Original Article **Open Access**

Health Law Journal

2024; 2: e1

International ThinkTank of Human Dignity | The Bioethics and Health Law Institute | The Iranian Association of Medical Law

Identifying Artificial Intelligence Cyber Security Challenges in Smart Medicine

Mahmoud Abbasi[1], Mehrdad Teymouri[1*]

1. Medical Ethics and Law Research Center, Shahid Beheshti University of Medical Sciences, Tehran, Iran.

ABSTRACT

Background and Aim: Today, artificial intelligence technology seeks to make medicine smarter, which is managed and exploited through this control, considering that the vital information of the health system is also transferred to this space or basically formed in this space; Therefore, the purpose of this research is to identify the cyber security challenges of artificial intelligence in smart medicine and provide cyber defense strategies.

Methods: This study was conducted in the months of August to October 2023. The sources of evidence were PubMed, Scopus and Web of Science databases, articles published in English and the source of authors in Farsi in the years 2016-22; which is a guide to understanding the nature through extensive literature review, analysis, scientific research and opinions of leading people in this field.

Ethical Considerations: In all stages of writing the present research, while respecting the originality of the texts, honesty and trustworthiness have been observed.

Results: Based on the findings, the main challenges of smart medicine include cyber security in remote treatment, endpoint device cyber security, lack of security awareness and human error in cyber security, which in line with cyber defense strategies in securing the remote work environment, device security management The final point, increased security awareness and increased security controls were presented.

Conclusion: Cyber problems have challenged the flexibility of smart medical information systems, affecting our ability to achieve health; Therefore, the management, control and maintenance of this space requires double attention. Due to the necessity of control, management and exploitation of cyber spaces and timely presence and performance in the field of cyber defense is essential.

Keywords: Cyber Security; Cyber Defense; Artificial Intelligence; Smart Health; Smart Medicine

Corresponding Author: Mehrdad Teymouri; **Email:** mehrdadteymoori1@gmail.com

Received: April 09, 2024; **Accepted:** July 12, 2024; **Published Online:** July 31, 2024

Please cite this article as:

Abbasi M, Teymouri M. Identifying Artificial Intelligence Cyber Security Challenges in Smart Medicine. Health Law Journal. 2024; 2: e1.

دسترسی آزاد | مقاله پژوهشی

مجله حقوق سلامت

دوره دوم، ۱۴۰۳

شناسایی چالش‌های امنیت سایبری هوش مصنوعی در پزشکی هوشمند

محمود عباسی[۱]، مهرداد تیموری[۱*]

۱. مرکز تحقیقات اخلاق و حقوق پزشکی، دانشگاه علوم پزشکی شهید بهشتی، تهران، ایران.

چکیده

زمینه و هدف: امروزه فناوری هوش مصنوعی درصدد هوشمندسازی پزشکی است که از طریق این کنترل، مدیریت و بهره‌برداری می‌شوند، با توجه به اینکه اطلاعات حیاتی نظام سلامت نیز به این فضا منتقل و یا اساساً در این فضا، شکل می‌گیرد، لذا هدف از پژوهش حاضر شناسایی چالش‌های امنیت سایبری هوش مصنوعی در پزشکی هوشمند و ارائه راهبردهای پدافند سایبری است.

روش: این مطالعه در ماه‌های آگوست تا اکتبر ۲۰۲۳ انجام شده است. منابع شواهد پایگاه‌های اطلاعاتی PubMed، Scopus و Web of Science مقالات منتشرشده به زبان انگلیسی و منبع نویسندگان به زبان فارسی در سال‌های ۲۲-۲۰۱۶ بودند که از طریق مرور ادبیات گسترده، تجزیه و تحلیل، تحقیقات علمی و نظرات افراد پیشرو در این حوزه و راهنمای درک ماهیت است.

ملاحظات اخلاقی: در تمام مراحل نگارش پژوهش حاضر، ضمن رعایت اصالت متون، صداقت و امانتداری رعایت شده است.

یافته‌ها: بر اساس یافته‌ها چالش‌های اصلی پزشکی هوشمند شامل امنیت سایبری در درمان از راه دور، امنیت سایبری دستگاه نقطه پایانی، عدم آگاهی امنیتی و خطای انسانی در امنیت سایبری می‌باشند که در راستای راهبردهای پدافند سایبری در ایمن‌کردن محیط کار از راه دور، مدیریت امنیت دستگاه نقطه پایانی، افزایش آگاهی امنیتی و افزایش کنترل‌های امنیتی ارائه شدند.

نتیجه‌گیری: مشکلات سایبری انعطاف‌پذیری سیستم اطلاعات پزشکی هوشمند را به چالش کشیده است که بر توانایی ما برای دستیابی به سلامت تأثیر گذاشته است. بنابراین مدیریت، کنترل و صیانت از این فضا نیازمند توجه مضاعف است. با توجه به ضرورت کنترل، مدیریت و بهره‌برداری از فضاهای سایبری و حضور و عملکرد به موقع در حوزه پدافند سایبری امری ضروری است.

واژگان کلیدی: امنیت سایبری؛ پدافند سایبری؛ هوش مصنوعی؛ سلامت هوشمند؛ پزشکی هوشمند

نویسنده مسئول: مهرداد تیموری؛ **پست الکترونیک:** mehrdadteymoori1@gmail.com

تاریخ دریافت: ۱۴۰۳/۰۱/۲۱؛ **تاریخ پذیرش:** ۱۴۰۳/۰۴/۲۲؛ **تاریخ انتشار:** ۱۴۰۳/۰۵/۱۰

خواهشمند است این مقاله به روش زیر مورد استناد قرار گیرد:

Abbasi M, Teymouri M. Identifying Artificial Intelligence Cyber Security Challenges in Smart Medicine. Health Law Journal. 2024; 2: e1.

مقدمه

با توجه به پیشرفت فناوری هوش مصنوعی در عصر نوین (Artificial Intelligence) و ایجاد تغییرات در زندگی اجتماعی انسان، امروزه می‌توان گفت که زندگی بشر وارد عصر هوش مصنوعی شده است. ورود به دوران هوش مصنوعی باعث ایجاد تغییراتی در چهارچوب‌های حقوق بشری خواهد شد. استفاده از هوش مصنوعی می‌تواند ضمن رعایت عدالت بهداشتی و درمانی، ارتقای حقوق سلامت را نیز بهبود بخشد. سیستم‌های مراقبت بهداشتی هوشمند همه دست‌اندرکاران نظام سلامت را ملزم به کسب دانش مناسب در مورد آن می‌کند. اینکه چگونه می‌توان از این فناوری‌ها به طور مناسب استفاده کرد و پیامدهای آن‌ها را درک کرد و در مدیریت سلامت به طور کلی و همچنین به صورت موردی در دانش پزشکی که به طور تصاعدی در حال گسترش است. مراقبت‌های بهداشتی و درمانی در حال حاضر در حال تحول دیجیتالی به سمت هوش مصنوعی است. یکی از کاربردهای هوش مصنوعی در توسعه پزشکی هوشمند است، مراقبت‌های بهداشتی و درمانی هوشمند با استفاده از فناوری‌های نوین اطلاعاتی، از طریق هوش مصنوعی و ابزارهایی مانند اینترنت اشیا ((Internet of Things (IoT)، پزشکی سنتی را متحول می‌کند و مراقبت‌های بهداشتی و درمانی در قالب بیمارستان هوشمند، کلینیک پزشکی هوشمند، داروخانه هوشمند و اتاق عمل هوشمند به وجود می‌آیند که این امر در تشخیص دقیق و سریع و کاهش خطاهای پزشکی بسیار مؤثر می‌باشد. بیمارستان‌ها به طورکلی یکی از مهم‌ترین مکان‌ها در درمان و آموزش پزشکی به شمار می‌روند. بیمارستان‌ها دارای قسمت‌های مختلف از ترایاژ گرفته تا داروخانه و بخش‌های درمانی استفاده از هوش مصنوعی در هر یک از بخش‌های بیمارستان کاربرد دارد که از جمله در استفاده از سیستم داروخانه محتمل است که با استفاده از یک برنامه مبتنی بر هوش مصنوعی قبل از رسیدن بیمار به بیمارستان با ارسال اطلاعات از آمبولانس به بیمارستان قسمت‌های مختلف از ترایاژ بخش اتاق عمل و داروخانه با برقراری ارتباط هوش مصنوعی می‌تواند تشخیص‌های لازم را در ادامه روند درمان انجام دهد با آماده‌سازی داروهای موردنیاز، اعلان به بخش جهت آماده‌سازی اعلام به اتاق عمل جهت آماده‌سازی، آماده‌سازی خون در صورت نیاز و اطلاع پزشک از بیماری که تا چند دقیقه دیگر به مرکز درمانی خواهد رسید. این همان فرصت ازدست‌رفته در معالجات پزشکی است که هوش مصنوعی از آن پیشگیری می‌کند (۱).

سیاستگذاران نظام سلامت ممکن است نیاز به تغییر سیاست‌ها داشته باشند تا اجازه دهند فناوری‌های نوین هوش مصنوعی طور گسترده در مراقبت‌های بهداشتی و درمانی مورد استفاده قرار گیرد. با در دسترس‌بودن کلان داده‌ها (Big Data)، یادگیری ماشین (Machine Learning) نقش اساسی در زمینه مراقبت‌های بهداشتی هوشمند ایفا می‌کند (۲). از سوی دیگر، داده‌های پزشکی مانند پرونده سلامت، توالی ژن، داده‌های بیومتریک، تصویر پزشکی بسیار حساس و خصوصی هستند و جمع‌آوری یا انتقال بین سازمان‌های مختلف دشوار است. علاوه بر این، با افزایش آگاهی از امنیت داده‌ها و حریم خصوصی کاربران، امری بسیار مهم و ضروری است (۳). لازم به ذکر است که امنیت مفهومی متغیر و وابسته به زمان و مکان است، اما ویژگی‌های خاص خود را دارد؛ از سویی نیز جرائم سایبری خیلی سریع با تغییرات وضعیت جهانی سازگار می‌شود. مواردی که مربوط به امنیت سایبری است که باید رعایت گردد، چراکه امنیت فضای سایبری که گردش اطلاعات در آن صورت می‌گیرد می‌بایست تأمین شود و از سرقت اطلاعات مراکز بهداشتی و درمانی که برای نظام سلامت می‌تواند حیاتی باشد جلوگیری گردد.

ملاحظات اخلاقی

در پژوهش حاضر جنبه‌های اخلاقی مطالعه کتابخانه‌ای شامل اصالت متون، صداقت و امانتداری رعایت شده است.

روش

این مطالعه در ماه‌های آگوست تا اکتبر ۲۰۲۳ انجام شده است. منابع شواهد پایگاه‌های اطلاعاتی Scopus، PubMed و Web of Science مقالات منتشرشده به زبان انگلیسی و منبع نویسندگان به زبان فارسی در سال‌های ۲۲-۲۰۱۶ بودند که از طریق مرور ادبیات گسترده، تجزیه و تحلیل، تحقیقات علمی و نظرات افراد پیشرو در حوزه هوش مصنوعی در مراقبت‌های بهداشتی و درمانی و ویژگی‌های آن، مبتنی بر روش‌های دیالکتیکی، مقایسه‌ای، تحلیلی، ترکیبی و جامع است.

یافته‌ها

یافته‌های پژوهش حاکی از این است که استفاده فناوری هوش مصنوعی و هوشمندسازی پزشکی می‌تواند بسیار مفید باشد، لیکن همچنان چالش‌هایی نیز در حوزه امنیت سایبری از جمله امنیت سایبری در درمان از راه دور، امنیت سایبری دستگاه نقطه پایانی، عدم آگاهی امنیتی و خطای انسانی در امنیت سایبری وجود دارد. همچنین راهبردهای پدافند سایبری از جمله ایمن‌کردن محیط کار از راه دور، مدیریت امنیت دستگاه نقطه پایانی، افزایش آگاهی امنیتی و افزایش کنترل‌های امنیتی مورد بحث قرار گرفته است.

بحث

۱. مفاهیم اصلی پژوهشی: به منظور تبیین مفاهیم به کاررفته در مقاله حاضر به تعریف مفهوم‌های هوش مصنوعی، امنیت سایبری و پدافند سایبری می‌پردازیم.

۱-۱. هوش مصنوعی: هوش مصنوعی شاخه‌ای از علوم کامپیوتر است که بر خودکارسازی رفتار هوشمند تمرکز دارد. یادگیری ماشینی زیرشاخه‌ای از هوش مصنوعی است که از تکنیک‌های داده‌محور برای کشف الگوها و پیش‌بینی رفتار استفاده می‌کند (۴). هوش مصنوعی چهارچوب‌ها و الگوریتم‌های محاسباتی که می‌توانند چندین کار مرتبط با هوش انسانی از جمله تصمیم‌گیری، ادراک بصری، تشخیص گفتار و استدلال را انجام دهند. هوش مصنوعی شامل چندین روش مانند یادگیری ماشینی، یادگیری عمیق، بینایی کامپیوتری و پردازش زبان طبیعی است. به دیگر سخن هوش مصنوعی شامل بررسی روش‌های استفاده از سیستم‌های مبتنی بر رایانه جهت انجام وظایف یا حل مسائلی است که به طور معمول توسط هوش فیزیولوژیک انسان‌ها انجام می‌شوند.

۱-۲. امنیت سایبری: امنیت سایبری به تمام جنبه‌های حفاظت از یک سازمان و کارکنان و دارایی‌های آن در برابر تهدیدات سایبری اشاره دارد. با رایج‌ترشدن حملات سایبری و پیچیده‌ترشدن شبکه‌های شرکتی، راه حل‌های امنیتی سایبری متنوعی برای کاهش ریسک سایبری شرکت‌ها مورد نیاز است. امنیت سایبری حوزه وسیعی است که چندین رشته را دربر می‌گیرد. می‌توان آن را به هفت رکن اصلی تقسیم کرد که شامل: ۱ـ امنیت شبکه (Network Security)؛ ۲ـ امنیت ابری (Cloud Security)؛ ۳ـ امنیت نقطه پایانی (Endpoint Security)؛ ۴ـ امنیت موبایل (Mobile Security)؛ ۵ـ امنیت اینترنت اشیا (IoT Security)؛ ۶ـ امنیت برنامه (Application Security)؛ ۷ـ اعتماد صفر (Zero Trust) هستند (۵). قرارگرفتن در معرض حملات سایبری از طریق مکانیسم درک تهدید منجر به حمایت بیشتر از مقررات سخت‌گیرانه امنیت سایبری می‌شود (۶).

۱-۳. پدافند سایبری: اصطلاح «پدافند سایبری» به توانایی جلوگیری از حملات سایبری از آلوده‌کردن یک سیستم یا دستگاه رایانه‌ای اشاره دارد. پدافند سایبری مجموعه‌ای از شرایط را ارزیابی می‌کند که تحت آن اقدامات متقابل می‌تواند وسیله مناسبی برای تهاجمی سایبری باشد و هدف دفاع و بازدارندگی، حفاظت از زیرساخت‌های حیاتی است که باید اقدامات متقابلی انجام شود، لذا دفاع فعال و بازدارندگی آن‌ها می‌توانند به عنوان ابزاری برای دفاع از زیرساخت‌های حیاتی باشند (۷). به دیگر سخن پدافند سایبری با استفاده از راهبردها و روش‌های در مورد جنبه‌های استراتژیک، عملیاتی و تاکتیکی حوزه امنیت سایبری و پیشگیری و مقابله با تهدیدات امنیتی سایبری را با اقدام سریع دفع می‌کند.

۲. چالش‌های امنیت سایبری: هوشمندسازی پزشکی باعث می‌شود تا مراقبت‌های بهداشتی و درمانی را دقیق‌تر و کیفیت خدمات بهداشتی و درمانی را بهبود بخشد، لیکن علیرغم تأثیرات مثبت فناوری‌های مبتنی بر هوش مصنوعی چالش‌های نیز در حوزه امنیت سایبری وجود دارد که در لذا در ادامه به مهم‌ترین چالش‌های امنیت سایبری در پزشکی هوشمند اشاره می‌گردد.

۲-۱. امنیت سایبری در درمان از راه دور: در بحث امنیت کار از راه دور از آنجایی که کار از راه دور اکنون یک عنصر جدایی‌ناپذیر از ارائه خدمات مراقبت‌های بهداشتی است، کارکنان بهداشتی برای دسترسی به شبکه‌های داخلی به پروتکل‌های دسکتاپ از راه دور سازمانی و شبکه‌های خصوصی مجازی متکی هستند. با این حال، این‌ها با خطرات خاصی همراه است که دشمنان به دنبال بهره‌برداری از آن هستند. به عنوان مثال (VPN) پروتکل دسکتاپ از راه دور دارای تاریخچه‌ای از مسائل امنیتی است و به طور کلی نباید بدون حفاظت‌های اضافی مانند فایروال، فهرست‌ها دارای آسیب‌پذیری‌های شناخته‌شده و vpn سفید و احراز هویت چندعاملی در دسترس عموم قرار گیرد (۸)، چراکه سیستم‌های بهداشتی و درمانی چه در سمت سرویس‌گیرنده و چه در سمت سرور که سال‌ها توسط مجرمان سایبری مورد سوءاستفاده قرار گرفته است (۹). این هوشمندسازی در ارائه خدمات درمانی و مشاوره از محیط کار از راه دور چالش امنیت سایبری را ایجاد کرده‌اند.

اگرچه روبات‌های انسان‌نما در مراقبت‌های بهداشتی مفید هستند، لیکن برای اطمینان از تعامل موفق با روبات‌های انسان‌نما، ضروری است که عواملی که بر احساس امنیت کاربران تأثیر می‌گذارند، درک شوند. اطمینان از احساس امنیت بیماران به عنوان یک اصل کلیدی مراقبت خوب در نظر گرفته می‌شود (۱۰). از آنجایی که خدمات بهداشتی از انواع دستگاه‌های پزشکی استفاده می‌کنند، اتصال و قابلیت همکاری مشکلاتی را ایجاد می‌کند، زیرا اکنون از محیط شبکه داخلی خدمات بهداشتی خارج از آن قابل دسترسی است. رسانه و نحوه دسترسی مشکلاتی را ایجاد می‌کند، زیرا دسترسی به بخش‌های حساس خدمات بهداشتی را می‌توان از طریق اتصالات شبکه ناامن یا سیستم‌های وصله‌نشده توسط کارکنانی که از راه دور کار می‌کنند، قابل دسترسی بود (۱۱). علاوه بر این، برخی از دستگاه‌های پزشکی از نرم‌افزارهای آماده استفاده می‌کنند، مانند سیستم‌عامل‌های تجاری (به عنوان مثال، نسخه‌های قدیمی‌تر ویندوز). این سیستم‌ها در برابر انواع زیادی از تهدیدات مانند بدافزار، باج‌افزار و... آسیب‌پذیر هستند (۱۲). به طور کلی، صنعت مراقبت‌های بهداشتی به طور قابل توجهی از نظر امنیت سایبری از سایر صنایع عقب است و همراه با کمبود سواد دیجیتال در میان کارکنانی که عمدتاً از خانه کار می‌کنند، آن را به یک هدف برجسته تبدیل می‌کند (۱۴-۱۳). در مواقع اضطراری همچون پاندمی کووید-۱۹ از آنجایی که کارکنان بهداشتی و بیماران از نظر جا به جایی به دلیل قرنطینه محدودیت دارند، کاهش تحرک و بسته‌شدن مرزها باعث می‌شود افراد و سازمان‌ها برای ارائه خدمات بهداشتی ضروری مانند قرار ملاقات، تشخیص و حتی عمل به فناوری روی بیاورند. به عنوان مثال می‌توان به استفاده از خدمات مشاوره الکترونیکی (مشاوره الکترونیکی) برای بیماران و گروه‌های چندرشته‌ای الکترونیکی اشاره کرد، اگرچه این فناوری‌ها مزایای خود را دارند، اما کاربران و گیرندگان این فناوری‌ها را در معرض انواع حملات مانند کمپین‌های فیشینگ و حملات باج‌افزار قرار می‌دهند (۱۵).

۲-۲. امنیت سایبری دستگاه نقطه پایانی: از مهم‌ترین چالش‌های امنیت سایبری در پزشکی هوشمند امنیت سایبری دستگاه نقطه پایانی است. در این خصوص باید خاطرنشان ساخت که یک شبکه (Network) از گروهی از دستگاه‌های کامپیوتری تشکیل‌شده که داده‌ها را مبادله می‌کنند، هریک از این دستگاه‌ها اغلب «نقطه پایانی (Endpoint)» نامیده می‌شوند. نقطه پایانی هر دستگاهی است که به شبکه کامپیوتری متصل می‌شود. لازم به ذکر است که دستگاه‌های زیرساختی که شبکه بر روی آن‌ها اجرا می‌شود، نقاط پایانی محسوب نمی‌شوند، بلکه تجهیزات زیرساختی در نظر گرفته

می‌شوند. این تجهیزات موارد زیر را شامل می‌شوند: روترها (Routers)، سوئیچ‌ها (Switches)، دروازه‌های شبکه (Network Gateways)، فایروال‌ها (Firewalls) و متعادل‌کننده بار (Load Balancers) مهاجمان سعی می‌کنند دستگاه‌های نقاط پایانی را به طور مرتب تحت کنترل خود درآورند یا به آن‌ها نفوذ کنند. آن‌ها ممکن است برای انجام این کار اهداف مختلفی را در ذهن داشته باشند: آلوده‌کردن دستگاه به بدافزار، ردیابی فعالیت کاربر در دستگاه، رمزگذاری یا سرقت اطلاعات موجود در دستگاه جهت باج‌خواهی، استفاده از دستگاه به عنوان بخشی از شبکه مخرب یا همان بات‌نت (Botnet)، استفاده از دستگاه به عنوان نقطه شروع و توسعه آلودگی در شبکه (Move Laterally) و نفوذ به سایر تجهیزات شبکه و... است. مدیریت نقطه پایانی (Endpoint Management) به معنای نظارت بر نقاط پایانی موجود در شبکه است. در واقع باید اطمینان حاصل شود که تنها نقاط پایانی تأیید و احراز هویت‌شده به شبکه دسترسی دارند؛ به این ترتیب، مدیریت نقطه پایانی آن نقاط پایانی را ایمن نموده و نرم‌افزارهایی که روی نقاط پایانی نصب شده (از جمله نرم‌افزارهای غیر امنیتی) را مدیریت می‌کند. نرم‌افزار مدیریت نقطه پایانی گاهی اوقات به صورت متمرکز (Centralized) پیاده‌سازی می‌شود. همچنین می‌توان آن را بر روی هر دستگاه جداگانه نصب نمود تا سیاست‌ها و قوانین امنیتی را اعمال و اجرا کند (۱۶). تعدادی از دستگاه‌های نقطه پایانی که شامل تجهیزات مختلف نظارت بر بیمار هستند که به اینترنت یا شبکه‌های پراکنده قدیمی متصل می‌شوند، اغلب اصلاح نشده‌اند (۱۷). از دیدگاه معماری سازمانی، داشتن یکپارچگی بیشتر در محیط فناوری اطلاعات (IT) از نظر چابکی سازمان مثبت است. با این حال، شبکه را در برابر حملات سایبری مانند فیشینگ ایمیل، باج‌افزار، DDoS و نقض داده‌های شبکه آسیب‌پذیر می‌کند (۱۸). ادغام دستگاه‌های نقطه پایانی جدید با سیستم‌های قدیمی می‌تواند آسیب‌پذیری‌ها را افزایش دهد (۱۹). با این حال، سازمان‌ها بیش از حد به دفاع پیرامونی (آنتی‌ویروس، فایروال‌ها) و سایر اشکال حفاظت اولیه در برابر حملات سایبری متکی هستند (۲۰). این در حالی است که بیشترین تأثیر را بر امنیت سایبری در مراکز بهداشتی و درمانی می‌گذارد، پیچیدگی نقطه پایانی است.

۲-۳. عدم آگاهی امنیتی: یکی دیگر از چالش‌های مهم در پزشکی هوشمند عدم آگاهی امنیتی است. همچنانکه متداول‌ترین اقدامی که در پاسخ به مخرب‌ترین رخنه‌ها یا حملات انجام می‌شود، آموزش یا ارتباطات اضافی کارکنان است (۲۱). بر پایه تحقیقات انجام‌شده کارکنان بهداشتی از عواقب برخی رفتارها آگاهی ضعیفی داشتند و فقدان خط مشی‌ها و تقویت رفتار ایمن وجود دارد. با این حال، افزایش آگاهی امنیت سایبری برای بخش سلامت لازم است تا از خود و بیماران خود در برابر تهدیدات سایبری بالقوه مانند فیشینگ و باج‌افزار محافظت کند. به دلیل فقدان برنامه‌ریزی و آموزش قبلی کارکنان مراقبت‌های بهداشتی به آموزش و حمایت بیشتری نیاز دارند (۲۲). اگر امنیت سایبری از ابتدا در چرخه عمر پروژه ادغام نشود، خطرات همچنان رشد خواهند. قابلیت امنیت سایبری یک دارایی استراتژیک است که هر سازمان بهداشتی باید همراه با مفاهیم ایجاد انعطاف‌پذیری سازمانی و ظرفیت بازیابی از حوادث و درس‌گرفتن از اشتباهات به منظور حفظ تداوم کسب و کار اتخاذ کند (۲۳)، همچنانکه سازمان بهداشت جهانی (WHO) ایمیل‌های فیشینگ حاوی کلمات کلیدی مانند چگونگی اعتبارسنجی منابع اطلاعاتی قابل اعتماد به منظور جلوگیری از حملات باج‌افزار را توصیه کرده است.

۲-۴. خطای انسانی در امنیت سایبری: تحقیقات موجود نشان داده است که اکثر حوادث امنیت اطلاعات مربوط به خطای انسانی است، زمانی که کارکنان مشغول تمرکز بر نجات جان و سازگاری با محیط‌های کاری و فناوری‌های جدید هستند، گرایش به خطای انسانی وجود دارد. با تغییرات ناگهانی در شیوه‌های کاری، قرارگرفتن در معرض استرس برای مدت طولانی، کارکنان را در برابر حیله‌های مخرب و مرتکب اشتباه آسیب‌پذیر می‌کند. بین حجم کار و احتمال بازکردن ایمیل فیشینگ توسط کارکنان مراقبت‌های بهداشتی

رابطه مثبت معنی‌داری وجود دارد. یک مدل نفوذ چندسطحی با استفاده از تکنیک‌های مهندسی اجتماعی برای کشف چگونگی سوءاستفاده مجرمان سایبری برای جلوگیری از حوادث امنیتی مرتبط با خطای انسانی، به ویژه حوادث ناشی از خطای انسانی غیر عمدی ایجاد شده است (۲۴). با استفاده گسترده از دستگاه‌های پزشکی اینترنت اشیا، تهدیدات سایبری را می‌توان از طریق دستگاه‌های آسیب‌پذیر اینترنت اشیا به سیستم‌های فیزیکی ـ سایبری پزشکی معرفی کرد (۲۵)، اگرچه برخی تلاش‌ها در به کارگیری تکنیک تجزیه و تحلیل قابلیت اطمینان برای تجزیه و تحلیل انسانی در زمینه امنیت اطلاعات علل خطای انسانی اصلی انجام شده است (۲۶)، اما چنین رویکردهایی به طور گسترده مورد استفاده قرار نگرفته است.

۳. راهبردهای پدافند سایبری: با توجه به اینکه پزشکی هوشمند در ارزیابی آسیب‌پذیری‌ها و برنامه‌های واکنشی و بازیابی با مسائلی مواجه می‌شوند که درنهایت مستلزم توجه بر امنیت در مراکز بهداشتی و درمانی است، لذا در ادامه راهبردهای پدافند سایبری برای افزایش امنیت سایبری در پزشکی هوشمند مورد بررسی قرار می‌گیرد.

۳-۱. ایمن‌کردن محیط کار از راه دور: در خصوص درمان از راه دور از راهبردهای موجود ایمن‌کردن محیط کار از راه دور است که شامل استفاده از احراز هویت چندعاملی و نظارت بر فعالیت حساب‌های کاربری و لغو دسترسی به حساب‌ها در صورت عدم نیاز است (NHS). به عنوان یک راه حل امنیتی محیطی برای فعال‌کردن علاوه بر این، یک سرویس دیجیتالی جدیدتر و ارائه نظارت امنیتی و دسترسی ایمن برای کارکنان معرفی شد (۲۷). NHS یک پروژه امنیتی محیطی است که یک راه حل امنیتی محیطی برای محافظت در برابر تهدیدات سرویس امنیتی را ارائه می‌دهد.

۳-۲. مدیریت امنیت دستگاه نقطه پایانی: در خصوص امنیت دستگاه نقطه پایانی راهبرد مدیریتی است، لذا به کارکنان بهداشتی توصیه می‌شود که فناوری‌ها و دستگاه‌هایی را که استفاده می‌کنند، محدود کنند تا در طول همه‌گیری‌ها با مقررات امنیتی مانند حمل‌پذیری بیمه سلامت و قانون پاسخگویی مطابقت داشته باشند. همچنانکه ایالات متحده قانون درمان قرن ۲۱ را برای ارتقای قابلیت همکاری سوابق سلامت الکترونیکی و ترویج کنترل بیشتر بیمار بر اطلاعات سلامتی خود و در عین حال محافظت از حریم خصوصی و امنیت سایبری تصویب کرد (۲۸). با این حال، سازمان‌های مراقبت‌های بهداشتی عمدتاً به دفاع پیرامونی (به عنوان مثال، آنتی‌ویروس، فایروال) برای محافظت در برابر حملات سایبری احتمالی پاسخ می‌دهند، لذا پزشکی هوشمند باید سیاست‌های امنیتی و قوانینی را برای مدیریت امنیت سایبری فراهم نماید. قوانین و مقررات برای محافظت از سیستم‌های فیزیکی سایبری پزشکی امری ضروری است.

۳-۳. افزایش آگاهی امنیتی: در خصوص آگاهی امنیتی از راهبردهای موجود افزایش آگاهی امنیتی است که شامل استفاده از برنامه‌های آموزشی امنیت سایبری و کلاس‌های آگاهی سایبری است در یک کلاس آگاهی امنیت سایبری، بخش فناوری اطلاعات ایمیل‌های فیشینگ جعلی را برای کارکنان خود ارسال می‌کند و آموزش‌های بیشتری را برای کسانی که موفق به شناسایی این ایمیل‌ها نمی‌شوند، ارائه می‌کند (۲۹)، اگرچه جهان به اهمیت افزایش آگاهی در مورد حملات سایبری پی برده است، لیکن تحقیقات نشان می‌دهد که جو سازمانی مثبت می‌تواند بر رفتار افراد تأثیر بگذارد (۳۰)، لذا مراکز بهداشتی و درمانی هوشمند می‌بایست برنامه‌های امنیت سایبری برای افزایش سطح آگاهی امنیتی کارکنان داشته باشند.

۳-۴. افزایش کنترل‌های امنیتی: مردم احتمالاً مرتکب اشتباه می‌شوند، به خصوص در زمینه تغییرات در شیوه سنتی کارشان. سازمان‌های مراقبت‌های بهداشتی ملزم به اتخاذ فرهنگ عدم سرزنش در گزارش‌دهی حوادث هستند. بخش بهداشت باید بر تجزیه و تحلیل علت اصلی تمرکز کند (۳۱). در خصوص خطای انسانی از راهبردهای موجود افزایش کنترل‌های امنیتی است؛ کنترل‌های فنی امنیتی اعمال‌شده توسط بخش بهداشت شامل رمزگذاری، احراز هویت و مجوز

برای محافظت از داده‌ها در برابر تهدیدات سایبری است (۳۲). امنیت رمزنگاری برای رسیدگی به اشتراک‌گذاری داده‌ها و ذخیره‌سازی اطلاعات بیمار در سراسر سیستم‌های شبکه استفاده می‌شود (۳۳). رمزگذاری هم‌شکل برای تضمین امنیت قوی و تضمین حریم خصوصی در حالی که امکان تجزیه و تحلیل داده‌های رمزگذاری‌شده و اطلاعات حساس پزشکی را فراهم می‌کند، اعمال می‌شود (۳۴). بلاک‌چین همچنین به دلیل تغییرناپذیری، شفافیت و غیر متمرکزبودن برای تسهیل قابلیت همکاری مراقبت‌های بهداشتی استفاده می‌شود (۳۵). بخش‌بندی و جداسازی شبکه نیز باید توسط بخش بهداشت در نظر گرفته شود (۳۶). با تقسیم‌بندی شبکه، ترافیک شبکه را می‌توان برای محدودکردن و/یا جلوگیری از دسترسی بین مناطق شبکه ایزوله و/یا فیلتر کرد. به عنوان مثال، در صورت به خطرافتادن سیستم‌ها، باید هرگونه فعالیت در سیستم را مسدود کرد، دستگاه‌های آلوده را از هر درایو خارجی یا دستگاه پزشکی جدا کرد و از شبکه آفلاین شد (۳۷).

نتیجه‌گیری

تضمین امنیت در پزشکی هوشمند نشان‌دهنده حفاظت از داده‌ها، اطلاعات و شبکه‌ها در برابر هرگونه حملات و فعالیت‌های مخرب است. با این حال، برخی چالش‌های امنیت سایبری وجود دارند که دستیابی به امنیت را در پزشکی هوشمند پیچیده می‌سازند. سخت‌افزارها و نرم‌افزارهای به کار گرفته‌شده در پزشکی هوشمند، به طور معمول بدون بررسی و آزمایش مناسب و کافی از نظر امنیت سایبری از سوی فروشندگان به فروش می‌رسند، لذا استفاده از این محصولات ناایمن می‌تواند موجب هک‌شدن و ورود داده‌ها و اطلاعات جعلی به سیستم‌ها گردد. همچنین زنجیره تأمین مراقبت‌های بهداشتی و درمانی می‌تواند در برابر حملات سایبری آسیب‌پذیرتر باشد. ما برای ارزیابی چگونگی هوشمندسازی یک مرکز بهداشتی و درمانی، می‌بایست به سطح خودکارسازی و سیستم‌های رایانه‌ای که از آن استفاده می‌کنند و همچنین یکپارچگی سیستم‌ها توجه کنیم. حملات سایبری منجر به تأثیرات منفی بر در دسترس‌بودن خدمات ضروری مراقبت‌های بهداشتی و درمانی شده و سازمان‌های مراقبت‌های بهداشتی و درمانی را در حفاظت از محرمانه‌بودن و یکپارچگی اطلاعات مراقبت‌های بهداشتی و درمانی به چالش می‌کشد، در نتیجه مسائل مرتبط با امنیت سایبری در پزشکی هوشمند، مسائلی مهم هستند و مستلزم تحلیل و بررسی فناوری‌های هوش مصنوعی می‌باشند. بنابراین امنیت، حفظ حریم خصوصی و مسائل مرتبط با آن، موضوعات مهمی هستند، به خصوص اینکه فناوری‌های هوش مصنوعی استفاده‌شده در سیستم‌های پزشکی هوشمند برای حفظ سلامتی و بهبود کیفیت زندگی بسیار مهم هستند.

مشارکت نویسندگان

محمود عباسی: طراحی ایده، مرور و بازبینی متن.
مهرداد تیموری: جمع‌آوری و تجزیه و تحلیل داده‌ها، نگارش اولیه، اصلاح متن و تدوین کلی مقاله.
نویسندگان نسخه نهایی را مطالعه و تأیید نموده و مسئولیت پاسخگویی در قبال پژوهش را پذیرفته‌اند.

تشکر و قدردانی

ابراز نشده است.

تضاد منافع

نویسندگان هیچ‌گونه تضاد منافع احتمالی را در رابطه با تحقیق، تألیف و انتشار این مقاله اعلام نکرده‌اند.

تأمین مالی

نویسندگان اظهار می‌نمایند که هیچ‌گونه حمایت مالی برای تحقیق، تألیف و انتشار این مقاله دریافت نکرده‌اند.

References

1. Abbasi M, Teymouri M. A Review of the Ethical and Legal Challenges of Using Artificial Intelligence in the Health System. Journal of Medical Ethics. 2023; 17(48): 1-11. [Persian]

2. Garg A, Mago V. Role of machine learning in medical research: A survey. Comput Sci Rev. 2021; 40(7): 1-7.

3. Qayyum A, Qadir J, Bilal M, Al-Fuqaha A. Secure and robust machine learning for healthcare: A survey. IEEE Rev Biomed Eng. 2020; 14(1): 156-180.

4. Balthazar P, Harri P, Prater A, Safdar NM. Protecting your patients' interests in the era of big data, artificial intelligence and predictive analytics. Journal of Am Coll Radiol. 2018; 15(3, pt B): 580-586.

5. Available at: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/.

6. Keren LGS, Ryan S, Shay Z, Daphna C. Cyberattacks, cyber threats and attitudes toward cybersecurity policies. Journal of Cybersecurity. 2021; 7(1): 1-11.

7. Katagiri N. Three Conditions for Cyber Countermeasures: Opportunities and Challenges of Active-Defense Operations. The Cyber Defense Review. 2022; 7(3): 79-90.

8. Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin M, Calcavecchia F, Anderson D, et al. Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. BMC Med Inform Decis Mak. 2020; 20(146): 1-10.

9. Offner KL, Sitnikova E, Joiner K, MacIntyre CR. Towards understanding cybersecurity capability in Australian healthcare organisations: A systematic review of recent trends, threats and mitigation. Intelligence and National Security. 2020; 35(4): 556-585.

10. Nyholm L, Santamäki-Fischer R, Fagerström L. Users' ambivalent sense of security with humanoid robots in healthcare. Journal of Informatics for Health & Social Care. 2021; 46(2): 218-226.

11. Jalali MS, Bruckes M, Westmattelmann D, Schewe G. Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. Journal of Med Internet Res. 2020; 22(1): 1-6.

12. Ronquillo J, Erik Winterholler J, Cwikla K, Szymanski R, Levy C. Health IT, hacking and cybersecurity: National trends in data breaches of protected health information. JAMIA Open. 2018; 1(1): 15-19.

13. Sardi A, Rizzi A, Sorano E, Guerrieri A. Cyber Risk in Health Facilities: A Systematic Literature Review. Sustainability. 2020; 12(17): 1-16.

14. Kim D, Choi J, Han K. Risk management-based security evaluation model for telemedicine systems. BMC Med Inform Decis Mak.2020; 20(106): 1-14.

15. Weil T, Murugesan S. IT Risk and Resilience-Cybersecurity Response to Covid-19. Journal of IT Prof. 2022; 22(3): 4-10.

16. Available at: https://www.bitav.ir/what-is-endpoint/.

17. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018; 113(1): 48-52.

18. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. THC. 2017; 25(1): 1-10.

19. Naidoo R. A multi-level influence model of Covid-19 themed cybercrime. European Journal of Information Systems. 2020; 29(3): 306-321.

20. Reagin MJ, Gentry MV. Enterprise Cybersecurity. Frontiers of Health Services Management. 2018; 35(1): 13-22.

21. Coventry L, Branley-Bell D, Sillence E, Magalini S, Mari P, Magkanaraki A, et al. Cyber-risk in health carexploring facilitators and barriers to secure behaviour, in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Copenhagen: 22nd International Conference on Human Computer Interaction; 2020. p.105-122.

22. Kaplan B. Evisiting health information technology ethical, legal and social issues and evaluation: Telehealth/ telemedicine and Covid-19. Int Journal Med Inform. 2020; 143(1): 104239.

23. Jalali M, Russell B, Razak S, Gordon William J. EARS to cyber incidents in health care. Journal of Am Med Inform Assoc. 2029; 26(1): 81-90.

24. Evans M, He Y, Maglaras L, Yevseyeva I, Janicke H. Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. Int Journal Med Inform. 2019; 127(1): 109-119.

25. Chen Y, Ding S, Xu Z, Zheng H, Yang S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. Journal of Med Syst. 2018; 43(1): 1-5.

26. Evans M, He Y, Luo C, Yevseyeva I, Janicke H, Zamani E, et al. Real-Time Information Security

Incident Management: A Case Study Using the IS-CHEC Technique. IEEE Access. 2019; 7(1): 142147-142175.

27. Deebak BD, Al-Turjman F, Nayyar A. Chaotic-map based authenticated security framework with privacy preservation for remote point-of-care. Multimed Tools Appl. 2020; 12(1): 1-26.

28. Hoffman D. Increasing access to care: telehealth during Covid-19. Journal of Law Biosci. 2020; 7(1): 1-2.

29. Gordon W, Wright A, Glynn Robert J, Kadakia J, Mazzone C, Leinbach E, et al. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. Journal of Am Med Inform Assoc. 2019; 26(6): 547-552.

30. Kessler SR, Pindek S, Kleinman G, Andel SA, Spector PE. Information security climate and the assessment of information security risk among healthcare employees. Health Informatics Journal. 2020; 26(1): 461-473.

31. Evans M, He Y, Maglaras L, Janicke H. HEART-IS: A novel technique for evaluating human error-related information security incidents. Computers & Security. 2019; 80(1): 74-89.

32. Yaseen M, Saleem K, Orgun MA, Derhab A, Abbas H, Al-Muhtadi J, et al. Secure sensors data acquisition and communication protection in eHealthcare: Review on the state of the art. Telematics and Informatics. 2018; 35(4): 702-726.

33. Gardiyawasam Pussewalage HS, Oleshchuk VA. Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. International Journal of Information Management. 2016; 36(6): 1161-1173.

34. Raisaro J, McLaren PJ, Fellay J, Cavassini M, Klersy C, Hubaux J. Swiss HIV Cohort Study Are privacy-enhancing technologies for genomic data ready for the clinic? A survey of medical experts of the Swiss HIV Cohort Study. Journal of Biomed Inform. 2018; 79(1): 1-6.

35. Narikimilli NRS, Kumar A, Antu AD, Xie B. Blockchain Applications in Healthcare - A Review and Future Perspective. Edited by Chen Z, Cui C, Palanisamy BB, Zhang LJ. Blockchain - ICBC 2020. ICBC 2020. Lecture Notes in Computer Science. 2020; 12404(1): 198-218.

36. Hakak S, Khan WZ, Imran M, Choo KR, Shoaib M. Have You Been a Victim of Covid-19-Related Cyber Incidents? Survey, Taxonomy and Mitigation Strategies. IEEE Access. 2020; 8(1): 124134-124144.

37. He Y, Aliyu A, Evans M, Luo C. Health Care Cybersecurity Challenges and Solutions under the Climate of Covid-19: Scoping Review. Journal of Med Internet Res. 2021; 23(4): 1-23.