فصل پنجم

امنیت و استراتژی داده باز در سلامت

گردآورندگان:

دکتر فهیمه قاسمی
عضو هیات علمی گروه هوش مصنوعی

دکتر فرزاد مسعود کبیر
رئیس پژوهشکده بیماریهای قلب و عروق، مرکز قلب تهران

دکتر امیرعلی حمیدیه
رئیس پژوهشکده ژن، سلول و بافت

دکتر مسلم تقی زاده
پژوهشگر هوش مصنوعی و تحول دیجیتال دانشگاه تهران

دکتر بغدادی
محقق و پژوهشگر هوش مصنوعی دانشگاه صنعتی امیر کبیر

سوالات کلیدی:

۱- چه اقداماتی برای اطمینان از حفظ حریم خصوصی و حفاظت از داده‌های بیمار هنگام استفاده از هوش مصنوعی در مراقبت‌های بهداشتی وجود دارد؟

۲- خطرات نقض داده‌ها یا دسترسی غیرمجاز هنگام پیاده سازی سیستم‌های هوش مصنوعی در تنظیمات مراقبت‌های بهداشتی چیست؟

۳- چگونه می توان از هوش مصنوعی برای افزایش امنیت داده‌ها و محافظت از اطلاعات حساس مراقبت‌های بهداشتی استفاده کرد؟

۴- چه چارچوب‌های نظارتی و استانداردهای انطباق بر امنیت داده‌ها در محیط‌های مراقبت‌های بهداشتی مبتنی بر هوش مصنوعی حاکم است؟

۵- بهترین روش‌ها برای تضمین امنیت داده‌ها در طول چرخه عمر برنامه‌های هوش مصنوعی در مراقبت‌های بهداشتی چیست؟

۶- چه استراتژی‌هایی را می توان برای ایجاد اعتماد در بین بیماران و متخصصان مراقبت‌های بهداشتی در مورد امنیت سیستم‌ها و داده‌های مراقبت‌های بهداشتی مبتنی بر هوش مصنوعی به کار گرفت؟

امنیت داده به اقدامات و شیوه‌هایی اطلاق می‌شود که برای محافظت از داده‌های دیجیتال در برابر دسترسی غیرمجاز، افشا، تغییر، تخریب یا سرقت انجام می‌شود. این شامل فناوری‌ها، سیاست‌ها و رویه‌های مختلفی است که برای محافظت از اطلاعات حساس و اطمینان از محرمانه بودن، یکپارچگی و در دسترس بودن آن طراحی شده‌اند. در حوزه مراقبت‌های بهداشتی و علوم پزشکی، امنیت داده‌ها به محافظت از اطلاعات حساس بیمار، سوابق پزشکی و سایر داده‌های مراقبت‌های بهداشتی از دسترسی، افشا، تغییر یا تخریب غیرمجاز اشاره دارد. با توجه به ماهیت بسیار حساس داده‌های مراقبت‌های بهداشتی، که اغلب شامل اطلاعات سلامت شخصی و اطلاعات بهداشتی محافظت شده است، امنیت داده‌ها در مراقبت‌های بهداشتی برای اطمینان از حفظ حریم خصوصی بیمار، رعایت مقررات و یکپارچگی عملیات مراقبت‌های بهداشتی از اهمیت بالایی برخوردار است. یکی از موارد ضروری در حفظ امنیت داده آن است که وزارت بهداشت بایستی دسترسی را برای محدود کردن دسترسی به داده‌های بیمار فقط برای افراد مجاز اجرا کند که با اجرای مکانیسم‌های احراز هویت کاربر و سیاست‌های مجوز کاربر برای اطمینان از اینکه فقط پرسنل مجاز می‌توانند به اطلاعات دسترسی داشته باشند، امکان پذیر کند. اما با گسترش الگوریتم‌های هوش مصنوعی، یکی از موارد استفاده از این فناوری، بکارگیری آن در حفظ امنیت هوش مصنوعی در سلامت است.

۵-۱- مولفه‌های کلیدی امنیت داده‌ها

مؤلفه‌های کلیدی امنیت داده‌ها شامل اقدامات و شیوه‌های مختلفی است که برای محافظت از داده‌های دیجیتال از دسترسی، افشا، تغییر یا تخریب غیرمجاز طراحی شده‌اند. این اجزا برای اطمینان از محرمانه بودن، یکپارچگی و در دسترس بودن داده‌ها با هم کار می کنند. این موارد بطور خلاصه عبارتند از:

کنترل دسترسی: مکانیسم‌های کنترل دسترسی تعیین می‌کنند که چه کسی مجاز به دسترسی به داده‌های خاص است و چه اقداماتی مجاز است انجام دهد. این شامل احراز هویت کاربر (تأیید هویت کاربران)، مجوز (اعطای مجوزها و امتیازات مناسب) و محدودیت‌های دسترسی بر اساس نقش‌ها یا ویژگی‌ها است.

رمزگذاری: رمزگذاری شامل تبدیل داده‌ها به قالب غیرقابل خواندن با استفاده از الگوریتم‌های رمزنگاری برای جلوگیری از دسترسی غیرمجاز است. رمزگذاری داده‌ها را هم در حین انتقال (مثلاً از طریق شبکه) و هم در حالت استراحت (مانند ذخیره شده در دستگاه‌ها یا سرورها) محافظت می‌کند. فقط اشخاص مجاز دارای کلید رمزگشایی می‌توانند به داده‌های رمزگذاری شده دسترسی داشته باشند.

احراز هویت: احراز هویت کاربران یا سیستم‌هایی را که تلاش میکنند به داده‌ها یا منابع دسترسی داشته باشند تأیید می‌کند. روش‌های رایج احراز هویت شامل گذرواژه‌ها، بیومتریک (به عنوان مثال، اسکن اثر انگشت یا عنبیه)، نشانه‌ها و احراز هویت چند عاملی (که نیاز به چندین اشکال تأیید هویت دارد).

یکپارچگی داده‌ها: یکپارچگی داده تضمین می کند که داده‌ها در طول چرخه عمر خود دقیق، کامل و بدون تغییر باقی میمانند. تکنیک‌هایی مانند اعتبارسنجی داده‌ها، جمع‌بندی‌های چک و امضای دیجیتال، صحت داده‌ها را تأیید می‌کنند و هرگونه تغییر یا دستکاری غیرمجاز را شناسایی می‌کنند.

حسابرسی و نظارت: مکانیزم‌های حسابرسی و نظارت فعالیت‌های مربوط به دسترسی، اصلاح و استفاده از داده‌ها را ردیابی و ثبت می کنند. گزارش‌های حسابرسی اطلاعاتی مانند اینکه چه کسی به داده‌ها دسترسی داشته، چه تغییراتی ایجاد شده است و چه زمانی این اقدامات انجام شده است را ضبط می‌کند. ابزارهای نظارتی به طور مداوم الگوهای دسترسی به داده‌ها را تجزیه و تحلیل می کنند و رفتار مشکوک یا غیرعادی را تشخیص می دهند.

امنیت فیزیکی: اقدامات امنیتی فیزیکی با ایمن سازی زیرساخت فیزیکی که داده‌ها در آن ذخیره یا پردازش می شوند، داده‌ها را از دسترسی غیرمجاز، سرقت یا آسیب محافظت می کند. این شامل کنترل‌های دسترسی به مراکز داده، اتاق سرور و سایر

مناطـق حسـاس و همچنیـن اقداماتـی ماننـد قفل‌هـا، دوربین‌هـای نظارتـی و کنترل‌هـای محیطـی اسـت.

سیاسـت‌ها و رویه‌هـای امنیتـی: سیاسـت‌های امنیتـی قوانیـن، دسـتورالعمل‌ها و رویه‌هایـی را بـرای حفاظـت از داده‌هـا و مدیریـت ریسـک‌های امنیتـی در یـک سـازمان تعریـف می‌کننـد. ایـن خط‌مشـی‌ها بـه موضوعاتـی ماننـد طبقه‌بنـدی داده‌هـا، اسـتفاده قابـل قبـول، مدیریـت رمـز عبـور، پاسـخ بـه حادثـه و مسـئولیت‌های کارکنـان می‌پردازنـد. رویه‌هـای امنیتـی مراحـل خاصـی را بـرای اجـرای کنترل‌هـای امنیتـی و واکنـش بـه حـوادث امنیتـی مشـخص مـی کنـد.

۵-۲- جایگاه هوش مصنوعی در امنیت داده

امـروزه هـوش مصنوعـی بـه طـور فزاینـده ای در امنیـت داده‌هـا بـرای تقویـت تشـخیص تهدیـد، پاسـخ و وضعیـت کلـی امنیـت سـایبری اسـتفاده مـی شـود. یکـی از کاربردهـای اصلـی در بکارگیـری هـوش مصنوعـی در امنیـت داده بـه تشـخیص و تجزیـه و تحلیـل تهدیـد بـر می‌گـردد. سیسـتم‌های تشـخیص تهدیـد مبتنـی بـر هـوش مصنوعـی از الگوریتم‌هـای یادگیـری ماشـین بـرای تجزیـه و تحلیـل حجـم زیـادی از داده‌هـا، شناسـایی الگوهـا و شناسـایی ناهنجاری‌هایـی کـه نشـان‌دهنده تهدیـدات امنیتـی بالقـوه اسـت، اسـتفاده می‌کننـد. ایـن سیسـتم‌ها می‌تواننـد رفتارهـای مشـکوک ماننـد ترافیـک غیرمعمـول شـبکه، تلاش‌هـای دسترسـی غیرمجـاز یـا آلودگی‌هـای بدافـزار را شناسـایی کننـد و بـه تیم‌هـای امنیتـی هشـدار دهنـد تـا اقدامـی انجـام دهنـد. از طـرف دیگـر، تجزیـه و تحلیـل رفتـاری مبتنـی بـر هـوش مصنوعـی می‌توانـد رفتـار کاربـر و موجودیـت را در سراسـر شـبکه‌ها، سیسـتم‌ها و برنامه‌هـا بـرای ایجـاد الگوهـای رفتـاری پایـه و شناسـایی انحرافاتـی کـه ممکـن اسـت نشـان دهنـده تهدیـدات داخلـی، حسـاب‌های در معـرض خطـر یـا فعالیت‌هـای غیرمجـاز باشـد، شناسـایی کنـد. بـا تجزیـه و تحلیـل تعامـلات کاربـر و الگوهـای دسترسـی، ایـن سیسـتم‌ها می‌تواننـد رفتـار غیرعـادی را شناسـایی کـرده و بـه طـور فعـال خطـرات امنیتـی را کاهـش دهنـد. لـذا، سـازمان‌ها را قـادر می‌سـازد تـا تلاش‌هـای امنیتـی را اولویت‌بنـدی کننـد، منابـع را بـه طـور مؤثـر تخصیـص دهنـد، و بـه طـور فعالانـه بـه تهدیـدات نوظهـور قبـل از تبدیـل شـدن بـه حـوادث امنیتـی رسـیدگی کننـد.

یکـی دیگـر از قابلیت‌هـای هـوش مصنوعـی در امنیـت داده، پاسـخ خـودکار بـه حـوادث مبتنـی بـر شناسـایی، تجزیـه و تحلیـل و پاسـخ خـودکار بـه حـوادث امنیتـی اسـت کـه سـازمان‌ها را قـادر می‌سـازند تـا بـه سـرعت بـه تهدیـدات سـایبری پاسـخ دهنـد و تأثیـر نقض‌هـای امنیتـی را بـه حداقـل برسـانند. ایـن پلتفرم‌هـا می‌تواننـد وظایفـی ماننـد تجزیـه و تحلیـل بدافـزار، شـکار تهدیـد و تریـاژ حادثـه را به‌طـور مسـتقل یـا بـا حداقـل دخالـت انسـان انجـام دهنـد. بعـلاوه، می‌تـوان از ایـن تکنولـوژی بـرای تشـخیص بدافـزار مبتنـی بـر هـوش مصنوعـی برپایـه تجزیـه

و تحلیل رفتار فایل، ترافیک شبکه و فعالیت سیستم برای شناسایی و مسدود کردن نرم‌افزارهای مخرب و تهدیدات دائمی پیشرفته استفاده کرد.

۵-۳- ضرورت بکارگیری هوش مصنوعی در نظام سلامت

بکارگیری هوش مصنوعی در امنیت داده‌های مراقبت‌های بهداشتی امری ضروری و اجتناب ناپذیر است. سازمان‌های مراقبت‌های بهداشتی مقادیر زیادی از اطلاعات حساس بیمار، از جمله پرونده الکترونیک سلامت، داده‌های تصویربرداری پزشکی، داده‌های ژنومی و غیره را تولید و ذخیره می کنند. مدیریت و ایمن سازی این داده‌ها به دلیل حجم و پیچیدگی آن به طور فزاینده ای چالش برانگیز می شود. هوش مصنوعی می‌تواند به تجزیه و تحلیل، طبقه‌بندی و محافظت مؤثرتر از این داده‌ها کمک کند و خطر نقض داده‌ها و دسترسی غیرمجاز را کاهش دهد. از طرف دیگر، تهدیدات سایبری که سازمان‌های مراقبت‌های بهداشتی را هدف قرار می دهند روز به روز پیچیده تر و مکرر می شوند. عوامل مخرب از تکنیک‌های پیشرفته‌ای مانند باج‌افزار، فیشینگ، و تهدیدات داخلی برای سوءاستفاده از آسیب‌پذیری‌ها و سرقت اطلاعات حساس بیمار استفاده می‌کنند. سیستم‌های تشخیص و پاسخ تهدید مبتنی بر هوش مصنوعی می‌توانند به سازمان‌های مراقبت‌های بهداشتی کمک کنند تا این تهدیدات را سریع‌تر و دقیق‌تر شناسایی کرده و به آنها پاسخ دهند و تأثیر حوادث امنیتی و نقض داده‌ها را به حداقل برسانند.

یکی از نکات قابل تامل در حوزه سلامت، کمبود متخصصان امنیت سایبری ماهر و خبره می‌باشد که منجر می‌شود صنعت مراقبت‌های بهداشتی قادر به رسیدگی به ماهیت پیچیده و در حال تحول تهدیدات سایبری هستند، نباشند. هوش مصنوعی می‌تواند با خودکار کردن وظایف امنیتی معمول، تجزیه و تحلیل حجم زیادی از داده‌های امنیتی، و ارائه بینش‌های عملی به تیم‌های امنیتی، تخصص انسان را افزایش دهد. این امر به سازمان‌های مراقبت‌های بهداشتی امکان می‌دهد تا قابلیت‌های امنیت سایبری خود را بدون تکیه صرف به منابع انسانی افزایش دهند. علاوه بر آن، رویکردهای امنیتی سنتی، مانند سیستم‌های مبتنی بر قانون و تشخیص مبتنی بر امضا، دیگر برای مبارزه با تهدیدات سایبری مدرن که دائماً در حال تغییر و تطبیق هستند، کافی نیستند. هوش مصنوعی سازمان‌های مراقبت‌های بهداشتی را قادر می‌سازد تا با تجزیه و تحلیل حجم زیادی از داده‌ها، شناسایی الگوهای نشان‌دهنده فعالیت‌های مخرب و ایجاد هشدارهای به موقع به تیم‌های امنیتی، حوادث امنیتی را در زمان واقعی شناسایی و به آنها پاسخ دهند. این رویکرد پیشگیرانه به کاهش تأثیر نقض امنیت و به حداقل رساندن آسیب به بیمار کمک می کند.

به طور کلی، استفاده از هوش مصنوعی در امنیت داده‌های مراقبت‌های بهداشتی برای

محافظت از اطلاعات حساس بیمار، حفاظت از زیرساخت‌های مراقبت‌های بهداشتی و اطمینان از رعایت الزامات قانونی ضروری است. با استفاده از فناوری‌های هوش مصنوعی، سازمان‌های مراقبت‌های بهداشتی می‌توانند قابلیت‌های امنیت سایبری خود را افزایش دهند، تهدیدات سایبری را به طور مؤثرتری شناسایی و به آنها پاسخ دهند، و خطرات مرتبط با نقض داده‌ها و حوادث امنیتی را کاهش دهند.

۵-۴- تکنیک‌های هوش مصنوعی در امنیت داده

تا کنون چندین تکنیک هوش مصنوعی پیشنهاد شده است که معمولاً در امنیت داده‌ها برای شناسایی و کاهش تهدیدات سایبری استفاده می شود. یادگیری ماشین، یکی از رایج ترین تکنیکها در این حوزه است. یادگیری ماشین شامل الگوریتم‌های آموزشی برای تشخیص الگوها و پیش بینی بر اساس داده‌ها است. در امنیت داده‌ها، الگوریتم‌های یادگیری ماشین برای تجزیه و تحلیل حجم زیادی از داده‌های امنیتی، مانند گزارش‌ها، ترافیک شبکه، و فعالیت نقطه پایانی، برای شناسایی الگوهای نشان‌دهنده تهدیدات سایبری استفاده می‌شوند. تکنیک‌های یادگیری ماشین شامل یادگیری تحت نظارت (به عنوان مثال، طبقه بندی، رگرسیون)، یادگیری بدون نظارت (به عنوان مثال، خوشه بندی، تشخیص ناهنجاری)، و یادگیری تقویتی است. تشخیص ناهنجاری از موارد دیگر در امنیت داده است. تکنیک‌های تشخیص ناهنجاری، انحرافات از رفتار عادی یا الگوهای مورد انتظار را که ممکن است نشان دهنده حوادث یا تهدیدات امنیتی باشد، شناسایی می کند. الگوریتم‌های تشخیص ناهنجاری مبتنی بر هوش مصنوعی، مانند خوشه‌بندی، نزدیک‌ترین همسایه و جنگل جداسازی، داده‌ها را برای شناسایی نقاط پرت یا ناهنجاری‌هایی که نیاز به بررسی بیشتر دارند، تجزیه و تحلیل می‌کنند. تشخیص ناهنجاری را می توان در موارد مختلف استفاده از امنیت، از جمله تشخیص نفوذ شبکه، تشخیص تهدیدات داخلی و تشخیص تقلب اعمال کرد. یادگیری عمیق، به عنوان یکی از زیر شاخه‌های اصلی یادگیری ماشین،) برای یادگیری الگوها و نمایش‌های پیچیده از داده‌ها بکار برده می‌شود.

تکنیک‌های یادگیری عمیق، مانند شبکه‌های عصبی کانولوشن (CNN)، شبکه‌های عصبی تکراری (RNN)، و شبکه‌های متخاصم تولیدی (GANs)، در امنیت داده‌ها برای کارهایی مانند تشخیص تصویر، تشخیص بدافزار و تشخیص نفوذ استفاده می‌شوند. مدل‌های یادگیری عمیق می‌توانند به‌طور خودکار ویژگی‌های سلسله مراتبی را از داده‌های خام بیاموزند و قابلیت‌های تشخیص تهدید دقیق‌تر و مقیاس‌پذیرتر را ممکن می‌سازند. یادگیری تقویتی شامل آموزش الگوریتم‌هایی برای تصمیم گیری متوالی در یک محیط برای به حداکثر رساندن پاداش تجمعی است. در امنیت داده‌ها، تکنیک‌های یادگیری تقویتی را می‌توان برای توسعه سیاست‌های امنیتی تطبیقی، سیستم‌های پاسخ به

تهدید مستقل، و مکانیسم‌های کنترل دسترسی پویا مورد استفاده قرار داد. الگوریتم‌های یادگیری تقویتی از بازخورد و تجربه یاد می گیرند تا تصمیمات امنیتی را بهینه کنند و با تغییر چشم اندازهای تهدید در زمان واقعی سازگار شوند. بعلاوه، شبکه‌های بیزی مدل‌های گرافیکی احتمالی هستند که وابستگی‌های بین متغیرهای تصادفی را نشان می‌دهند. شبکه‌های بیزی برای استدلال احتمالی، ارزیابی ریسک و تصمیم گیری در شرایط عدم قطعیت استفاده می شود. تکنیک‌های استنتاج بیزی، تحلیلگران امنیتی را قادر می‌سازد تا روابط پیچیده بین رویدادهای امنیتی را مدل‌سازی کنند، احتمال سناریوهای مختلف حمله را ارزیابی کنند و اقدامات پاسخ را بر اساس استدلال احتمالی اولویت‌بندی کنند. این تکنیک‌های هوش مصنوعی، در میان سایر روش‌ها، در پیشرفت قابلیت‌های امنیت داده‌ها، افزایش قابلیت‌های شناسایی و پاسخ به تهدید، و کاهش خطرات امنیت سایبری در یک چشم‌انداز تهدید به‌طور فزاینده پیچیده و پویا، مفید هستند. با استفاده از فناوری‌های هوش مصنوعی، سازمان‌ها می‌توانند تخصص انسانی را افزایش دهند، عملیات امنیتی را خودکار کنند و وضعیت کلی امنیت سایبری خود را تقویت کنند.

۵-۵- جمع بندی

استفاده از هوش مصنوعی در امنیت داده‌های مراقبت‌های بهداشتی به دلیل چندین عامل به طور فزایندهای ضروری می‌شود. اولاً، سازمان‌های مراقبت‌های بهداشتی مقادیر زیادی از اطلاعات حساس بیمار، از جمله پرونده‌های سلامت الکترونیکی، داده‌های تصویربرداری پزشکی، داده‌های ژنومی و غیره را تولید و ذخیره می‌کنند. مدیریت و ایمن سازی این داده‌ها به دلیل حجم و پیچیدگی آن به طور فزایندهای چالش برانگیز می‌شود. با گسترش سیستم‌های مراقبت‌های بهداشتی دیجیتال و پذیرش فناوری‌های نوظهور مانند پزشکی از راه دور و دستگاه‌های پوشیدنی، میزان داده‌های تولید شده به طور تصاعدی در حال افزایش است. این رشد تصاعدی در داده‌های مراقبت‌های بهداشتی چالش‌های مهمی را برای رویکردهای سنتی امنیت داده‌ها ایجاد می‌کند، که ممکن است برای همگام شدن با چشم‌انداز تهدید ایجاد کرده و همراهی نداشته باشد. هوش مصنوعی می‌تواند با ارائه راه‌حل‌های امنیتی مقیاس‌پذیر و تطبیقی که می‌تواند داده‌های مراقبت‌های بهداشتی را به طور مؤثرتری تجزیه و تحلیل، طبقه‌بندی و محافظت کند، به رفع این چالش‌ها کمک کند. با استفاده از تجزیه و تحلیل مبتنی بر هوش مصنوعی و الگوریتم‌های یادگیری ماشینی، سازمان‌های مراقبت‌های بهداشتی می‌توانند بینش عمیق‌تری در مورد داده‌های خود به دست آورند، الگوهای نشان‌دهنده تهدیدات امنیتی را شناسایی کنند و پیش از اینکه به حوادث امنیتی تبدیل شوند، به طور فعال خطرات را کاهش دهند. ثانیا، تهدیدات سایبری که سازمان‌های مراقبت‌های بهداشتی را هدف قرار

می‌دهند پیچیده‌تر و مکرر می‌شوند. عوامل مخرب، از جمله مجرمان سایبری، بازیگران دولت-ملت، و تهدیدهای داخلی، به دلیل ارزش و پتانسیل بالای آن برای بهره برداری، به طور فزاینده ای سیستم‌های مراقبت‌های بهداشتی و داده‌های بیماران را هدف قرار می دهند. نقض داده‌های مراقبت‌های بهداشتی می‌تواند عواقب شدیدی هم برای بیماران و هم برای سازمان‌های مراقبت‌های بهداشتی داشته باشد، از جمله خسارات مالی، آسیب به شهرت، و مسئولیت‌های قانونی. علاوه بر این، ماهیت حساس داده‌های مراقبت‌های بهداشتی، که اغلب شامل اطلاعات سلامت شخصی و اطلاعات بهداشتی محافظت‌شده می‌شود، آن را به یک هدف جذاب برای مجرمان سایبری تبدیل می‌کند که به دنبال ارتکاب سرقت هویت، کلاهبرداری یا اخاذی هستند. در سال‌های اخیر، سازمان‌های مراقبت‌های بهداشتی با تعداد فزاینده‌ای از تهدیدات سایبری، از جمله حملات باج‌افزار، کمپین‌های فیشینگ، تهدیدات داخلی و حملات زنجیره تامین مواجه شده‌اند. این حملات می‌توانند عملیات مراقبت‌های بهداشتی را مختل کنند، مراقبت از بیمار را به خطر بیندازند و اعتماد به سیستم مراقبت‌های بهداشتی را از بین ببرند. سیستم‌های تشخیص و پاسخ تهدید مبتنی بر هوش مصنوعی می‌توانند به سازمان‌های مراقبت‌های بهداشتی کمک کنند تا این تهدیدات را سریع‌تر و دقیق‌تر شناسایی کرده و به آنها پاسخ دهند و تأثیر حوادث امنیتی و نقض داده‌ها را به حداقل برسانند. ثالثاً، کمبود متخصصان امنیت سایبری ماهر، چالش مهمی را برای سازمان‌های مراقبت‌های بهداشتی ایجاد می‌کند که به دنبال ارتقای قابلیت‌های امنیت سایبری خود هستند. شکاف مهارت‌های امنیت سایبری، که به اختلاف بین تقاضا برای استعدادهای امنیت سایبری و در دسترس بودن متخصصان واجد شرایط اشاره دارد، به‌ویژه در صنعت مراقبت‌های بهداشتی شدید است. بر اساس گزارش‌های صنعت، انتظار می‌رود تقاضا برای متخصصان امنیت سایبری در مراقبت‌های بهداشتی از عرضه پیشی بگیرد و منجر به کمبود فزاینده پرسنل ماهر شود. این کمبود استعدادهای امنیت سایبری می تواند توانایی سازمان‌های مراقبت‌های بهداشتی را برای مقابله موثر با تهدیدات سایبری رو به رشدی که با آن مواجه هستند، مختل کند. هوش مصنوعی می‌تواند به پر کردن این شکاف مهارتی با خودکار کردن وظایف امنیتی معمول، افزایش تخصص انسانی، و امکان دادن به سازمان‌های مراقبت‌های بهداشتی برای انجام کارهای بیشتر با منابع محدود کمک کند. راه‌حل‌های امنیتی مبتنی بر هوش مصنوعی می‌توانند حجم زیادی از داده‌های امنیتی را تجزیه و تحلیل کنند، الگوهای نشان‌دهنده تهدیدات امنیتی را شناسایی کنند، و بینش‌های عملی را به تیم‌های امنیتی ارائه دهند و به آن‌ها اجازه می‌دهند تا تلاش‌های خود را بر روی وظایف استراتژیک‌تر و حوادث امنیتی با اولویت بالا متمرکز کنند. علاوه بر این، چشم انداز نظارتی حاکم بر امنیت داده‌های مراقبت‌های بهداشتی به طور فزاینده ای پیچیده و دقیق می شود. سازمان‌های مراقبت‌های بهداشتی مشمول طیف گسترده ای

از مقـررات و الزامـات انطبـاق بـا هـدف حفاظـت از حریـم خصوصـی بیمـار و تضمیـن امنیـت داده‌هـای مراقبت‌هـای بهداشـتی هسـتند. در ایـالات متحـده، قانـون قابـل حمـل و پاسـخگویی بیمـه سـلامت (HIPAA) الزاماتـی را بـرای حفاظـت از اطلاعـات بهداشـتی محافظـت شـده (PHI) ایجـاد مـی کنـد و مجازات‌هـای قابـل توجهـی را بـرای عـدم انطبـاق اعمـال مـی کنـد. بـه طـور مشـابه، مقـررات عمومـی حفاظـت از داده‌هـا (GDPR) در اتحادیـه اروپـا الزامـات سـختگیرانه ای را بـرای پـردازش و حفاظـت از داده‌هـای شـخصی، از جملـه داده‌هـای مراقبت‌هـای بهداشـتی، تحمیـل مـی کنـد. عـدم رعایـت ایـن مقـررات مـی توانـد منجـر بـه مجازات‌هـای شـدید از جملـه جریمـه، مسـئولیت‌های قانونـی و آسـیب بـه شـهرت شـود. راه‌حل‌هـای مدیریـت انطبـاق مبتنـی بـر هـوش مصنوعـی می‌تواننـد بـه سـازمان‌های مراقبت‌هـای بهداشـتی کمـک کننـد تـا بـا خودکارسـازی ارزیابی‌هـای انطبـاق، نظـارت بـر کنترل‌هـای دسترسـی بـه داده‌هـا و تولیـد گزارش‌هـای حسابرسـی، از پایبنـدی بـه الزامـات قانونـی اطمینـان حاصـل کننـد. بـا اسـتفاده از فناوری‌هـای هـوش مصنوعـی، سـازمان‌های مراقبت‌هـای بهداشـتی می‌تواننـد فرآیندهـای انطبـاق را ساده‌سـازی کننـد، خطـرات انطبـاق را کاهـش دهنـد و تعهـد خـود را بـه حفاظـت از حریـم خصوصـی و امنیـت بیمـار نشـان دهنـد. در نتیجـه، اسـتفاده از هـوش مصنوعـی (AI) در داده‌هـای مراقبت‌هـای بهداشـتی

در نتیجـه، اسـتفاده از هـوش مصنوعـی (AI) در امنیـت داده‌هـای مراقبت‌هـای بهداشـتی بـرای حفاظـت از اطلاعـات حسـاس بیمـار، حفاظـت از زیرسـاخت‌های مراقبت‌هـای بهداشـتی و اطمینـان از انطبـاق بـا الزامـات نظارتـی ضـروری اسـت. راه‌حل‌هـای امنیتـی مبتنـی بـر هـوش مصنوعـی می‌تواننـد حجـم زیـادی از داده‌هـای امنیتـی را تجزیـه و تحلیـل کننـد، الگوهـای نشـان‌دهنده تهدیـدات امنیتـی را شناسـایی کننـد، و بینش‌هـای عملـی را بـه تیم‌هـای امنیتـی ارائـه دهنـد، و آنهـا را قـادر می‌سـازد تـا تهدیـدات سـایبری را بـه طـور مؤثرتـری شناسـایی و بـه آنهـا پاسـخ دهنـد. بـا اسـتفاده از فناوری‌هـای هـوش مصنوعـی، سـازمان‌های مراقبت‌هـای بهداشـتی می‌تواننـد قابلیت‌هـای امنیـت سـایبری خـود را افزایـش دهنـد، خطـرات مربـوط بـه نقـض داده‌هـا و حـوادث امنیتـی را کاهـش دهنـد و از حریـم خصوصـی بیمـار و اعتمـاد بـه سیسـتم مراقبت‌هـای بهداشـتی محافظـت کننـد.