که هوش مصنوعی باعث آسیب شود، باید مشخص شود که چرا چنین می کند و جایی که یک سیستم هوش مصنوعی در تصمیم گیری قضایی دخالت دارد، استدلال آن باید توسط حسابرس انسانی قابل تأیید باشد. چنین اصولی به نگرانی هایی پاسخ می دهد که هوش مصنوعی ممکن است با سرعت زیادی داده ها را استدلال کند و به طیفی از داده ها دسترسی داشته باشد که تصمیمات مبتنی آن به طور فزاینده ای مبهم باشد، و اگر تحلیل هایش به بیراهه رفتند، تشخیص آن غیرممکن می شود. این اصول همچنین بر همسویی ارزش پافشاری می کنند و تأکید می کنند که «سیستم های هوش مصنوعی بسیار خودمختار، باید طوری طراحی شوند که بتوان اهداف و رفتارهای آن ها را برای همسویی با ارزش های انسانی در طول عملیاتشان تضمین کرد»[۲]. با توجه به نفش عظیم تأثیر هوش مصنوعی بر زندگی فردی و اجتماعی شهروندان، هوش مصنوعی در محدوده رژیم های حقوقی در چند بخش خاص قرار می گیرد. این رژیم ها، قانون حمایت از داده ها، قانون حمایت از مصرف کننده و قانون رقابت را شامل می شود. اگرچه همانطور که اشاره شد، هوش مصنوعی وارد یک فضای قانونی تنظیم شده می شود، اما تأثیرات اجتماعی فراگیر و گاهی مخل آن همیشه با پاسخ های قانونی کافی مواجه نمی شود. بنابراین، مسائل مربوط به هوش مصنوعی ممکن است پیشنهادهایی را برای تغییرات قانونی ایجاد کند. چنین پیشنهادهایی معمولاً شناسایی آنچه در قوانین و رویه های حقوقی فعلی ناکافی است را با پیشنهادهایی برای تغییر ترکیب می کند. تغییر در قانون ممکن است از طریق ملاحظات اخلاقی(احتمالاً پیوند دادن اخلاق با اصول حقوقی) یا با توسل به اهداف اجتماعی یا سیاسی که در میان اقشار عمومی و فاعلان سیاسی مشترک است، استدلال شود[۳]. به عنوان مثال، ممکن است قانون استفاده از هوش مصنوعی را برای تشخیص چهره در فضاهای عمومی ممنوع کند، یا اینکه اقتصاد باز ایجاب می کند که قانون اجازه استفاده گسترده تر ازداده های شخصی را برای اهداف یادگیری ماشینی بدهد یا اینکه برای قوانین مربوط به مسئولیت مدنی نیاز باشد.

۱- Mathias Risse ۲۰۱۸,۷

۲- -Lauren Goode(۲۰۱۸)"Facial recognition software is biased towards white men, researcher finds," thVerge,https://www.theverge.com/۱۷۰۰۱۲۱۸/۱۱/۲/۲۰۱۸/facial-recognition-software-accuracytechnology-mit-white-men-black-women-error

۳- -Sartor,۲۰۲۰,۲۲

٤ – الزامات امنیتی داده های شخصی در استفاده از هوش مصنوعی

امنیت داده های شخصی در زمینه سیستم های هوش مصنوعی قابل توجه است. به طور کلی داده های شخصی باید به گونه ای پردازش شوند؛ که سطوح مناسبی از امنیت را در برابر پردازش غیرمجاز یا غیرقانونی، از دست دادن تصادفی، تخریب یا آسیب تضمین کند. با این حال هوش مصنوعی ممکن است؛ خطرات امنیتی را بدتر کند وکنترل آنها را دشوارتر کند. بنابراین حریم خصوصی داده ها و .الزامات امنیتی باید به دقت تنظیم شوند

در استفاده از هوش مصنوعی برای پردازش داده های شخصی ۵ – الزامات
تصمیم گیری خودکار، هر تصمیمی است که بدون دخالت معنادار انسانی اتخاذ می شود وآثار قانونی بر روی شخص دارد یا به طور مشابه به طور قابل توجهی بر او تأثیر می گذارد. این ممکن است تا حدی با نمایه سازی همپوشانی داشته باشد یا ناشی از آن باشد، اما همیشه اینطورنیست و الزامات خاصی بر پروفایل و تصمیم گیری خودکار تحمیل میشود. استفاده ازیک سیستم هوش مصنوعی در رابطه با افراد اغلب شامل پروفایل سازی و گاهی اوقات تصمیم گیری خودکار است. به عنوان مثال، هنگام استفاده از یک سیستم هوش مصنوعی برای فیلتر کردن برنامه های کاربردی برای یک شغل خالی، ازپروفایل سازی برای تعیین اینکه آیا متقاضی برای شغل خالی مناسب است یا خیر؟ استفاده می شود [۱]. اگر سیستم هوش مصنوعی متقاضیانی را که مناسب می داند؛ فیلترکند و سایر متقاضیان .برای این موقعیت در نظر گرفته نشوند، این تصمیم گیری خودکار نسبت به گروه دوم اعمال می شود

٦ – الزامات قانونی برای کاربران هوش مصنوعی

الزامات قانونی بر هر کسی که از سیستم هوش مصنوعی برای پروفایل ویا اهداف تصمیم گیری خودکار استفاده می کند، تحمیل می شود حتی اگر آنها سیستم را از شخص ثالث به دست آورده :باشند. الزامات به شرح زیر است[۲]
انصاف که شامل جلوگیری از تبعیض افراد می شود.– شفافیت نسبت به افراد، از جمله اطلاعات معناداردرمورد منطق درگیر در سیستم هوش مصنوعی؛– حق مداخله انسانی، موارد فوق فرد را قادر .می سازد تا تصمیم گیری خودکار را به چالش بکشد

۷ – الزامات عمومی برای سیستم های هوش مصنوعی پرخطر

قانون هوش مصنوعی الزامات کلی زیر را بر روی سیستم های هوش مصنوعی پرخطر تحمیل می :کند[۳]
– یک سیستم مدیریت ریسک ایجاد شود.آن سیستم به طور مداوم در تمام طول مدت حفظ شود؛
– همچنین طول عمر سیستم برای شناسایی و تجزیه و تحلیل ریسک های شناخته شده و قابل پیش . بینی، تخمین و ارزیابی شود
– داده های آموزشی، اعتبار سنجی و آزمایش لازم ارائه شود. از جمله ارتباط دقت، کامل بودن آن، نظارت، تشخیص و تصحیح سوگیری، که ممکن است بر اساس منافع عمومی مقررات حفاظت از داده .ها ی عمومی برای آنها استفاده شود
– تهیه مستندات فنی که نشان می دهد؛ سیستم هوش مصنوعی با قانون هوش مصنوعی مطابقت دارد.

۱– McCarthy. ۲۰۲۲,۱۱
۲– European Commission: ۲۰۱۷
۳– Artzt,et al,۲۰۲۲,٤۹

ایجاد سیستم خودکار برای اطمینان از سطح ردیابی سیستم عملکرد؛ –
شفافیت را تضمین کنید تا کاربر سیستم را قادر سازد؛ هوش مصنوعی را به همراه خروجی سیستم و –
.استفاده مناسب از آن تفسیر کند
نظارت انسانی فعال شود. در سیستم هوش مصنوعی با هدف به حداقل رساندن خطرات به سلامت، –
ایمنی یا حقوق اساسی، توسط فردی که توانایی ها و محدودیت های سیستم را به طور کامل درک می
.کند
ازدقت، استحکام و امنیت سایبری اطمینان حاصل کنید. برای تقویت تاب آوری در مورد خطاها، –
.ناهماهنگی ها، نقص فنی، استفاده غیرمجاز،یا بهره برداری ازآسیب پذیری ها[1]
قانون هوش مصنوعی الزامات کلی را برای سیستم های هوش مصنوعی پرخطرمعرفی می کند که از
الزامات خاص هستند. به عنوان مثال، قانون هوش مصنوعی الزامات خاصی را برای آموزش، اعتبار
سنجی و آزمایش داده ها به منظور جلوگیری از تعصب و تبعیض اعمال می کند، در حالی که مقررات
حفاظت از داده ها ی عمومی صرفا[2]ایجاب می کند که هر گونه پردازش داده های شخصی منصفانه
باشد. مثال دیگر الزام به نظارت انسانی است. اگرچه مقررات حفاظت از داده های عمومی به افراد
حق مداخله انسانی در موارد تصمیم گیری خودکار را می دهد، این الزام فقط برای شرکتی که تصمیم
.خودکارمی گیرد؛ اعمال می شود و نه برای شرکتی که سیستم هوش مصنوعی مرتبط را ارائه می کند

۸ – روندهای امنیت سایبری

امنیت سایبری با چالش های مختلفی مواجه است که یکی از آنها حفاظت از داده های شخصی و امنیت داده ها است. هوش مصنوعی با تجزیه و تحلیل حجم عظیمی از داده ها از جمله داده های شخصی کار می کند. بنابراین، موسسات باید حفاظت از داده ها و امنیت داده ها را در برنامه های کاربردی هوش مصنوعی تضمین کنند. هوش مصنوعی در حال تبدیل شدن به یک بازیگر کلیدی در فرآیند تحول دیجیتال است و مزایای آن مانند کارایی و بهبود مدیریت ریسک به کابران کمک می کند تا فناوری های دیجیتال جدید را پیاده سازی کنند[3] .تحقیقات بیشتر نشان می دهد که حملات سایبری در حال افزایش است، به ویژه حملاتی که شرکت ها و ارگان های دولتی را هدف قرار می دهند. انتظار می رود حملات سایبری خودکار و تصفیه شده مانند حملات مبتنی بر هوش مصنوعی در سال ۲۰۲۳ بر اهمیت مدیریت تهدید، مدیریت حوادث، حفاظت از داده ها و آموزش امنیت افزایش یابد. مطالعه سایبری کارکنان برای شرکت ها برای ایجاد و اجرای استراتژی های امنیت سایبری مولد تاکید دارد. به علاوه این مطالعه به جزئیات تغییرات قوانین و مقررات و همچنین روندهای تجاری و فناوری می .پردازد که ممکن است بر محیط امنیت سایبری در سال۲۰۲۳ تأثیر بگذارد[3]

۱- Artzt,et al,۲۰۲۲,۱۱

۲-Appinventiv,۲۰۲۳,۳۲ AI in Banking – How Artificial Intelligence is Used in Banks. https://appinventiv.com/blog/ai-in-b

۳- Deloitte,۲۰۲۳,۱٤ Global Future of Cyber Survey, Building long-term value by putting cyber at the heart of the business. https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.h

حملات سایبر ی به ویژه در بخش تولید، آموزش و مراقبت های بهداشتی ادامه خواهد یافت. گسترش ۵ چالش های امنیتی فناوری های اخیر مانند ابزارهای اینترنت اشیا (اینترنت اشیا) و شبکه های جدیدی را به همراه خواهد داشت. تهدیدات ذکر شده؛ شامل حملات مبتنی بر هوش مصنوعی و یادگیری ماشینی، دستکاری در شبکه های رسانه های اجتماعی و رشد بیشتر حملات باج افزار است.

۹ – هوش مصنوعی در امنیت سایبری

تکامل روزافزون تهدیدات سایبری، چه از نظر تعداد و چه از نظر پیچیدگی، اکنون امنیت فضای سایبری را با مشکل جدی مواجه کرده است. علاوه بر این، بسیاری از این نوع تهدیدها از فناوری های مجهز به هوش مصنوعی برای بهبود اثربخشی خود سوء استفاده می کنند و اشکال سنتی دفاع را بی فایده می کنند. حملاتی که توسط هوش مصنوعی پشتیبانی می شوند خطرناک تر هستند و بیشتر دفاع هابه اندازه کافی برای این مبارزه آماده نیستند.[۱]

هوش مصنوعی در صنعت امنیت سایبری برای مدیریت تهدیدات سایبری اهمیت فزاینده ای پیدا می کند. هوش مصنوعی پیامدهای بالقوه ای را معرفی می کند: بیش از ۶۰ درصد از شرکت هایی که هوش مصنوعی را پیاده سازی می کنند، خطر امنیت سایبری مرتبط با هوش مصنوعی را به عنوان مهم ترین خطر شناسایی می کنند.[۲] تقاضا برای فناوری های هوش مصنوعی در امنیت سایبری مانند گذشته در حال افزایش است. بنابراین نقش بسیار مهمی در امنیت فعال ایفا می کند. از این رو می توان از هوش مصنوعی برای مقابله با تهدیدات ناشناخته در مقیاس بزرگ و در زمان واقعی استفاده کرد و به آن اجازه می دهد حملاتی را که مدل های سنتی تشخیص نمی دهند، مسدود کند.[۳]

۱۰ – رویکردهای مبتنی بر هوش مصنوعی در امنیت سایبری

به لطف پیشرفت در فناوری محاسبات، جامعه ما به سرعت در حال تغییر است[۴]. روال روزمره مردم و اشتغال به طور قابل توجهی تحت تاثیر این امر قرار دارد. برخی ازاین فناوری ها امکان توسعه رایانه هایی را فراهم کرده اند که توانایی های شناختی مشابه انسان ها از جمله توانایی یادگیری، تصمیم گیری و حل مشکلات دارند. به عنوان مثال، هوش مصنوعی می تواند حجم عظیمی از داده ها را تجزیه و تحلیل کند و میتواند در زمان استفاده از هوش قضاوت کند. زمینه های متعددی از تحقیقات و فناوری از استفاده از تکنیک های هوش مصنوعی سودمی برند[۵]. بر کسی پوشیده نیست که اینترنت پر از داده های شخصی است که منجر به مشکلات امنیت سایبری زیادی می شود. اولاً، مقدار داده، تجزیه و تحلیل دستی

۱- Mateus ,۲۰۲۲,۱۲۳. Security in microservices architectures," Procedia Computer Science, vol. ۱۸۱, pp. ۲۰۲۱ ,۱۲۳۶–۱۲۲۵

۲- -ibid,۱۲۲۲

۳- Arnaud, Matos, January۲۰۲۳; Accepted January ۲۰۲۳; Available online January ۲۰۲۳

۴- -Badotra & Mehra۲۰۲۱

۵- -Achi,et al ,۲۰۲۱ 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

را غیرممکن می کند. ثانیاً، ممکن است خطراتی مبتنی بر هوش مصنوعی یا افزایش تهدیدات وجود داشته باشد. علاوه بر این، هزینه های پیشگیری از تهدیدها به دلیل هزینه بالای استخدام متخصصان افزایش می یابد[۱] .توسعه و استفاده از الگوریتم ها برای شناسایی این خطرات نیز مستلزم صرف زمان، هزینه و تلاش زیادی است. استفاده از تکنیک های مبتنی بر هوش مصنوعی یک راه حل برای این مشکلات است. هوش مصنوعی قادر به تجزیه و تحلیل سریع، صحیح و کارآمد داده های عظیم است. یک سیستم مبتنی بر هوش مصنوعی می تواند حملات آینده را پیش بینی کند که مشابه حملاتی هستند که قبلاً با استفاده از تاریخچه تهدید رخ داده اند، حتی اگر الگوهای آن حملات متفاوت باشد. هوش مصنوعی می تواند داده های گسترده ای را مدیریت کند، تغییرات جدید و قابل توجهی را در حملات پیدا کند و به طور مداوم پاسخ سیستم امنیتی خود را به تهدیدات بهبود بخشد. استفاده از هوش مصنوعی در امنیت سایبری رویکرد امنیتی سنتی را از واکنشی به پیشگیرانه و کمک به شناسایی .و کاهش تهدیدات در زمان واقعی تغییر داده است[۲]

۱۱ – هوش مصنوعی و چشم انداز تهدید سایبری

استقرار اجزای هوش مصنوعی برای مقاصد مرتبط باسایبر می تواند بر چشم انداز تهدیدات سایبری تأثیر بگذارد. بدون اتخاذ هر گونه اقدام پیشگیرانه اساسی، هوش مصنوعی می تواند؛ تهدیدات سایبری موجود (کمیت) را گسترش دهد. هوش مصنوعی می تواند مجموعه مجریانی را که قادر به انجام فعالیت های مخرب سایبری هستند، و مجموعه اهداف قابل قبول را گسترش دهد. این ادعا به دنبال کارایی، مقیاس پذیری و سازگاری هوش مصنوعی و همچنین«دموکراتیزه کردن» تحقیق و توسعه در این زمینه است. به طور خاص، انتشار مؤلفه های هوش مصنوعی در میان مجریان سنتی تهدید سایبری، جنایتکاران، هکتیویست ها و گروه های تروریستی می تواند تعداد نهادهایی را که انجام حملات برای آنها مقرون به صرفه باشد، افزایش دهند. با توجه به اینکه برنامه های کاربردی هوش مصنوعی نیز مقیاس پذیر هستند، مجریانی که دارای قابلیت هستند ممکن است توانایی برای انجام حملات را با نرخ بالاتری به دست آورند. اهداف جدید برای ضربه زدن ممکن است برای آنها ارزشمند شود[۳] .ازنقطه نظر کیفی، حملات سایبری مبتنی بر هوش مصنوعی می توانند در اقدامات و حملات مؤثرتر، دقیق تر و پیچیده تر نیز ظاهر شوند. افزایش اثربخشی از ویژگی های کارایی، مقیاس پذیری و .سازگاری این راه حل ها ناشی می شود و اهداف بالقوه، راحت تر شناسایی و بررسی می شوند در این راستا، امنیت سایبری خود به تحقیق و توسعه هوش مصنوعی مرتبط می شود.برای حفظ عملکرد مناسب، قابلیت اطمینان، یکپارچگی و همچنین برای جلوگیری از اثرات شوم، سیستم های سایبری یک پارچه هوش مصنوعی نیاز به حفاظت در برابر حوادث یا حملات سایبری دارند. اتخاذ شیوه های امنیت سایبری و همچنین ترویج گسترد سازوکارهای

۱- ,Ansari,۲۰۲۲,۱۲TheImpactandLimitationsofArtificialIntelligenceinCybersecurity:ALiteratureReview.IJARCCE,۹)۱۱).https://doi.org/۱۰,۱۷۱٤۸/ijarcce.۲۰۲۲,۱۱۹۱۲

۲- -Rawat et al,۲۰۲۲,۲٤۷ The Empirical Analysis of Artificial Intelligence Approaches for Enhancing the Cyber Security for Better Quality. ٥ ۲۰۲۲th International Conference on Contemporary Computing and Informatics (IC۳I), ۲٥۰–۲٤۷. https://doi.org/۱۰,۱۱۰۹/IC۳I٥٦۲٤۱,۲۰۲۲,۱۰۰۷۲۸۷۷

۳- Bonfanti, Matteo,۲۰۲۰,۲

سایبری با الزامات خاص برای تحقیق،توسعه و کاربرد هوش مصنوعی به عنوان «امنیت سایبری برای هوش مصنوعی» نامیده می شود[1].

۱۲ – تشخیص تهدید با استفاده از روش مصنوعی هوشمند

چه در امنیت فیزیکی، چه امنیت سایبری و چه امنیت داخلی تشخیص تهدید یکی از اجزای ضروری برای ایمن نگه داشتن افراد و سازمان ها است.به لطف پیشرفت های فناوری هوش مصنوعی، شناسایی وحذف تهدیدات در زمان واقعی آسان تر شده است[2].

سیستم های تشخیص تهدید مبتنی بر هوش مصنوعی می توانند خطرات و تهدیدها را سریع تر، دقیق تر و کارآمدتر شناسایی کنند. این سیستم های تشخیص تهدید از حجم عظیمی از داده ها یاد می گیرند و الگوهایی را پیدا می کنند که می توانند به خطرات احتمالی با استفاده از الگوریتم ها و تکنیک های یادگیری ماشین اشاره کنند. ترافیک شبکه، فیلم های نظارت تصویری و فیدهای رسانه های اجتماعی تنها تعدادی از انواع داده هایی هستند که ممکن است برای آموزش الگوریتم های هوش مصنوعی برای شناسایی و اطلاع پرسنل امنیتی از نقض ها یا تهدیدات احتمالی امنیتی استفاده شوند. استفاده از تکنیک های یادگیری عمیق به الگوریتم ها اجازه می دهد؛ تا از مجموعه داده های گسترده یاد بگیرند و حتی الگوهای کوچک را کشف کنند. این ممکن است نشان دهد که خطرات احتمالی یکی از مهمترین جنبه های تشخیص تهدید مبتنی بر هوش مصنوعی است[3].

یادگیری عمیق، فرآیند یادگیری مغز انسان را با استفاده از شبکه های عصبی شبیه سازی می کند که به الگوریتم ها اجازه می دهد در طول زمان با شناسایی و یادگیری از نقاط داده جدید دقیق تر شوند. تیم های امنیتی به لطف تشخیص تهدید مبتنی بر هوش مصنوعی که در شناسایی تهدیدهادر زمان واقعی بسیار مؤثر است، می توانند سریع پاسخ دهند و از تبدیل شدن خطرات احتمالی به رویدادهای امنیتی مهم جلوگیری کنند[4] . این سیستم ها می توانند به طور همزمان داده ها را ازچندین منبع تجزیه و تحلیل کنند و آنها را قادر می سازد تهدیدات را در سیستم ها و شبکه های مختلف شناسایی و ردیابی کنند. بسته به نوع داده ها و الگوریتم های مورد استفاده، سیستم های تشخیص تهدید مبتنی بر هوش مصنوعیمی توانند خطرات مختلفی را شناسایی کنند[5] .این فناوری ها برای مثال می توانند بدافزار، کلاهبرداری های فیشینگ و سایر خطرات آنلاین را تشخیص دهند. هوش مصنوعی می تواند فعالیت یا رفتار مشکوک را در فیلم های نظارت تصویری مانند دسترسی غیرمجاز یا سرقت در زمینه امنیت فیزیکی شناسایی کند. هوش مصنوعی می تواند داده های فید رسانه های اجتماعی در امنیت داخلی را برای شناسایی بررسی کند .تهدیدات بالقوه تروریستی هوش مصنوعی برای تشخیص

۱- .-Bonfanti, Matteo,٤, ۲۰۲۰

۲- Rehman, ۲۰۲۲,۳۲

۳- - Welukar et al,۲۰۲۱‘Black box AI’. Retrieved from: https://www.techtarget.com/whatis/definition/black-box-AI [accessed ۱۲ December ۲۰۲۲]

۴- - Kuzlu, et al,۲۰۲۱ Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things, ۱)۱). https://doi.org/۱۰,۱۰۰۷/s٤-۰۰۰۰۱-۰۲۰-٤۳۹۲٦

تهدید چندین مزیت دارد. زیرا سیستم های مبتنی بر هوش مصنوعی بسیار موثر و دقیق هستند و تیم های امنیتی می توانند تهدیدات را فوراً شناسایی کرده و اقدام کنند. این سیستم ها برای تجزیه و تحلیل داده ها از چندین منبع به طور همزمان عالی هستند زیرا می توانند به سرعت حجم عظیمی از داده ها را تجزیه و تحلیل کنند. دقت سیستم های هوش مصنوعی را نیز می توان در طول زمان با یادگیری ازداده های جدید و تطبیق با آن ها بهبود بخشید که احتمال مثبت کاذب را کاهش می دهد[۱].

۱۳ – تکنیک های هوش مصنوعی درامنیت سایبری

تکنیک های هوش مصنوعی حوزه امنیت سایبری را متحول کرده است. این ها تکنیک هایی هستند که متخصصان امنیت سایبری را قادر می سازند تامقادیر زیادی از داده ها را تجزیه و تحلیل کنند، ناهنجاری ها و الگوها و تهدیدات بالقوه را قبل از تبدیل شدن به حملات واقعی شناسایی کنند[۲]. در ادامه راجع به برخی از تکنیک های رایج مصنوعی که در امنیت سایبری استفاده می شوند، بحث می شود.

۱۳– ۱ – فراگیری ماشین

این یک نوع هوش مصنوعی است که سیستم ها را قادر می سازد از داده ها بدون برنامه ریزی صریح یاد بگیرند. الگوریتم های یادگیری ماشین بر روی مجموعه داده های بزرگی از ترافیک پیچیده برای شناسایی الگوها و شناسایی تهدیدات بالقوه آموزش داده می شوند و برای کارهایی مانند تشخیص . بدافزار، تشخیص نفوذ شبکه و تشخیص ناهنجاری استفاده میشود[۳]

۱۳–۲ – پردازش زبان طبیعی

این یک نوع هوش مصنوعی است که رایانه ها را قادر می سازد زبان انسان را درک و تفسیر کنند. در امنیت سایبری برای تجزیه و تحلیل منابع داده بدون ساختار مانند فید رسانه های اجتماعی و انجمن های آنلاین برای تهدیدات احتمالی استفاده می شود[۴].

۱۳–۳– یادگیری عمیق

زیر مجموعه ای از یادگیری ماشین است که از شبکه های عصبی عمیق برای یادگیری الگوهای پیچیده از داده ها استفاده می کند. در امنیت سایبری برای کارهایی مانندتشخیص بدافزار، تشخیص فیشینگ و تشخیص کلاهبرداری استفاده میشود. یا زیر مجموعه ای دیگر از که بر قضاوت تاکید دارد. یادگیری تقویتی می تواند در امنیت سایبری برای آموزش

۱- Sadiku,etal,۲۰۲۰

۲- -Thuraisingham,۲۰۲۰,۱۶

۳- Almuhtadi & Merat, ۲۰۲۰WITHDRAWN: Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings. https://doi.org/۱۰,۱۰۱۶/j.matpr.۲۰۲۱,۰۲,۵۳۱

۴- Rizvi ,۲۰۲۳,۵۵

سیستم ها برای تصمیم گیری در مورد نحوه پاسخگویی به حملات بر اساس موقعیت و سطح تهدید درک شده استفاده شود[1].

۱۳-٤ – سیستم های خبره

سیستم های هوش مصنوعی هستند که توانایی های تصمیم گیری یک متخصص انسانی را در یک حوزه خاص تقلیدمی کنند. در امنیت سایبری، این سیستم ها برای کارهایی مانند تشخیص نفوذ و پاسخگویی و ارزیابی آسیب پذیری استفاده می شوند.

١٤ – حفاظت از هوش مصنوعی

مسئله اصلی در مورد محافظت از خود هوش مصنوعی در برابر بهره برداری از آسیب پذیری ها و سایر تهدیدات ناشی از حملاتهدفمندبه هوش مصنوعی است[2]. در همین حال، ما باید از آسیب رساندن هوش مصنوعی به انسان جلوگیری کنیم. علاوه بر دفاع در برابر حملات شناخته شده، امنیت خود مدل هوش مصنوعی نیز باید تقویت شود تا از حملات احتمالی با اعتبارسنجی مدل یا ابزارهای دیگر جلوگیری شود. مهم تر از همه، سیستم های هوش مصنوعی می توانند تهدیدی بالقوه برای انسان ها باشند، به ویژه هنگام استفاده از هوش مصنوعی در روبات ها آنها می توانند به طور مستقل و بدون مداخله دستی اقداماتی را ایجاد کنند و به دلیل قابلیت های خودآموزی می توانند از کنترل انسان جدا شوند[3].

نتیجه گیری

هوش مصنوعی به عنوان یک فناوری پیشرفته و قدرتمند، تاثیر بزرگی بر امنیت سایبری و حفاظت از داده‌ها دارد. از یک سو، هوش مصنوعی قادر است به صورت خودکار و با دقت بالا تهدیدات امنیتی را شناسایی کرده، الگوهای حملات را پیش‌بینی کرده و به صورت سریع واکنش مناسب را نسبت به حملات امنیتی نشان دهد. از سوی دیگر، استفاده از هوش مصنوعی ممکن است باعث نقض حریم خصوصی و پرهزینه شدن فرآیندهای امنیتی شود. همچنین، خطرات احتمالی نظیر حملات به خود هوش مصنوعی نیز وجود دارد.

با این حال، با مدیریت مناسب و تعامل با تکنولوژی هوش مصنوعی، می‌توان بهبود قابل توجهی در امنیت سایبری و حفاظت از داده‌ها داشت. لذا، سازمان‌ها باید با دقت و با استفاده از استانداردهای امنیتی مناسب، هوش مصنوعی را در سیستم‌های خود پیاده‌سازی کنند و به منظور کاهش خطرات احتمالی، به مداوم آن را به روز رسانی کنند. به طور کلی،

۱- -Rizvi ,۲۰۲۳,٥٦.

۲- Rawal, et al,۲۰۲۱,۱۲ The Empirical Analysis of Artificial Intelligence Approaches for Enhancing the Cyber Security for Better Quality. ٥ ۲۰۲۱th International Conference on Contemporary Computing and Informatics (IC۳I), ۲٥۰–۲٤۷. https://doi.org/۱۰,۱۱۰۹/IC۳I٥٦۲٤۱,۲۰۲۲,۱۰۰۷۲۸۷۷.

۳- Boyko,et, al, ۲۰۱۹ Advantages and Disadvantages of the Data Collection›s Method Using SNMP», International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), pp. ۲۰۱۹ ,٥-۱

هوش مصنوعی می‌تواند نقش مهمی در تقویت امنیت سایبری و حفاظت از داده‌ها ایفا کند، اما نیاز به مدیریت مناسب و توجه به جنبه‌های امنیتی آن وجود دارد.

جایگاه هوش مصنوعی در امنیت سایبری به سرعت در حال توسعه است و اهمیت آن بیشتر و بیشتر می شود.روش های سنتی تشخیص و پیشگیری ازتهدید دیگر کافی نیستند. سیستم های مبتنی بر هوش مصنوعی روش های پیچیده و پیشرفته ای را برای مقابله با حملات سایبری ارائه می کنند. برای شناسایی و متوقف کردن خطرات سایبری،سیستم هایمبتنی بر هوش مصنوعی از روش هایی مانند یادگیری ماشینی،یادگیری عمیق، پردازش زبان طبیعی، تجزیه و تحلیل پیش بینی کننده و تحلیل رفتاری استفاده می کنند.

هوش مصنوعی قادر است به صورت خودکار و با دقت بالا تهدیدات امنیتی را شناسایی کرده و اقدامات مناسب برای مقابله با آن‌ها را انجام دهد. با استفاده از الگوریتم‌های هوش مصنوعی، می‌توان الگوهای حملات سایبری را تشخیص داد و پیش‌بینی کرد تا اقدامات پیشگیرانه مناسب انجام شود.و همچنین هوش مصنوعی قادر است به صورت خودکار و سریع به حملات سایبری پاسخ دهد و از اطلاعات جمع‌آوری شده در زمان واقعی استفاده کند.علاوه بر این نقاط قوت ذکره شده استفاده از هوش مصنوعی در حفاظت از داده ها و امنیت سایبری نقاط ضعفی هم به همراه دارد:هوش مصنوعی نیز ممکن است به عنوان یک نقطه ضعف در سامانه‌های امنیتی مورد حمله قرار گیرد و توسط مهاجمان به سوءاستفاده تبدیل شود استفاده ازهوش مصنوعی در حفاظت از داده‌ها ممکن است باعث نقض حریم خصوصی کاربران شود و اطلاعات حساس آن‌ها در خطر قرار گیرد همچنین پیاده‌سازی و استفاده از تکنولوژی هوش مصنوعی در حفاظت از داده‌ها ممکن است هزینه‌بر باشد و برای برخی سازمان‌ها قابل دسترس نباشد. برای مدیریت و کنترل تاثیر هوش مصنوعی بر آزادی های اساسی و حقوق بشر، می توان از اتخاذقوانین و مقررات برای محدود کردن استفاده از هوش مصنوعی در زمینه‌هایی که ممکن است به حقوق بشر و ازادی های اساسی آسیب بزند کمک گرفت وهمچنین بررسی و نظارت منظم بر استفاده از هوش مصنوعی توسط سازمان‌های مستقل و قدرتمند به منظور جلوگیری از سوءاستفاده و تضمین رعایت حقوق بشر واطلاع‌رسانی صحیح و شفاف از استفاده از هوش مصنوعی در تصمیم‌گیری‌ها و فرآیندهای مختلف، به منظور افزایش اطمینان عمومی و کاهش نگرانی ها می‌تواند به مدیریت و کنترل تاثیر هوش مصنوعی بر حقوق بشر و ازادی‌های اساسی کمک کند و اطمینان حاصل کند که تکنولوژی همچنان به نفع انسان‌ها استفاده می‌شود.

فهرست منابع

۱. ابوذری، مهرنوش (۱۴۰۱)،حقوق و هوش مصنوعی، تهران میزان.

۲. ریتون، م (۱۳۹۸)آینده جنگ و هوش مصنوعی مسیر قابل مشاهده ترجمه شبنم امیر ،جاوید انتشارات پشتیبان.

۳. مصطفوی اردبیلی ، سید محمدمهد ی، تقی زاده انصاری، مصطفی و رحمتی فر، سمانه (۱۴۰۱)،کارکردها و بایستههای هوش مصنوعی از منظردادرسی منصفانه. حقوق فناوری های نوین.

١. Li, J. hua: Cyber security meets artificial intelligence: A survey. Front. Inf. Technol. Electron. Eng. ١٤٧٤–١٤٦٢ ,١٩ ,٢٠١٨. [CrossRef]
٢.A. Rawal, J. Mccoy, D. B. Rawat, B. Sadler and R. Amant, «Recent Advances in Trustworthy Explainable Artificial Intelligence: Status, Challenges and Perspectives,» in IEEE Transactions on Artificial Intelligence, doi: ١٠,١١٠٩/TAI.٢٠٢١,٣١٣٣٨٤٦.
٣. Achi, A., Kuwunidi Job, G., Shittu, F., Baba Atiku, S., Unimke Aaron, A., & Zahraddeen Yakubu, I. (٢٠٢١). 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
٤.Alhayani, B., Jasim Mohammed, H., Zeghaiton Chaloob, I., & Saleh Ahmed, J. (٢٠٢١). WITHDRAWN: Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings. https://doi.org/١٠,١٠١٦/j.matpr.٢٠٢١,٠٢,٥٣١
٥.Angelopoulos, A.; Michailidis, E.T.; Nomikos, N.; Trakadas, P.; Hatziefremidis, A.;Voliotis, S.; Zahariadis, T. Tackling Faults inthe Industry ٤,٠ Era-A Survey of Machine-Learning Solutions and Key Aspects. Sensors ١٠٩ ,٢٠ ,٢٠٢٠. [CrossRef]
٦. Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (٢٠٢٢). The Impact and Limitations of Artificial IntelligenceinCybersecurity: ALiteratureReview. IJARCCE,٩)١١).https://doi.org/١٠,١٧١٤٨/ijarcce.٢٠٢٢,١١٩١٢
٧. Appinventiv (٢٠٢٣): AI in Banking – How Artificial Intelligence is Used in Banks. https://appinventiv.com/blog/ai-in-b
٨. Arnaud, Matos, Artificial Intelligence as a Support Tool to CybersecurityActivities,(٢٠٢٢), Advanced Research on Information Systems Security, an International Journal (ARIS٢Volume ٢, No ١, pp ١٢-٠٢
Boyko, V. Varkentin and T. Polyakova, «Advantages and Disadvantages of the Data Collection›s Method Using SNMP», International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), pp. ٢٠١٩ ,٥-١
٩. Deloitte (٢٠٢٣): Global Future of Cyber Survey, Building long-term value by putting cyber at the heart of the business. https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.h
European Commission (٢٠١٧), Guidelines of the European Data Protection Board on Automated individual decision-making and Profiling for the purposes of Regulation ٦٧٩/٢٠١٦, adopted on ٣ October ٢٠١٧, as last Revised and Adopted on ٦ February ٢٠١٨. Retrieved from: https://service.betterregulation.com/document/٣٠٦١٩٣ [accessed ١٢ December ٢٠٢٢]

۱۰. hildebrandt, m., koops, bj., The Challenges of Ambient Law and Legal Protection in the Profiling Era,in: Modern Law Review, -٤٢٨ ,(٣) ٧٣ ٤٦٠, May ٢٠١٠ ,٧. (Retrieved from ttps://onlinelibrary.wiley.com/doi/ full/١٠,١١١١/j.٢٢٣٠,٢٠١٠,٠٠٨٠٦-١٤٦٨.x – ٢٠٢١ .٠٢ .١٨.)
١١. ISHII, K., Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects, in: AI & Society, ٢٠١٩ ,٥٣٣-٥٠٩ ,٣٤.
Kaloudi, N.; Jingyue, L.I. The AI-based cyber threat landscape: A survey. ACM Comput. Surv. ٢٠ ,٥٣ ,٢٠٢٠. [CrossRef]
١٢. Kuzlu, M., Fair, C., & Guler, O. (٢٠٢١). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things, ١)١).
https://doi.org/١٠,١٠٠٧/s٤٣-٠٠٠٠١-٠٢٠-٤٣٩٢٦
١٣. Maad M. Mijwil١, Mohammad Aljanabi٢,٤, ChatGPT)٢٠٢٣)
January٢٠٢٣; Accepted January ٢٠٢٣; Available online January ٢٠٢٣
١٤.MATTHIAS ARTZT, TRAN VIET DUNG(٢٠٢٢), ARTIFICIAL INTELLIGENCE AND DATA PROTECTION: HOW TO RECONCILE BOTH AREAS FROM THE EUROPEAN LAW PERSPECTIVE, Vietnamese Journal of Legal Sciences, Vol. ٠٧, No. ٢٠٢٢ ,٠٢, pp. ٥٨-٣٩
١٥. McCarthy M. and Propp K. (٢٠٢١), Machines learn that Brussels writes the rules: The EU's new AI ١٦.regulation, Brookings Institution. Retrieved from:
https://www.brookings.edu/blog/techtank/٠٤/٠٥/٢٠٢١/machines-learn-that-brussels-writes-the-rules-the-eusnew-ai-regulation/ [accessed ١٢ December ٢٠٢
١٧. N. Mateus-Coelho, M. Cruz-Cunha, and L. G. Ferreira, "Security in microservices architectures," Procedia Computer Science, vol. ١٨١, pp. ٢٠٢١ ,١٢٣٦–١٢٢٥.
١٨.N. Mateus-Coelho, M. Cruz-Cunha, and P. Silva-Ávila, "Application of the industry ٤,٠ technologies to Mobile Learning and Health Education Apps," FME Transactions, vol. ٤٩, no. ٤, pp. ٢٠٢١ ,٨٨٥–٨٧٦.
Novikov, I (٢٠١٨), How AI can be applied to cyberattacks. Retrieved Novemb. ٢٠١٩ ,٢٥.
١٩. Rawat, B. S., Gangodkar, D., Talukdar, V., Saxena, K., Kaur, C., & Singh, S. P. (٢٠٢٢). The Empirical Analysis of Artificial Intelligence Approaches for Enhancing the Cyber Security for Better Quality. ٥ ٢٠٢٢th International Conference on Contemporary Computing and Informatics (IC٣I), ٢٠ .٢٥٠–٢٤٧. https://doi.org/١٠,١١٠٩/IC٣I٥٦٢٤١,٢٠٢٢,١٠٠٧٢٨٧٧
٢١.regulation (EU) ٦٧٩/٢٠١٦ of the European Parliament and of the Council of ٢٧ April ٢٠١٦ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive ٤٦/٩٥/EC (General Data Protection Regulation) Official Journal of the European Union | L ١/١١٩.