ماهنامه

پالسی نو

A New Pulse

First year - March 2026 No:06

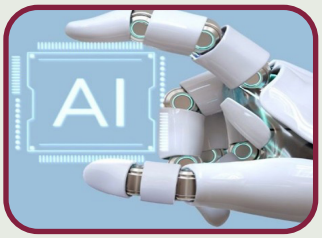
سال اول – شماره ششم – اسفند ۱۴۰۴

... سواد سلامت دیجیتال در بسیاری از کوریکولوم‌های علوم پزشکی به‌صورت پراکنده، ضمنی یا ناکافی مورد توجه قرار گرفته است. در حالی که آموزش مهارت‌های بالینی و دانش زیست‌پزشکی همچنان محور اصلی ... ص ۴

... زیرساخت شبکه برای تشخیص هوشمند بیماری‌ها شامل چند لایه حیاتی است که هر یک نقش منحصربه‌فردی در عملکرد کلی سیستم ایفا می‌کنند ... ص ۱۷

... دیپ‌فیک به‌عنوان یکی از جلوه‌های پیشرفته هوش مصنوعی مبتنی بر یادگیری عمیق، توانایی تولید و دست‌کاری محتوای صوتی و تصویری بسیار واقع‌گرایانه ... ص ۲۴

... کلان‌داده‌ها به مجموعه‌های داده‌ای بسیار بزرگ و پیچیده اشاره دارند که نمی‌توان آن‌ها را با ابزارهای سنتی پردازش کرد. این داده‌ها ... ص ۶

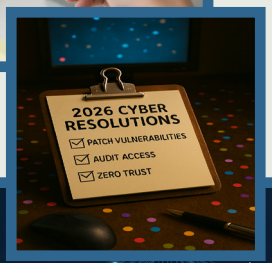


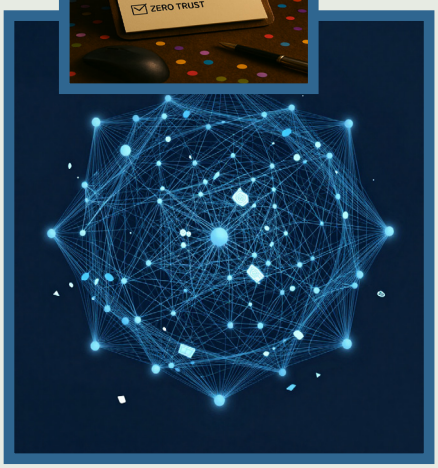
... محدودیت‌هایی در عملکرد هوش مصنوعی هستند که می‌توانند کاربران را به اشتباه بیندازند. اما چرا هوش مصنوعی چنین پاسخ‌هایی تولید می‌کند... ص ۱۴

... طعمه‌گذاری به کنجکاوی انسان، سهل‌انگاری کارکنان و کنترل‌های داخلی ضعیف برای به خطر انداختن سیستم‌ها متکی است... ص ۱۰

بخش قابل توجهی از تصاویر این نشریه، با بهره گیری از ابزارهای هوش مصنوعی تولید شده‌اند.

فهرست مطالب





مدیر مسئول و صاحب امتیاز: دکتر طاها صمد سلطانی

سردبیر: مهندس نویده خدائی

دبیر علمی: دکتر امیر تراب

شورای سیاستگذاری: دکتر احمدرضا جودتی، دکتر سعید اصلان آبادی، دکتر محمدرضا سیاهی، دکتر حسین عبداللهی، دکتر خسرو ادیب‌کیا، دکتر احمد کوشا، دکتر اصغر جعفری روحی، دکتر مهدی نظری.

شورای نویسندگان: مهندس وحید عباس‌زاده، مهندس جواد فرهادی، سیدمحمدحسن الهی، مهندس جواد ملکی، دکتر آیدین محمود علیلو، سوگند حبیبی.

مدیر اجرایی: دکتر سعید سقطی زاد

طراح و برنامه نویس: سیدمحمدحسن الهی

روابط عمومی: الناز هوشیان

سرمقاله

فناوری اطلاعات در گذار از نوآوری هیجانی به بلوغ راهبردی

نویده خدائی
دانشجوی دکتری مدیریت فناوری اطلاعات

با گسترش شتابان فناوری‌های دیجیتال در سال‌های اخیر، بسیاری از سازمان‌ها مرحله‌ای از هیجان‌زدگی فناورانه را تجربه کردند؛ دوره‌ای که در آن تمرکز بیشتر بر آزمودن فناوری‌های نوظهور بود تا بهره‌برداری راهبردی از آن‌ها. امروز اما فضای فناوری اطلاعات در حال ورود به مرحله‌ای پخته‌تر است؛ مرحله‌ای که در آن سازمان‌ها به‌جای دنبال کردن موج فناوری، به دنبال خلق ارزش پایدار، افزایش بهره‌وری و ارتقای تاب‌آوری دیجیتال هستند.

در این گذار، فناوری‌هایی مانند هوش مصنوعی عامل‌محور و سیستم‌های چندعامله نقش پررنگی پیدا کرده‌اند؛ سامانه‌هایی که قادرند به‌صورت خودکار تصمیم‌گیری کرده، وظایف پیچیده را مدیریت کنند و همکاری هوشمند میان اجزای مختلف سازمان را ممکن سازند. همزمان، توسعه مدل‌های زبانی و سامانه‌های هوش مصنوعی تخصصی امکان استفاده دقیق‌تر و ایمن‌تر از هوش مصنوعی را در حوزه‌هایی چون سلامت، آموزش و مدیریت فراهم کرده است.

از سوی دیگر، رشد هوش مصنوعی فیزیکی و ورود آن به ربات‌ها، تجهیزات خودکار و سامانه‌های عملیاتی، مرز میان دنیای دیجیتال و محیط فیزیکی را کمرنگ‌تر کرده و شیوه ارائه خدمات و مدیریت عملیات را دگرگون می‌کند. این تحول بدون زیرساخت‌های قدرتمند پردازشی و پلتفرم‌های محاسباتی پیشرفته ممکن نبود؛ زیرساخت‌هایی که امکان تحلیل داده‌های عظیم و اجرای مدل‌های پیچیده را فراهم می‌کنند.

در کنار این پیشرفت‌ها، موضوع اعتماد دیجیتال به یکی از دغدغه‌های اصلی سازمان‌ها تبدیل شده است. فناوری‌هایی نظیر پردازش محرمانه داده، منشأسنجی دیجیتال و پلتفرم‌های امنیتی مبتنی بر هوش مصنوعی تلاش می‌کنند اطمینان کاربران را نسبت به امنیت داده‌ها، صحت اطلاعات و پایداری خدمات افزایش دهند. همزمان، رویکردهای جدید امنیت سایبری با تمرکز بر پیشگیری از تهدیدها پیش از وقوع، جایگزین روش‌های صرفاً واکنشی شده‌اند.

همچنین، تغییر نگاه سازمان‌ها به محل استقرار داده و زیرساخت‌ها نشان می‌دهد که مدیریت داده دیگر صرفاً موضوعی فنی نیست، بلکه بخشی از راهبرد حاکمیت داده، امنیت ملی و تداوم خدمات محسوب می‌شود. در چنین شرایطی، فناوری اطلاعات از یک ابزار پشتیبان به موتور تحول سازمانی و تصمیم‌سازی راهبردی تبدیل شده است.

آنچه امروز بیش از هر زمان دیگری اهمیت دارد، حرکت به سوی طراحی آگاهانه، مسئولانه و هدفمند خدمات دیجیتال است؛ رویکردی که در آن فناوری، راهبردی برای ارتقای کیفیت زندگی، افزایش کارایی سازمان‌ها و توسعه پایدار خواهد بود.

سواد سلامت دیجیتال:
شایستگی بنیادین در آموزش پزشکی

دکتر امیر تراب میاندوآب
استادیار مدیریت اطلاعات سلامت مرکز تحقیقات آموزش پزشکی

در عصر حاضر که فناوری‌های دیجیتال به‌صورت گسترده در نظام‌های سلامت نفوذ کرده‌اند، توانایی تعامل مؤثر با اطلاعات و ابزارهای دیجیتال به یکی از الزامات حرفه پزشکی تبدیل شده است. سواد سلامت دیجیتال مفهومی است که به مجموعه‌ای از توانمندی‌ها برای جست‌وجو، ارزیابی، فهم و به‌کارگیری اطلاعات سلامت در بسترهای الکترونیکی اشاره دارد. این مفهوم فراتر از مهارت‌های عمومی کار با فناوری است و به‌طور خاص بر استفاده آگاهانه، ایمن و انتقادی از منابع دیجیتال سلامت تمرکز دارد. با توجه به گسترش پرونده‌های الکترونیک سلامت، اپلیکیشن‌های پزشکی، سامانه‌های تله‌مدیسین و ابزارهای مبتنی بر هوش مصنوعی، توجه به این شایستگی در آموزش پزشکی ضرورتی اجتناب‌ناپذیر است.
سواد سلامت دیجیتال نقشی دوگانه در آموزش پزشکی ایفا می‌کند. از یک سو، پزشکان آینده باید خود قادر باشند داده‌ها و اطلاعات دیجیتال را به‌درستی تحلیل و تفسیر کنند و از سوی دیگر، بتوانند بیماران را در استفاده ایمن و مؤثر از ابزارهای دیجیتال سلامت راهنمایی نمایند. شواهد پژوهشی نشان می‌دهد که ضعف در این حوزه می‌تواند به گسترش اطلاعات نادرست، تصمیم‌گیری‌های ناصحیح درمانی و تشدید نابرابری‌های سلامت منجر شود. ازاین‌رو، بسیاری از چارچوب‌های بین‌المللی آموزش علوم پزشکی بر لزوم گنجاندن مؤلفه‌هایی مانند ارزیابی اعتبار منابع آنلاین، اخلاق دیجیتال، حفاظت از داده‌های سلامت و آشنایی با محدودیت‌های فناوری تأکید دارند.

جایگاه سواد سلامت دیجیتال در کوریکولوم علوم پزشکی

بررسی برنامه‌های درسی موجود نشان می‌دهد که سواد سلامت دیجیتال در بسیاری از کوریکولوم‌های علوم پزشکی به‌صورت پراکنده، ضمنی یا ناکافی مورد توجه قرار گرفته است. در حالی که آموزش مهارت‌های بالینی و دانش زیست‌پزشکی همچنان محور اصلی کوریکولوم‌هاست، تحولات دیجیتال نیازمند بازنگری ساختاری در اهداف آموزشی هستند. رویکردهای نوین پیشنهاد می‌کنند که سواد سلامت دیجیتال یا به‌عنوان یک ماژول مستقل و یا به‌صورت تلفیقی در دروس موجود گنجانده شود تا دانشجویان بتوانند ارتباط میان فناوری و مراقبت بالینی را به‌طور عملی تجربه کنند.
تجربه برخی دانشگاه‌های پیشرو نشان می‌دهد که آموزش مبتنی بر پروژه، کار با داده‌های واقعی، و آشنایی کاربردی با سامانه‌های دیجیتال سلامت، اثربخشی بالایی در ارتقای این شایستگی دارد. در این الگوها، دانشجویان نه‌تنها با کارکرد فناوری‌ها آشنا می‌شوند، بلکه به ارزیابی انتقادی پیامدهای اخلاقی، اجتماعی و حرفه‌ای آن‌ها نیز ترغیب می‌گردند. با این حال، چالش‌هایی نظیر کمبود اعضای هیئت علمی متخصص، محدودیت منابع آموزشی و نبود سیاست‌های یکپارچه، از موانع اصلی اجرای مؤثر این رویکرد محسوب می‌شوند. همسوسازی کوریکولوم با استانداردهای بین‌المللی و سرمایه‌گذاری در توانمندسازی اساتید می‌تواند به رفع این چالش‌ها کمک کند.

یادگیری مبتنی بر پلتفرم‌های دیجیتال و هوش مصنوعی در آموزش پزشکی

گسترش پلتفرم‌های دیجیتال و کاربرد هوش مصنوعی، چشم‌انداز آموزش پزشکی را به‌طور قابل توجهی دگرگون کرده است. این فناوری‌ها امکان یادگیری شخصی‌سازی‌شده را فراهم می‌سازند، به‌گونه‌ای که محتوای آموزشی متناسب با سطح دانش و نیازهای هر دانشجو تنظیم می‌شود. شبیه‌سازهای بالینی و محیط‌های یادگیری مجازی، فرصت تمرین ایمن مهارت‌های تشخیصی و تصمیم‌گیری بالینی را ایجاد می‌کنند و می‌توانند مکمل آموزش

حضوری باشند. علاوه بر این، پلتفرم‌های آموزش آنلاین دسترسی به منابع آموزشی را گسترش داده و همکاری علمی میان دانشجویان و اساتید در سطح بین‌المللی را تسهیل می‌نمایند.
در عین حال، بهره‌گیری از این فناوری‌ها بدون مخاطره نیست. اتکای بیش از حد به سامانه‌های هوشمند ممکن است به تضعیف قضاوت بالینی و مهارت‌های ارتباطی منجر شود. همچنین، وجود تورش در الگوریتم‌های هوش مصنوعی، چالش‌های اخلاقی و نگرانی‌های مرتبط با محرمانگی داده‌ها، از مسائل جدی در این حوزه به‌شمار می‌روند. فقدان شواهد کافی درباره اثربخشی آموزشی برخی از این ابزارها نیز ضرورت ارزیابی مستمر و مبتنی بر شواهد را برجسته می‌سازد. در این زمینه، تدوین دستورالعمل‌های اخلاقی، آموزش اساتید و دانشجویان درباره محدودیت‌های فناوری، و توجه به امنیت سایبری از الزامات اساسی است.

جمع‌بندی و پیشنهادها

سواد سلامت دیجیتال به‌عنوان یکی از شایستگی‌های کلیدی قرن بیست‌ویکم، نقش تعیین‌کننده‌ای در کیفیت آموزش پزشکی و کارآمدی نظام سلامت ایفا می‌کند. بازنگری در کوریکولوم علوم پزشکی با هدف ادغام نظام‌مند این شایستگی، می‌تواند پزشکان آینده را برای مواجهه آگاهانه با فناوری‌های دیجیتال و هوش مصنوعی آماده سازد. در این مسیر، تمرکز بر آموزش کاربردی، یادگیری انتقادی و توجه هم‌زمان به ملاحظات اخلاقی و اجتماعی اهمیت ویژه‌ای دارد.
برای نظام آموزش پزشکی در ایران، پیشنهاد می‌شود سیاست‌گذاری آموزشی به‌گونه‌ای انجام گیرد که سواد سلامت دیجیتال به‌عنوان بخشی جدایی‌ناپذیر از شایستگی‌های حرفه‌ای پزشکان تعریف شود. سرمایه‌گذاری در زیرساخت‌های آموزشی دیجیتال، توانمندسازی اعضای هیئت علمی و تدوین چارچوب‌های اخلاقی شفاف، می‌تواند زمینه استفاده ایمن و مؤثر از این فناوری‌ها را فراهم آورد. در صورت تحقق این شرایط، آموزش پزشکی دیجیتال‌محور می‌تواند به ارتقای کیفیت مراقبت، کاهش خطاهای پزشکی و افزایش عدالت در دسترسی به خدمات سلامت منجر شود.

منابع:

1. Ban S, Kim Y, Seomun G. Digital health literacy: A concept analysis. Digital health. 2024 Oct;10:20552076241287894.
2. Zaghloul H, Fanous K, Ahmed L, Arabi M, Varghese S, Omar S, Al-Najjar Y, El-Khoury R, Gray J, Rakab A, Arayssi T. Digital health literacy in patients with common chronic diseases: systematic review and meta-analysis. Journal of medical Internet research. 2025 Aug 25;27:e56231.
3. Ji H, Dong J, Pan W, Yu Y. Associations between digital literacy, health literacy, and digital health behaviors among rural residents: evidence from Zhejiang, China. International Journal for Equity in Health. 2024 Apr 9;23(1):68.
4. Peimani M, Stewart AL, Ghodssi-Ghassemabadi R, Nasli-Esfahani E, Ostovar A. The moderating role of e-health literacy and patient-physician communication in the relationship between online diabetes information-seeking behavior and self-care practices among individuals with type 2 diabetes. BMC Primary Care. 2024 Dec 30;25(1):442.
5. Mukhtar T, Babur MN, Abbas R, Irshad A, Kiran Q. Digital Health Literacy: A systematic review of interventions and their influence on health-care access and sustainable development Goal-3 (SDG-3). Pakistan Journal of Medical Sciences. 2025 Mar;41(3):910.
6. Ogundiya O, Rahman TJ, Valnarov-Boulter I, Young TM. Looking back on digital medical education over the last 25 years and looking to the future: narrative review. Journal of Medical Internet Research. 2024 Dec 19;26:e60312.
7. Hamilton A. Artificial intelligence and healthcare simulation: the shifting landscape of medical education. Cureus. 2024 May 6;16(5).
8. Aydınlar A, Mavi A, Kütükçü E, Kırımlı EE, Alış D, Akın A, Altıntaş L. Awareness and level of digital literacy among students receiving health-based education. BMC Medical Education. 2024 Jan 8;24(1):38.
9. Lixia L, Jun H, Wenhao Y, Ali N. Construction of Digital Literacy Training System for Medical Students in the Age of Healthcare 4.0: Perspective of Educational Ecology. Canadian Journal of Educational and Social Studies. 2024 Jul 11;4(4):15-28.
10. Abou Hashish EA, Alnajjar H. Digital proficiency: assessing knowledge, attitudes, and skills in digital transformation, health literacy, and artificial intelligence among university nursing students. BMC Medical Education. 2024 May 7;24(1):508.

کلان‌داده‌ها و پزشکی داده‌محور

سوگند حبیبی
کارشناسی ارشد فناوری اطلاعات سلامت
کارشناس فناوری اطلاعات سلامت معاونت درمان

در عصر دیجیتال کنونی، جایی که حجم اطلاعات تولیدشده روزانه به طور نمایی افزایش می‌یابد، کلان‌داده‌ها (**Big Data**) به عنوان یکی از کلیدی‌ترین فناوری‌ها ظاهر شده‌اند. کلان‌داده‌ها به مجموعه‌های داده‌ای بسیار بزرگ و پیچیده اشاره دارند که نمی‌توان آن‌ها را با ابزارهای سنتی پردازش کرد. این داده‌ها از منابع گوناگونی مانند سوابق پزشکی بیماران، دستگاه‌های هوشمند پوشیدنی، آزمایش‌های ژنتیکی، تصاویر تشخیصی مانند **MRI** و **CT** اسکن، و حتی اطلاعات جمع‌آوری‌شده از شبکه‌های اجتماعی و اپلیکیشن‌های سلامت سرچشمه می‌گیرند. ویژگی‌های اصلی کلان‌داده‌ها شامل حجم عظیم (که می‌تواند به پتابایت‌ها برسد)، سرعت تولید بالا (مانند داده‌های **real time** از مانیتورهای قلبی)، تنوع فرمت‌ها (از متن و عدد تا تصاویر و ویدیوها)، و نیاز به بررسی اعتبار و کیفیت آن‌ها است. برای مدیریت این داده‌ها، از فناوری‌هایی مانند هوش مصنوعی، یادگیری ماشین و سیستم‌های ابری استفاده می‌شود تا الگوها و **insights** ارزشمندی استخراج گردد.

پزشکی داده‌محور (**Data-Driven Medicine**) نیز رویکردی نوین است که در آن، تصمیم‌گیری‌های پزشکی نه تنها بر اساس تجربه بالینی پزشکان، بلکه بر پایه تحلیل دقیق و علمی این کلان‌داده‌ها صورت می‌پذیرد. برای مثال، پزشکان می‌توانند با بررسی داده‌های هزاران بیمار مشابه، درمان‌های مؤثرتری پیشنهاد دهند یا حتی بیماری‌ها را پیش از بروز علائم پیش‌بینی کنند. این روش، پزشکی را از حالت سنتی و تجربی به سمت یک علم دقیق و شخصی‌سازی‌شده سوق می‌دهد، جایی که هر بیمار بر اساس داده‌های منحصربه‌فرد خود درمان می‌شود. این تحول نه تنها دقت تشخیص را افزایش می‌دهد، بلکه هزینه‌ها را کاهش داده و نتایج درمانی را بهبود می‌بخشد.

مزایای کلان‌داده‌ها در پزشکی داده‌محور

کلان‌داده‌ها مزایای گسترده‌ای در پزشکی ارائه می‌دهند که می‌توانند نظام‌های بهداشتی را کارآمدتر سازند. یکی از مهم‌ترین مزایا، امکان تشخیص زودهنگام بیماری‌هاست. با تحلیل الگوهای داده‌های بالینی، زیست‌محیطی و ژنتیکی، پزشکان می‌توانند عوامل خطر را شناسایی کرده و مداخلات پیشگیرانه‌ای اعمال کنند که نرخ مرگ‌ومیر را کاهش دهد. برای نمونه، در بیماری‌های مزمن مانند دیابت یا سرطان، داده‌های عظیم کمک می‌کنند تا روند پیشرفت بیماری پیش‌بینی شود و درمان‌های به‌موقع آغاز گردد.

علاوه بر این، پزشکی شخصی‌سازی‌شده یکی از برجسته‌ترین مزایای پزشکی داده محور است. در این رویکرد، درمان‌ها بر اساس داده‌های ژنتیکی، سبک زندگی و سابقه پزشکی فرد تنظیم می‌شوند، که اثربخشی را افزایش داده و عوارض جانبی را به حداقل می‌رساند. این روش بیماران را از درمان‌های عمومی نجات می‌دهد و به سمت مراقبت‌های **tailor-made** هدایت می‌کند. کلان‌داده‌ها همچنین هزینه‌های بهداشتی را کاهش می‌دهند. تحلیل داده‌ها، فرآیندهای بیمارستان را بهینه می‌سازد، بطورمثال، پیش‌بینی تقاضای تخت‌های بستری یا مدیریت منابع دارویی، منجر به صرفه‌جویی مالی قابل توجهی می‌شود.

روابط بیمار و پزشک نیز از این فناوری منتفع می‌گردد. داده‌های **real time** از دستگاه‌های پوشیدنی مانند ساعت‌های هوشمند، نظارت مداوم بر سلامت را ممکن می‌سازد و بیماران را در تصمیم‌گیری‌های خود مشارکت می‌دهد. در نهایت، مدیریت سلامت جامعه از طریق شناسایی روندهای اپیدمیولوژیک و سیاست‌گذاری‌های مبتنی بر داده بهبود می‌یابد.

چالش‌های کلان‌داده‌ها در پزشکی داده‌محور

علی‌رغم مزایا، چالش‌های متعددی در استفاده از کلان‌داده‌ها در پزشکی وجود دارد که باید به طور جدی بررسی شوند. یکی از اصلی‌ترین نگرانی‌ها، حفظ حریم خصوصی افراد است. داده‌های بهداشتی شامل اطلاعات حساس مانند سابقه بیماری‌ها یا نتایج آزمایش‌ها هستند و خطر افشای آن‌ها می‌تواند اعتماد مردم را به سیستم‌های بهداشتی سلب کند. برای مثال، اگر داده‌ها بدون مجوز به اشتراک گذاشته شوند، افراد ممکن است با تبعیض‌های اجتماعی یا شغلی روبرو گردند.
چالش دیگر، کیفیت و دقت داده‌هاست. داده‌ها ممکن است ناقص، اشتباه یا از منابع نامعتبر باشند، که منجر به تصمیم‌گیری‌های نادرست در درمان شود. تصور کنید اگر اطلاعات ورودی در سوابق پزشکی غلط باشد، تشخیص پزشک تحت تأثیر قرار گیرد و سلامت بیمار به خطر افتد. علاوه بر این، نابرابری دسترسی به فناوری یک مسئله عمومی است. در بسیاری از جوامع، افراد کم‌درآمد یا ساکن مناطق روستایی به دستگاه‌های هوشمند یا اینترنت پرسرعت دسترسی ندارند، که این امر شکاف دیجیتال را افزایش می‌دهد و مزایای پزشکی داده‌محور را تنها به گروه‌های خاصی محدود می‌سازد.
مسائل اخلاقی نیز برجسته هستند، مانند استفاده تجاری از داده‌ها بدون رضایت افراد یا ایجاد تورش در الگوریتم‌ها که ممکن است گروه‌های اقلیت را نادیده بگیرد. در نهایت، پیچیدگی درک این فناوری‌ها برای عموم مردم می‌تواند مانع پذیرش آن‌ها شود و نیاز به آموزش عمومی را برجسته سازد.

کاربردهای کلان‌داده‌ها در پزشکی داده‌محور

کاربردهای کلان‌داده‌ها در پزشکی متنوع هستند و تحولات چشمگیری ایجاد کرده‌اند. در پزشکی شخصی سازی شده، داده‌های ژنومیک و تصویربرداری برای شناسایی نشانگرهای زیستی و توسعه درمان‌های هدفمند استفاده می‌شوند. برای مثال، در ایالات متحده، پروژه **The Cancer Genome Atlas** یا **(TCGA)** با تحلیل داده‌های ژنتیکی هزاران بیمار، ژن‌های محرک سرطان را شناسایی کرده و به پیشرفت درمان‌های شخصی‌سازی‌شده کمک نموده است.
در نظارت بر بیماری‌ها، حسگرهای پوشیدنی داده‌های **real time** مانند ضربان قلب را تحلیل می‌کنند تا حملات قلبی را پیش‌بینی کنند. کاربرد دیگر در مدیریت بیماری‌های عفونی است، جایی که داده‌های رسانه‌های اجتماعی و سوابق بالینی برای ردیابی شیوع استفاده می‌شود. برای نمونه، در کره جنوبی طی پاندمی **COVID-19**، سیستم‌های بزرگ‌داده برای ردیابی تماس‌ها و نظارت بر قرنطینه به کار گرفته شد و نرخ ابتلا را به طور قابل توجهی کاهش داد.
در تحقیقات دارویی، کلان‌داده‌ها کشف دارو را تسریع می‌کنند و آزمایش‌های بالینی را بهینه می‌سازند. در سنگاپور، پلتفرم **HealthHub** با جمع‌آوری داده‌های شهروندان، خدمات بهداشتی شخصی‌سازی‌شده ارائه می‌دهد و مدیریت بیماری‌های مزمن را بهبود بخشیده است. همچنین، در تایوان، سیستم ملی بهداشت با استفاده از کلان‌داده‌ها برای پیش‌بینی روندهای بیماری، پاسخ‌های سریع به بحران‌های بهداشتی را ممکن ساخته است. پروژه **DEXHELPP** در اتریش از شبیه‌سازی داده‌محور برای سیاست‌گذاری‌های بهداشتی استفاده می‌کند و کارایی سیستم را افزایش داده است. در چین، شرکت **Ping An Good Doctor** با تحلیل داده‌های عظیم، مشاوره‌های مجازی ارائه می‌دهد و دسترسی به مراقبت‌های پزشکی را در مناطق دورافتاده تسهیل کرده است. این مثال‌ها نشان می‌دهند که چگونه کشورهای مختلف از این فناوری برای حل مسائل محلی خود بهره می‌برند.
با توجه به مباحث مطرح‌شده، می‌توان نتیجه گرفت که کلان‌داده‌ها و پزشکی داده‌محور ظرفیتی راهبردی برای ارتقای کیفیت نظام سلامت دارند، به‌ویژه در کشورهایی مانند ایران که با چالش‌هایی نظیر بار بالای بیماری‌های

مزمن، محدودیت منابع و نابرابری دسترسی مواجه‌اند. در این راستا، پیشنهاد می‌شود با تدوین سیاست‌های ملی شفاف در حوزه حکمرانی داده‌های سلامت، سرمایه‌گذاری هدفمند در زیرساخت‌های دیجیتال، و توسعه سامانه‌های یکپارچه پرونده الکترونیک سلامت، زمینه بهره‌برداری ایمن و مؤثر از کلان‌داده‌ها را فراهم شود. همچنین، آموزش نیروی انسانی حوزه سلامت در زمینه تحلیل داده و هوش مصنوعی، همراه با ارتقای سواد سلامت دیجیتال در میان عموم مردم، می‌تواند پذیرش اجتماعی این فناوری‌ها را افزایش دهد. توجه هم‌زمان به ملاحظات اخلاقی، حفظ حریم خصوصی و کاهش شکاف دیجیتال، شرط اساسی موفقیت این رویکرد در ایران است. در صورت تحقق این الزامات، پزشکی داده‌محور می‌تواند به ابزاری مؤثر برای تصمیم‌گیری مبتنی بر شواهد، پیشگیری و بهبود درمان، و در نهایت ارتقای عدالت و کارآمدی نظام سلامت کشور تبدیل شود.

منابع:

1. Al-Quraishi T, Al-Quraishi N, AlNabulsi H, AL-Qarishey H, Ali AH. Big data predictive analytics for personalized medicine: Perspectives and challenges. Applied Data Science and Analysis. 2024 Apr 11;2024:32-8.
2. Yang X, Huang K, Yang D, Zhao W, Zhou X. Biomedical big data technologies, applications, and challenges for precision medicine: a review. Global Challenges. 2024 Jan;8(1):2300163.
3. Rehan H. Advancing cancer treatment with ai-driven personalized medicine and cloud-based data integration. Journal of Machine Learning in Pharmaceutical Research. 2024;4(2):1-40.
4. Chowdhury RH. Big data analytics in the field of multifaceted analyses: A study on “health care management”. World Journal of Advanced Research and Reviews. 2024;22(3):2165-72.
5. Karakolias S. Mapping data-driven strategies in improving health care and patient satisfaction. World Journal of Advanced Engineering Technology and Sciences. 2024.
6. Baird T, Roychoudhuri R. Gs-tcga: gene set-based analysis of the cancer genome atlas. Journal of Computational Biology. 2024 Mar 1;31(3):229-40.
7. Tejerina L, Lee H, Kang D. The Republic of Korea’s Digital Tools for Fighting COVID-19.
8. Goda MB, Pang AS, Ong BD, Lim FN, Tan AK, Goh LH. Prevalence and determinants of HealthHub app utilization among community-dwelling adults in Singapore. PLoS One. 2025 Jul 17;20(7):e0327053.
9. Olaboye JA, Maha CC, Kolawole TO, Abdul S. Big data for epidemic preparedness in southeast Asia: An integrative study. International Medical Science Research Journal. 2024;4(6):667-80.
10. Stanak M. Telecardiology for heart failure patients: Benefit assessment and evaluation concept for telemedicine-supported care programs in Austria. Development. 2025 Aug.
11. Yu Z, Hu X, Li H, Hu N, Li Y. A thematic content analysis of the structure and effects of good doctor abilities in China. BMC Health Services Research. 2024 Jul 16;24(1):819.
12. Wilson S, Tolley C, Mc Ardle R, Lawson L, Beswick E, Hassan N, Slight R, Slight S. Recommendations to advance digital health equity: a systematic review of qualitative studies. NPJ digital medicine. 2024 Jun 29;7(1):173.

دل نوشت

برای خوانندگان پالسی نو

سید محمدحسن الهی

تبِ فراگیر هوش مصنوعی

در هر بخش و واحدی از دانشگاه‌مان، درباره مباحث هوش مصنوعی با شور و امید فراوان سخن گفته می‌شود. هر واحد و هر شخصی فارغ از تحصیلات و رشته تحصیلی و توانایی و دانش خود، خودش را متولی این قدرت نوظهور تصور می‌کند و مدعی مسئولیت آن است . رویایِ نفوذ، کشف آینده دانشگاه و مدیریت آن را در سر می‌پروراند.
با این حال، در میان این همهمه و جاه‌طلبی برای مدیریت و مسئولیت هوش مصنوعی در دانشگاه، همواره حقیقتی خاموش طنین‌انداز است. مسئولیت واقعی هوش مصنوعی، بر دوش پرسنل فناوری اطلاعات است و همیشه باید باشد. چرا که تحصیلات آنرا دارند و زیرساخت‌ها در دستان آنهاست، داده‌ها را محافظت می‌کنند و موانع نادیده را همواره می بینند.
اگر هوش مصنوعی قرار است در خدمت آینده دانشگاه باشد، باید با صداقت و درستی شرایطِ آن بیان شود و درک گردد. هوش مصنوعی در دانشگاه نمی‌تواند در ادعاهای پراکنده یا مالکیت تقسیم‌شده و جزیره‌ای شکل بگیرد و بزرگ شود و ببالد. وزنِ سنگینِ آن نیازمند یک پایه واحد و مستحکم است و آن پایه بر فناوری اطلاعات استوار است که در تقاطع میان سخت‌افزارها، نرم‌افزارها، امنیت، دانش و تحصیلات ایستاده است. مسئولیتِ کارکنان فناوری اطلاعات انتخاب خودشان نیست، بلکه به آنها داده شده است و با عزم راسخ باید پیگیری شود. نادیده گرفتن این واقعیت، تضعیفِ خودِ رؤیا است. دنیای هوش‌مصنوعی مگر می تواند بدون فناوری اطلاعات شکل بگیرد. اصولا بنیانِ هوش مصنوعی بر پایه فناوری اطلاعات شکل گرفته است.
اکنون باید تصمیم گرفت باید فناوری اطلاعات و وظایفِ جدیدِ آن به عنوان **پالسی نو** پذیرفته شود.

طعمه‌گذاری در شبکه‌های سازمانی: خطرات، مکانیسم‌ها و نقش پرسنل و کارکنان فناوری اطلاعات

جواد فرهادی
کارشناس ارشد نرم افزار

چکیده

طعمه‌گذاری همچنان یکی از مخرب‌ترین استراتژی‌های مهندسی اجتماعی است که شبکه‌های سازمانی را هدف قرار می‌دهد. برخلاف حملات پیچیده فنی، طعمه‌گذاری به کنجکاوی انسان، سهل‌انگاری کارکنان و کنترل‌های داخلی ضعیف برای به خطر انداختن سیستم‌ها متکی است. این مقاله طعمه‌گذاری را به عنوان یک تهدید اجتماعی-فنی بررسی می‌کند، عوامل خطر داخلی را در شبکه‌های سازمانی تجزیه و تحلیل می‌کند و مسئولیت‌های پرسنل فناوری اطلاعات را در پیشگیری، تشخیص و پاسخ روشن می‌کند.

مقدمه

امنیت اطلاعات در سازمان‌های مدرن نه تنها توسط تهدیدات سایبری خارجی، بلکه توسط دستکاری‌های انسانی نیز به طور فزاینده‌ای به چالش کشیده می‌شود. طعمه‌گذاری، نوعی مهندسی اجتماعی است که با ترغیب کارمندان به تعامل با دستگاه‌های آلوده یا لینک‌های دیجیتال، نرم‌افزارهای مخرب یا دسترسی غیرمجاز به شبکه اتفاق می‌افتد (**Majid & Pahl, 2023**). برخلاف فیشینگ که به فریب ارتباطی وابسته است، طعمه‌گذاری از کنجکاوی، طمع یا اعتماد سوءاستفاده می‌کند. از آنجا که کارکنان همچنان سطح حمله اصلی هستند، دانش داخلی و نظارت بر فناوری اطلاعات برای دفاع مؤثر ضروری است.

سازمان‌هایی با آموزش آگاهی محدود، تحرک بالای دستگاه، شیوه‌های استفاده از دستگاه شخصی (**BYOD**) و محیط‌های کاری ترکیبی به ویژه آسیب‌پذیر هستند (**Hadlington & Murphy, 2021**).

درک طعمه‌گذاری در شبکه‌های سازمانی

حملات طعمه‌گذاری از دو مؤلفه اصلی تشکیل شده‌اند: یک شیء طعمه مخرب و یک فرد هدف. به طور سنتی، طعمه‌گذاری شامل دستگاه‌های فیزیکی مانند فلش مموری‌های **USB** حاوی بدافزار بود که عمداً در مناطق کارمندان قرار داده می‌شدند (**Bhadauria & Soni, 2022**). تکنیک‌های اخیر اکنون شامل موارد زیر است:

۱. رسانه‌های قابل حمل آلوده (**USB**، کارت‌های **SD**، درایوهای قابل حمل).
۲. لینک‌های دانلود جعلی ابری که نوید محتوای رایگان می‌دهند.
۳. تله‌های کد **QR** که در فضاهای سازمانی قرار می‌گیرند.
۴. پیشنهادات هدیه مخرب که به عنوان پاداش یا نظرسنجی شرکتی پنهان شده‌اند.

۵. تبلیغات رسانه‌های اجتماعی مخرب که کاربران را به سایت‌های بدافزار هدایت می‌کنند.

موفقیت طعمه‌گذاری به تصمیم داوطلبانه کارمند برای تعامل با طعمه بستگی دارد. طبق تحقیقات؛ روانشناسی، کنجکاوی، هیجان‌خواهی و راحتی به طور قابل توجهی آسیب‌پذیری را افزایش می‌دهد (**Williams et al., 2020**).

پیامدهای طعمه‌گذاری موفق در سطح شبکه

پس از دسترسی به طعمه، سازمان‌ها ممکن است با تأثیرات فناوری متعددی روبرو شوند:

۱. انتقال بدافزار: بدافزار جاسازی‌شده و در دستگاه‌های ذخیره‌سازی به‌طور خودکار نصب می‌شود و ممکن است امکان کنترل از راه دور یا استخراج داده‌ها را فراهم کند (**Jagatic, 2019**).
۲. سرقت اعتبارنامه: بدافزار اعتبارنامه‌های حساب‌های کاربری را جمع‌آوری می‌کند و امکان دسترسی غیرمجاز به شبکه را فراهم می‌کند.
۳. انتشار در شبکه: اسکریپت‌های کرم-مانند می‌توانند به‌صورت جانبی در سراسر اشتراک‌های شبکه پخش شوند.
۴. نشت داده‌ها: اسناد حساس و منابع استراتژیک ممکن است به سرورهای خارجی نشت کنند.
۵. اختلال عملیاتی: امثال باج‌افزارها می‌تواند تولید یا ارائه خدمات را متوقف کند.
۶. عدم رعایت قوانین: نقض حریم خصوصی و مقررات ممکن است منجر به جریمه و پیگرد قانونی شود (**Chen & Zhao, 2021**).

سازمان‌ها اغلب سرعت انتقال تهدیدات داخلی در شبکه‌ها را دست کم می‌گیرند. حتی یک ایستگاه کاری آلوده می‌تواند سیستم‌های سازمانی را در عرض چند ساعت به خطر بیندازد.

عوامل انسانی و آسیب‌پذیری‌های داخلی

تحقیقات مداوم رفتار انسان را به عنوان علت اصلی موفقیت حملات طعمه‌گذاری شناسایی می‌کنند. نقاط ضعف رفتاری کلیدی عبارتند از:

- آگاهی امنیتی پایین
- اعتماد بیش از اندازه به دستگاه‌های محافظ
- کنجکاوی در مورد رسانه‌های رها شده
- فشار زمانی و استرس کاری و انواع نارضایتی ها
- این تصور که سیستم‌های داخلی ذاتاً ایمن هستند (**Hadnagy، 2020**)
- انکار بی‌مورد قوانین سیاست‌گذاری در بین کارمندان باتجربه‌ای که فرض می‌کنند حملات فقط شبکه‌های خارجی را هدف قرار می‌دهند، رایج است (**Bhadauria & Soni, 2022**). بنابراین، اجرای سیاست‌ها باید همه پرسنل را به طور یکسان هدف قرار دهد.

نقش پرسنل سازمانی

کارکنان غیر فنی به طور معناداری در دفاع در برابر طعمه‌گذاری نقش دارند. مسئولیت‌های آنها شامل موارد زیر است:

۱. رعایت سیاست‌های فناوری اطلاعات
۲. شرکت در آموزش‌های آگاهی‌بخشی

۳. گزارش فوری دستگاه‌ها یا لینک‌های مشکوک
۴. اجتناب از نصب نرم‌افزارهای غیرمجاز
۵. عدم سوءاستفاده از دستگاه شخصی در محل کار

کارمندان باید درک کنند که مهندسی اجتماعی نشانه بی‌کفایتی شخصی نیست. این روش برای دستکاری حتی افراد آموزش‌دیده طراحی شده است. ایجاد یک حمایت روانشناختی، فرهنگ گزارش‌دهی پویا، تشخیص زودهنگام حوادث را به طرز چشمگیری افزایش می‌دهد.

نقش استراتژیک کارکنان فناوری اطلاعات

تیم‌های فناوری اطلاعات مسئولیت مهمی در کاهش آسیب‌پذیری طعمه‌گذاری دارند. وظایف کلیدی عبارتند از:

- کنترل‌های فنی
- استراتژی‌های قفل کردن پورت **USB:** پلتفرم‌های امنیتی نقاط پایانی می‌توانند رسانه‌های قابل حمل غیرمجاز را غیرفعال کنند (**Majid & Pahl, 2023**).
- تشخیص و پاسخ فعال نقاط پایانی (**EDR**): ابزارهای تشخیص و پاسخ رفتار غیرطبیعی دستگاه‌های انتهایی شبکه را به سرعت تشخیص می‌دهند و اقدام متقابل می کنند.
- تقسیم‌بندی شبکه: تقسیم شبکه‌ها، شعاع انفجار یک نفوذ را محدود می‌کند.
- توسعه سیاست: کارکنان فناوری اطلاعات باید قوانین سختگیرانه‌ای برای دسترسی به دستگاه، الزامات موجودی دستگاه‌های ذخیره‌سازی و مدیریت رسانه‌های رمزگذاری شده وضع کنند.
- آموزش کارکنان: شبیه‌سازی‌های روتین فیشینگ، سمینارهای آموزشی و یادآوری‌های مکرر، میزان موفقیت حمله را به طور قابل توجهی کاهش می‌دهند (**Hadlington & Murphy, 2021**).

واکنش به حادثه

پس از کشف استفاده مشکوک از رسانه‌ها، پرسنل فناوری اطلاعات باید:

۱. نقطه پایانی آلوده را ایزوله کنند،
۲. جرم‌شناسی تهدید را انجام دهند،
۳. یافته‌ها را سریعا گزارش دهند، و
۴. کنترل‌های پیشگیرانه را به‌روزرسانی کنند.
۵. فرهنگ‌سازی سازمانی: کارکنان فناوری اطلاعات مسئولیت مشاوره‌ای دارند: ایجاد محیطی که کارمندان در آن احساس راحتی کنند و درخواست تأیید کنند، انعطاف‌پذیری را افزایش می‌دهد.

چارچوب دفاعی پیشنهادی

یک استراتژی موثر ضد طعمه‌گذاری، فناوری، فرآیند و پرسنل را باهم ترکیب می‌کند:

۱. معماری امنیتی جامع با استفاده از دسترسی با حداقل امتیاز
۲. مدیریت هویت بدون اعتماد
۳. نظارت رفتاری چند لایه

۴. آمادگی جرم‌شناسی دیجیتال
۵. آزمایش نفوذ منظم با هدف قرار دادن بردارهای طعمه‌گذاری

این مدل ترکیبی، انسان‌ها و ماشین‌ها را به عنوان دارایی‌های امنیتی به هم پیوسته در نظر می‌گیرد، نه اجزای جدا از هم.

نتیجه‌گیری

طعمه‌گذاری همچنان یک تهدید جدی برای شبکه‌های سازمانی است زیرا از نقاط ضعف انسانی به جای نقص‌های فنی سوءاستفاده می‌کند. رفتار پرسنل داخلی تأثیرگذارترین عامل در تعیین موفقیت طعمه‌گذاری است. مسئولیت‌های کارکنان فناوری اطلاعات فراتر از پیکربندی فنی است؛ آنها باید آگاهی ایجاد کنند، سیاست‌ها را اجرا کنند، تحقیقات را رهبری کنند، زیرساخت‌های دیجیتال را مدیریت کنند و فرهنگ را شکل دهند. با ترکیب شیوه‌های منظم پرسنلی، معماری امنیت شبکه و رهبری استراتژیک فناوری اطلاعات، سازمان‌ها می‌توانند خطر طعمه‌گذاری را به طور قابل توجهی کاهش داده و تاب‌آوری دیجیتال بلندمدت را تقویت کنند.

منابع:

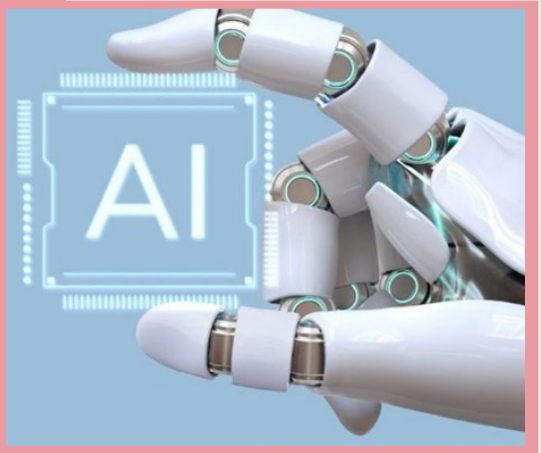
1. Bhadauria, S., & Soni, M. (2022). Analysis of social engineering attack strategies in modern workplaces. Journal of Information Security, 15(2), 45-59.
2. Chen, L., & Zhao, Y. (2021). Data protection and legal responsibility in cyber incident management. Information Law Review, 33(1), 55-68.
3. Hadlington, L., & Murphy, K. (2021). Human-centric risk analysis in cybersecurity incidents. Computers & Security, 104, 102-117.
4. Hadnagy, C. (2020). Social Engineering: The Science of Human Hacking. New York: Wiley Publishing.
5. Jagatic, T. (2019). USB-based intrusion methods and forensic challenges. Digital Investigation Journal, 27, 206-215.
6. Majid, R., & Pahl, C. (2023). Enterprise cybersecurity design frameworks for insider threat mitigation. IEEE Security & Privacy, 21(3), 19-29.
7. Williams, S., Holt, T., & Bossler, A. (2020). Psychological motivators of cyber victimization. ACM Transactions on Privacy and Security, 23(4), 1-23.

چالش‌های هوش مصنوعی

وحید عباس‌زاده
دانشجوی PHD الکترونیک
کارشناس شبکه

مقدمه

هوش مصنوعی به یکی از تحولات تأثیرگذار قرن بیست‌ویکم تبدیل شده و در بسیاری از جنبه‌های زندگی، از جستجوی اطلاعات روزمره تا کاربردهای پیچیده در حوزه‌هایی نظیر پزشکی، حقوق و مهندسی، نقشی جدی و پویا ایفا می‌کند. این فناوری با قابلیت پردازش حجم گسترده‌ای از داده‌ها و ارائه پاسخ‌های سریع، تأثیر زیادی بر ساده‌تر شدن زندگی انسان‌ها داشته است. اما پرسش اساسی این است که آیا می‌توان به طور کامل به دقت و صحت این پاسخ‌ها اعتماد کرد؟ برای مثال، زمانی که از یک مدل هوش مصنوعی درباره تاریخچه یک رویداد ساختگی سوال می‌شود، به جای بیان عدم آگاهی از موضوع، اطلاعاتی مطمئن ارائه می‌شود که به خوبی می‌دانیم حقیقت ندارند. در موارد دیگری نیز پاسخ‌هایی دریافت می‌شود که نه تنها غیر دقیق بلکه تا حدی گمراه‌کننده می‌باشد.



این موارد نشان‌دهنده محدودیت‌هایی در عملکرد هوش مصنوعی هستند که می‌توانند کاربران را به اشتباه بیندازند. اما چرا هوش مصنوعی چنین پاسخ‌هایی تولید می‌کند و از اعتراف به ندانستن خودداری می‌کند؟ این رفتار ناشی از نحوه طراحی و عملکرد آن است.
سیستم‌های هوش مصنوعی با وجود پیشرفت‌های چشمگیر، مبتنی بر شناسایی الگوهای آماری هستند و فاقد درک واقعی یا آگاهی نسبت به محدودیت‌های خود می‌باشند. بنابراین، به جای تشخیص حدود توانایی‌هایشان، تلاش می‌کنند پاسخی تولید کنند که به نظر قانع‌کننده برسد، حتی اگر اشتباه باشد.

چگونگی عملکرد هوش مصنوعی و محدودیت‌های آن

هوش مصنوعی، به‌ویژه مدل‌های پیشرفته زبانی، بر اساس تحلیل الگوهای آماری در حجم وسیعی از داده‌های متنی کار می‌کند. این سیستم‌ها که با داده‌هایی مانند کتاب‌ها، مقالات و وب‌سایت‌ها آموزش دیده‌اند، پاسخ‌هایی ارائه می‌دهند که در نگاه اول منطقی به نظر می‌رسند، اما لزوماً همیشه دقیق نیستند. برخلاف انسان، هوش مصنوعی فاقد درک واقعی از جهان است و صرفاً با استفاده از پیش‌بینی آماری کلمات را کنار هم قرار می‌دهد. این موضوع می‌تواند به تولید اطلاعاتی منجر شود که ظاهراً معتبر هستند ولی در واقع نادرست یا ساختگی‌اند. یکی از محدودیت‌های اساسی، ناتوانی هوش مصنوعی در تشخیص حدود دانش خود است. طبق تحقیقات منتشرشده در **Nature**، مدل‌های پیشرفته زبانی اغلب به جای اذعان به ناآگاهی خود، پاسخ‌های اشتباه ولی روان و مطمئن ارائه می‌دهند، چرا که هدف طراحی آن‌ها ایجاد خروجی‌های خوش‌ساخت و جذاب است. چالش دیگری که باید

در نظر گرفت، اعتماد بیش‌ازحد این سیستم‌ها به خود است.

هوش مصنوعی توانایی ارائه پاسخ‌های دقیق به سوالات شما را دارد !

با ظهور هر فناوری جدید، معمولاً ابتدا با مقاومت و نگرانی عمومی مواجه می‌شویم. اما پس از گذشت زمان، ورق برمی‌گردد و میزان استفاده از آن فناوری به صورت چشمگیری افزایش پیدا می‌کند. این روند تا جایی ادامه می‌یابد که مردم به ایرادات و محدودیت‌های آن پی برده و تلاش می‌کنند در استفاده از آن تعادل برقرار کنند؛ نه زیاده‌روی و نه کمبود. هوش مصنوعی نیز از این قاعده مستثنی نیست. در حال حاضر، شاهد هستیم که بسیاری بدون توجه جدی به چالش‌ها و مسائل مرتبط با این فناوری، به‌صورت روزمره به آن مراجعه کرده و نتایج ارائه شده‌اش را مبنا قرار می‌دهند.

دلایل پاسخ گمراه کننده هوش مصنوعی

دلایل احتمالی برای ارائه پاسخ‌های گمراه‌کننده توسط هوش مصنوعی می‌تواند شامل موارد زیر باشد:
محدودیت در داده‌ها: مدل‌های هوش مصنوعی بر اساس داده‌های آموزشی خود عمل می‌کنند. اگر داده‌ها ناقص، نادرست یا شامل اطلاعات گمراه‌کننده باشند، احتمال تولید پاسخ‌هایی نادرست افزایش می‌یابد.
عدم درک واقعی: هوش مصنوعی توانایی درک عمیق یا مفاهیم انسانی را ندارد و پاسخ‌ها بر اساس الگوها و احتمالات ارائه می‌شود، نه درک واقعی از موضوع.
پیچیدگی سوال: اگر سوال مبهم یا بسیار پیچیده باشد، مدل ممکن است نتواند پاسخ دقیقی ارائه دهد و اطلاعاتی نامرتبط یا گمراه‌کننده تولید کند.
محدودیت‌های فعلی فناوری: هوش مصنوعی هنوز به سطحی از هوشمندی نرسیده که بتواند همیشه نتایج بی‌نقص ارائه دهد. مسائل مختلفی مانند عدم تفکیک اطلاعات قدیمی از جدید یا تفسیر اشتباه معنا می‌تواند باعث این موضوع شود.
سوء برداشت از ورودی: اگر اطلاعات ورودی به درستی ساختاربندی نشده باشد یا شامل ابهام باشد، خروجی نهایی نیز ممکن است به همان اندازه گمراه‌کننده باشد. برای کاهش این احتمال، مهم است که ورودی دقیق و شفاف باشد و از مدل‌های پیشرفته‌تر با داده‌های به‌روز استفاده شود.
فقدان خودآگاهی: این مدل‌ها از توانایی ارزیابی محدودیت‌های دانش خود بی‌بهره‌اند و به همین خاطر، به جای توقف هنگام مواجهه با فقدان اطلاعات دقیق، پاسخ‌هایی ارائه می‌دهند که گاهی فاقد معنا یا دقت کافی است.
الزام به تولید پاسخ: بسیاری از این سیستم‌ها به نحوی طراحی شده‌اند که حتی در شرایط کمبود اطلاعات، باز هم پاسخ‌هایی تولید کنند، و همین امر می‌تواند منجر به پاسخ‌های نادرست شود.

ترکیب مطالب درست و غلط

هم‌آمیختگی مطالب درست و غلط، معمولاً به‌طور آگاهانه یا ناآگاهانه، می‌تواند منجر به ایجاد سردرگمی و برداشت‌های نادرست شود. این ترکیب گاه در رسانه‌ها، فضای مجازی و حتی در مکالمات روزمره دیده می‌شود. افراد ممکن است برای جلب توجه یا تأثیرگذاری بیشتر، بخش‌هایی از حقیقت را با اطلاعات نادرست درهم آمیزند؛ به طوری که تشخیص صحیح از غلط دشوار شود. این مسأله تأکیدی بر ضرورت دقت در بررسی منابع، افزایش سواد رسانه‌ای و اعتماد به اطلاعات معتبر دارد.
هوش مصنوعی نیز گاهی بدون قصد و نیت، از این الگو تبعیت می‌کند. این مسئله به دلیل وجود خطاها یا اشکالات فنی در سیستم ایجاد می‌شود. با توجه به تنوع منابعی که هوش مصنوعی از آنها استفاده می‌کند، امکان دارد داده‌های نادرستی در میان این منابع وجود داشته باشد. در چنین مواردی، نتیجه نهایی ترکیبی از حقایق و اشتباهات خواهد بود که می‌تواند کاربران را به تصمیم‌گیری‌های غلط سوق دهد. متأسفانه، هوش مصنوعی توانایی تفکیک منابع معتبر از نامعتبر یا تصحیح اطلاعات نادرست را ندارد.

راهکار ها

راهکارهای به‌کارگیری مسئولانه هوش مصنوعی برای بهره‌برداری بهینه از هوش مصنوعی و کاهش خطر گمراهی، می‌توان از روش‌های زیر استفاده کرد:

- تأیید صحت اطلاعات از منابع معتبر: همواره پاسخ‌های ارائه‌شده توسط هوش مصنوعی را با اطلاعات موجود در کتاب‌ها، مقالات علمی یا وب‌سایت‌های معتبر بررسی کنید. استفاده از منابع متنوع کمک می‌کند تا از دقت اطلاعات اطمینان حاصل شود.
- تقویت تفکر انتقادی: با نگاهی تحلیلگرانه به پاسخ‌ها توجه کنید و بدون ارزیابی منطقی آنها را نپذیرید. پرسش‌هایی مانند (آیا این جواب قابل قبول است؟) یا (منبع این داده‌ها چیست؟) می‌تواند مانع از بروز اشتباهات ناشی از اعتماد کورکورانه شود.
- انتخاب ابزارهای شفاف: از سامانه‌هایی بهره ببرید که فرآیند تصمیم‌گیری خود را شفاف‌سازی می‌کنند، مثل مدل‌هایی که مستندات و توضیحات فنی دارند.
- پرهیز از اتکا برای تصمیم‌گیری‌های حساس: در مسائل حیاتی مانند موضوعات پزشکی یا حقوقی، از متخصصان انسانی کمک بگیرید و هوش مصنوعی را فقط به‌عنوان ابزار مشورتی به کار گیرید.
- افزایش آگاهی درباره هوش مصنوعی: مطالعه و یادگیری درباره عملکرد و محدودیت‌های این فناوری، شما را در ارزیابی پاسخ‌ها و جلوگیری از سوءبرداشت توانمندتر می‌کند.
- گزارش‌دهی خطاها: در صورت دریافت پاسخ‌های نادرست، آنها را به توسعه‌دهندگان اطلاع دهید تا در جهت بهبود سیستم اقدام شود.

نتیجه گیری

هوش مصنوعی یک ابزار تحول‌آفرین به شمار می‌آید، اما به دلیل وابستگی به داده‌های آماری، عدم توانایی در شناسایی محدودیت‌ها و ایجاد اطمینان کاذب، ممکن است گاهی پاسخ‌هایی نادرست و گمراه‌کننده ارائه کند. با فهم بهتر از نحوه عملکرد این فناوری، توجه به مسائلی همچون شفافیت و انصاف، و همچنین به‌کارگیری نگرشی انتقادی، می‌توان درجه اعتماد به آن را ارتقا داد. آینده هوش مصنوعی وابسته به بهبود طراحی سیستم‌ها و افزایش مسئولیت‌پذیری کاربران است تا این فناوری بتواند به ابزاری قابل اطمینان و ایمن تبدیل شود.

منابع:

1. Ars Technica. (2024). Google’s AI Overview Can Give False, Misleading, and Dangerous Answers.
2. Nature. (2023). Challenges in Evaluating Large Language Models.

زیرساخت محاسباتی و ارتباطی برای تشخیص بیماری‌ها

جواد ملکی
کارشناس ارشد مهندسی شبکه‌های کامپیوتری
مسئول IT شبکه بهداشت و درمان جلفا

مقدمه

تشخیص هوشمند بیماری‌ها با استفاده از فناوری‌های مدرن همچون اینترنت اشیا (**IoT**)، رایانش لبه (**Edge**) و مه (**Fog**)، و هوش مصنوعی (**AI**)، یکی از مهم‌ترین محورهای تحول در پزشکی دیجیتال است. این فناوری‌ها امکان جمع‌آوری، انتقال، پردازش و تحلیل داده‌های بهداشتی را در زمان واقعی فراهم می‌کنند و به پزشکان کمک می‌کنند تا تشخیص دقیق‌تر و سریع‌تری ارائه دهند. برای رسیدن به این هدف، زیرساخت شبکه‌ای قوی، امن و انعطاف‌پذیر ضروری است تا حجم عظیمی از داده‌های پزشکی را به‌طور پایدار و قابل اعتماد منتقل و پردازش کند.

اجزای اصلی زیرساخت شبکه هوشمند تشخیص بیماری

زیرساخت شبکه برای تشخیص هوشمند بیماری‌ها شامل چند لایه حیاتی است که هر یک نقش منحصربه‌فردی در عملکرد کلی سیستم ایفا می‌کنند:

۱. لایه حسگرها و دستگاه‌های **IoT:** در این لایه، دستگاه‌های حسگر و ابزارهای پوشیدنی داده‌های حیاتی را از بیماران جمع‌آوری می‌کنند، مانند ضربان قلب، فشار خون، سطح گلوکز و الگوهای حرکتی. این دستگاه‌ها معمولاً از شبکه‌های بی‌سیم مثل **Wi-Fi** یا پروتکل‌های خاص **IoT** برای انتقال داده استفاده می‌کنند.

۲. شبکه ارتباطی: زیرساخت شبکه باید قابلیت پشتیبانی از انتقال امن و سریع داده‌ها را از حسگرها به نقاط پردازش داشته باشد. به‌علت حساسیت داده‌های پزشکی و نیاز به سرعت بالا برای تحلیل‌های تشخیصی، شبکه‌های با تاخیر کم و پهنای باند بالا اهمیت زیادی دارند. تکنولوژی‌های نوین مانند **G5** و **Multi-Ac-cess Edge Computing** نیز در این بخش بهبود عملکرد را امکان‌پذیر می‌کنند.

۳. رایانش لبه (**Edge**) و مه (**Fog Computing**): برای کاهش تأخیر و حجم انتقال داده به سرورهای ابری، بسیاری از پردازش‌ها در نزدیکی منبع داده انجام می‌شود. رایانش لبه و مه کمک می‌کند تا تحلیل‌های اولیه و فیلتر داده‌ها سریع‌تر انجام شوند و تنها اطلاعات مهم به مرکز داده منتقل شود. این روش باعث کاهش ترافیک شبکه، افزایش سرعت پاسخ‌دهی و بهبود کیفیت تشخیص می‌شود.

۴. مرکز داده‌های متمرکز یا ابری: در این لایه، داده‌های جمع‌آوری‌شده ذخیره، مدیریت و برای تحلیل‌های عمیق‌تر توسط مدل‌های هوش مصنوعی منتقل می‌شوند. رایانش ابری می‌تواند ذخیره‌سازی امن، مقیاس‌پذیر و دسترسی به منابع محاسباتی قوی را فراهم آورد که برای تحلیل‌های پیچیده ضروری است.

نقش شبکه در بهبود تشخیص بیماری‌ها

۱. تحلیل داده در زمان واقعی: با اتصال دستگاه‌های **IoT** به شبکه و انتقال سریع داده‌ها به لایه‌های پردازش، امکان تحلیل داده‌های حیاتی بیماران در زمان واقعی فراهم می‌شود. این زیرساخت شبکه‌ای باعث می‌شود که تحلیل‌های مبتنی بر هوش مصنوعی، پاسخ‌های تشخیصی سریع و دقیق ارائه دهند، به‌ویژه در مواردی که زمان

واکنش بالینی حیاتی است مانند تشخیص حمله قلبی یا ناهنجاری‌های تنفسی.

۲. کاهش تأخیر (**Latency**): برای کاربردهای پزشکی حساس به زمان، تأخیر در انتقال و پردازش داده‌ها می‌تواند خطرناک باشد. استفاده از لایه‌های **Edge** و **Fog** در شبکه باعث کاهش چشمگیر تاخیر می‌شود، زیرا پردازش داده‌ها نزدیک به منبع انجام می‌شود و نیاز به ارسال کامل به سرورهای ابری را کاهش می‌دهد.

۳. پشتیبانی از مدل‌های هوش مصنوعی پیچیده: زیرساخت شبکه باید قادر باشد حجم زیادی از داده‌ها را به ماشین‌های پردازش قوی هدایت کند تا مدل‌های یادگیری عمیق و شبکه‌های عصبی بتوانند الگوهای پنهان در داده‌های پزشکی را تشخیص دهند. به‌عنوان مثال، شبکه‌های عمیق می‌توانند تصاویر پزشکی را تحلیل و تشخیص تومور یا آسیب‌دیدگی‌ها را سریع‌تر و با دقت بالا انجام دهند.

چالش‌های شبکه‌ای در تشخیص هوشمند بیماری‌ها

۱. امنیت و حریم خصوصی داده‌ها: یکی از مهم‌ترین چالش‌ها در زیرساخت شبکه پزشکی، حفاظت از داده‌های حساس بیماران است. داده‌های پزشکی باید در طول انتقال و ذخیره‌سازی رمزگذاری شوند و پروتکل‌های امنیتی قوی برای جلوگیری از دسترسی غیرمجاز و نقض حریم خصوصی تدوین شود.

۲. مقیاس‌پذیری و مدیریت حجم داده: هر روز میلیون‌ها داده پزشکی تولید می‌شود، از حسگرهای **IoT** گرفته تا تصاویر پزشکی. شبکه باید توانایی مقیاس‌پذیری داشته باشد تا بتواند این حجم عظیم را مدیریت کند بدون اینکه عملکرد تحلیل‌های **AI** تحت تأثیر قرار گیرد.

۳. ارتباطات نامطمئن و تاخیر شبکه: در برخی مناطق، شبکه‌های ارتباطی ممکن است پایدار نباشند یا پهنای باند محدود باشد. این موضوع می‌تواند مانع انتقال سریع داده‌ها و تحلیل‌های زمان واقعی شود. بهبود شبکه از طریق فناوری‌های نوین **MEC**، **G5** و شبکه‌های پهن‌باند برای تضمین کیفیت خدمات (**QoS**) ضروری است.

۴. یکپارچگی با سیستم‌های قدیمی (**Legacy Systems**): بسیاری از مراکز درمانی هنوز از سیستم‌های قدیمی و جداگانه برای ذخیره و مدیریت داده‌های بیماران استفاده می‌کنند. این مسئله موجب می‌شود که یکپارچگی داده‌ها با سیستم‌های جدید مبتنی بر **AI** و شبکه‌های پیشرفته به‌صورت پیچیده انجام شود.

راهکارهای ارتقاء زیرساخت شبکه

۴.۱. طراحی شبکه مبتنی بر لایه‌های **Edge/Fog/Cloud**: شبکه‌ای که به‌طور هوشمند بین لایه‌های **Edge**، **Fog** و **Cloud** تقسیم شده باشد می‌تواند پاسخ‌های سریع‌تر و قابل اعتمادتر ارائه دهد. با پردازش داده‌های حساس در لبه شبکه و انتقال داده‌های کم‌اهمیت به مرکز داده‌های ابری، می‌توان کارایی سیستم را بهینه کرد.

۴.۲. استفاده از استانداردهای ارتباطی پیشرفته: استانداردهای ارتباطی مانند **NB-IoT**، **Wi-Fi6**، **5G** و **MEC** می‌توانند پهنای باند مناسب و تأخیر کم را برای شبکه پزشکی فراهم کنند، که مخصوصاً در کاربردهای تشخیص هوشمند و تحلیل داده‌های بزرگ ضروری هستند.

۴.۳. تقویت امنیت داده و رمزگذاری **End-to-End**: برای حفاظت از داده‌های بیماران، باید از رمزگذاری انتها تا انتها، مدیریت کلیدهای امن و پروتکل‌های احراز هویت چندعاملی استفاده شود تا از دسترسی غیرمجاز جلوگیری شود و اعتماد بیماران افزایش یابد.

نتیجه‌گیری

زیرساخت شبکه برای تشخیص هوشمند بیماری‌ها یکی از مهم‌ترین بخش‌های تحول در مراقبت‌های بهداشتی است. شبکه‌ای که بتواند داده‌ها را با امنیت، سرعت و دقت بالا منتقل و پردازش کند، امکان تحلیل‌های هوش مصنوعی پیشرفته را فراهم می‌کند و می‌تواند به بهبود کیفیت تشخیص بیماری‌ها، کاهش هزینه‌های درمانی و ارتقای خدمات مراقبت سلامت منجر شود. برای رسیدن به این هدف، طراحی شبکه‌های لایه‌ای، استفاده از

فناوری‌های نوین ارتباطی، و تقویت امنیت داده‌ها ضروری است.

منابع:

1. Smart healthcare systems: A new IoT-Fog based disease diagnosis framework for smart healthcare projects. Ain Shams Engineering Journal, 2024, doi:10.1016/j.asej.2024.102941.
2. AI augmented edge and fog computing for Internet of Health Things, PMC article on fog and edge computing architectures for healthcare AI.
3. A Comprehensive Review on Smart Health Care: Applications and Technologies, PMC, 2022.
4. AI Driven Resource Allocation in Edge-Fog Computing, The Scientific and Technical Research Council, 2025.
5. Edge-Computing Framework for Smart Healthcare in Smart Cities, Sustainability Journal, 2023.
6. Smart Health Infrastructure: Integrating IoT with Edge Computing, SEEJPH 2024.
7. Smart IoT with the hybrid evolutionary method and image processing for brain tumor detection, Nature 2025.
8. Multi-Access Edge Computing (MEC), ETSI network standard concept

ویکی واژه

در عصری که دنیای دیجیتال روز به روز پیچیده‌تر می‌شوند، درک زبان فنی دیگر تنها در حوزه متخصصان نیست. بخش ویکی‌واژه در «پالسی نو» با هدف پر کردن شکاف بین اصطلاحات فنی و درک روزمره ارائه شده است. در هر شماره، ویکی‌واژه مجموعه‌ای منتخب از مفاهیم را معرفی می‌کند که با دقت به دلیل ارتباط، عمق و تأثیرشان انتخاب شده‌اند. این بخش از طریق توضیحات روشن و زمینه عملی، خوانندگان را با واژگانی که کمتر شناخته شده اند اما اساسی و پایه ای هستند آشنا می کند تا با آگاهی و اعتماد به نفس بیشتری در دنیای دیجیتال فعالیت کنند.

نویده خدائی
دانشجوی دکتری مدیریت فناوری اطلاعات

بلاک‌چین (Blockchain)

بلاک‌چین یک فناوری دفترکل توزیع‌شده است که داده‌ها را در قالب بلوک‌هایی به‌هم‌پیوسته و رمزنگاری‌شده ذخیره می‌کند. این ساختار باعث می‌شود داده‌ها پس از ثبت، عملاً غیرقابل تغییر باشند و شفافیت و اعتماد در تبادل اطلاعات افزایش یابد. بلاک‌چین بدون نیاز به نهاد مرکزی عمل می‌کند و همین ویژگی آن را به زیرساختی مهم برای اقتصاد دیجیتال تبدیل کرده است. علاوه بر ارزهای دیجیتال، این فناوری در مدیریت زنجیره تأمین، ثبت سوابق پزشکی، رأی‌گیری الکترونیکی و مدیریت هویت دیجیتال کاربرد دارد. بلاک‌چین نقش مهمی در ایجاد اعتماد دیجیتال و کاهش تقلب ایفا می‌کند. با این حال، چالش‌هایی مانند مقیاس‌پذیری، مصرف انرژی و مقررات‌گذاری همچنان مطرح هستند و پژوهش‌های اخیر به دنبال ارائه مدل‌های پایدار و کم‌مصرف‌تر برای این فناوری هستند.

شبکه خصوصی مجازی (Virtual Private Network)

ابزاری برای ایجاد ارتباط امن در بستر شبکه‌های عمومی است. این فناوری با رمزنگاری داده‌ها، از دسترسی غیرمجاز جلوگیری می‌کند و حریم خصوصی کاربران را حفظ می‌نماید. VPN برای دسترسی ایمن کارکنان به شبکه‌های سازمانی، انجام تراکنش‌های حساس و حفاظت از اطلاعات شخصی کاربرد فراوان دارد. این فناوری به ویژه در دورکاری و محیط‌های با تهدیدات سایبری بالا اهمیت پیدا می‌کند.

الگوریتم ژنتیک (Genetic Algorithm)

یکی از روش‌های بهینه‌سازی مبتنی بر الهام از تکامل زیستی است. این الگوریتم با تولید جمعیتی از راه‌حل‌ها، اعمال فرآیند انتخاب، ترکیب و جهش، به تدریج بهترین پاسخ‌ها را شناسایی می‌کند. الگوریتم ژنتیک برای مسائل پیچیده و غیرخطی که روش‌های کلاسیک در آن‌ها کارآمد نیستند بسیار مفید است. این روش در هوش مصنوعی، مهندسی، زمان‌بندی، تصمیم‌گیری و طراحی سیستم‌های پیچیده کاربرد دارد. انعطاف‌پذیری، توان جست‌وجوی گسترده و قابلیت انطباق با شرایط مختلف از مزایای اصلی آن است.

هوش مصنوعی مولد
(Generative Artificial Intelligence)

شاخه‌ای از هوش مصنوعی است که توانایی تولید داده و محتوای جدید بر اساس الگوهای آموخته‌شده از داده‌های پیشین را دارد. این فناوری می‌تواند متن، تصویر، ویدئو، صدا و حتی کد نرم‌افزاری تولید کند. مدل‌های زبانی بزرگ و شبکه‌های مولد از مهم‌ترین نمونه‌های این حوزه هستند. هوش مصنوعی مولد تحول قابل‌توجهی در آموزش، پژوهش، تولید محتوای علمی، طراحی و نوآوری ایجاد کرده است. با این حال، چالش‌هایی مانند دقت علمی، سوگیری داده‌ها، تولید محتوای جعلی و مسائل مالکیت فکری، استفاده از آن را نیازمند سیاست‌گذاری و نظارت دقیق کرده است. آینده این فناوری به استفاده مسئولانه و آگاهانه آن وابسته است.

هوش مصنوعی عامل محور
(Agentic Artificial Intelligence)

به نسل جدیدی از سامانه‌های هوشمند اشاره دارد که قادرند به‌صورت فعالانه هدف‌گذاری کنند، برنامه‌ریزی انجام دهند و مجموعه‌ای از اقدامات را برای رسیدن به یک هدف مشخص اجرا کنند. برخلاف سیستم‌های واکنشی یا صرفاً تحلیلی، این نوع هوش مصنوعی می‌تواند نقش یک «عامل مستقل» را در محیط‌های دیجیتال ایفا کند. عامل‌های هوشمند معمولاً از ترکیب مدل‌های زبانی پیشرفته، موتورهای تصمیم‌گیری، حافظه و ابزارهای اجرایی تشکیل می‌شوند. این فناوری در اتوماسیون فرایندهای سازمانی، مدیریت دانش، آموزش هوشمند و سلامت دیجیتال کاربرد گسترده‌ای دارد.

هوش تصمیم
(Decision Intelligence)

هوش تصمیم یک رویکرد میان‌رشته‌ای است که با هدف بهبود کیفیت تصمیم‌گیری در محیط‌های پیچیده طراحی شده است. این مفهوم داده‌ها، تحلیل‌های پیشرفته، هوش مصنوعی، شبیه‌سازی و قضاوت انسانی را در یک چارچوب یکپارچه ترکیب می‌کند. هوش تصمیم به سازمان‌ها کمک می‌کند پیامدهای احتمالی تصمیم‌ها را پیش‌بینی کرده و ریسک‌ها را بهتر مدیریت کنند. این رویکرد فراتر از تحلیل داده، به فرایند تصمیم‌سازی توجه دارد. کاربرد آن در مدیریت سازمانی، سلامت، سیاست‌گذاری عمومی و مدیریت بحران بسیار گسترده است. هوش تصمیم به‌عنوان یکی از ترندهای کلیدی آینده فناوری اطلاعات شناخته می‌شود.

سیستم‌های ماینر (ASIC Mining Systems)

سیستم‌های ماینر **ASIC** سخت‌افزارهایی هستند که به‌طور اختصاصی برای انجام محاسبات رمزنگاری طراحی شده‌اند. این دستگاه‌ها تنها یک نوع الگوریتم خاص را اجرا می‌کنند و به همین دلیل بهره‌وری بسیار بالایی دارند. استفاده از **ASIC** باعث افزایش سرعت استخراج و کاهش مصرف انرژی نسبت به پردازنده‌های عمومی می‌شود. با این حال، انعطاف‌پذیری این سیستم‌ها بسیار محدود است و تنها در حوزه استخراج کاربرد دارند. تمرکز قدرت پردازشی در ماینرهای **ASIC** از جمله چالش‌های مهم اکوسیستم بلاک‌چین محسوب می‌شود و بحث‌هایی درباره تمرکززدایی واقعی در شبکه‌های رمزارزی ایجاد کرده است.

تحـــول دیجیتـــال در نظـــام ســـلامت ایران؛ از داده‌محـــوری تـــا بیمارمحوری

دکتر آیدین محمودعلیلو
فلوشیپ فوق تخصص طب اورژانس کودکان
مرکز آموزشی درمانی فوق تخصصی زهرا مردانی آذر

تحول دیجیتال در نظام سلامت ایران، دیگر یک انتخاب نیست، بلکه ضرورتی انکارناپذیر در مسیر دستیابی به عدالت، کارآمدی و تاب‌آوری سلامت است. با رشد شتابان فناوری‌های نوین، داده‌محوری به رکن اصلی تصمیم‌سازی در نظام سلامت تبدیل شده و بیمار از جایگاه منفعل، به نقش فعال در مسیر درمان ارتقا یافته است. در این مقاله، به بررسی ابعاد تحول دیجیتال، چالش‌های اجرایی و راهبردهای تحقق بیمارمحوری در بستر داده‌های سلامت پرداخته می‌شود.

مقدمه

نظام سلامت ایران طی دهه‌های اخیر پیشرفت‌های چشمگیری در حوزه‌های زیرساختی، نیروی انسانی و گسترش خدمات به دست آورده است. با این حال، رشد جمعیت، تغییر الگوی بیماری‌ها، بحران‌های بهداشتی نوظهور و نیاز به تصمیم‌سازی سریع و دقیق، موجب شده است که الگوی سنتی مدیریت سلامت پاسخ‌گوی چالش‌های امروز نباشد.
تحول دیجیتال در این میان نه به‌عنوان یک فناوری، بلکه به‌عنوان یک پارادایم مدیریتی جدید مطرح است که محور آن، داده، تحلیل و مشارکت فعال بیمار در فرآیند درمان است.

داده‌محوری در نظام سلامت

در دنیای امروز، تصمیم‌سازی بالینی و سیاست‌گذاری سلامت بدون داده غیرممکن است. داده‌های جمع‌آوری‌شده از بیمارستان‌ها، سامانه‌های ثبت بیماری‌ها و مراکز درمانی، نه‌تنها بازتاب وضعیت سلامت جامعه‌اند، بلکه ابزار اصلی برای پیش‌بینی اپیدمی‌ها، مدیریت منابع و بهینه‌سازی خدمات محسوب می‌شوند.
در ایران، طرح‌هایی مانند پرونده الکترونیک سلامت (**EHR**)، سامانه‌های یکپارچه ثبت دارو و نسخه‌نویسی الکترونیک، نخستین گام‌های عملی در مسیر داده‌محوری بوده‌اند. با وجود این، پراکندگی داده‌ها در میان سامانه‌های متعدد و عدم ارتباط ساختاریافته میان آن‌ها، همچنان مانعی جدی در بهره‌برداری از ظرفیت واقعی داده‌هاست.

زیرساخت و چالش‌ها

تحقق تحول دیجیتال، مستلزم وجود زیرساخت‌های فناورانه، فرهنگی و آموزشی است. زیرساخت فناورانه شامل شبکه ارتباطی امن، مراکز داده با ظرفیت بالا، و سامانه‌های استاندارد تبادل داده است. در سطح فرهنگی، پذیرش تغییر از سوی کارکنان درمان، پزشکان و بیماران نقش حیاتی دارد.
یکی از چالش‌های مهم، امنیت داده‌ها و حفظ حریم خصوصی بیماران است. اعتماد عمومی به نظام سلامت در گرو اطمینان از محرمانگی اطلاعات شخصی است. از سوی دیگر، کمبود سواد دیجیتال در میان کادر درمان، یکی از عوامل کندکننده اجرای طرح‌های دیجیتال سلامت به شمار می‌رود. آموزش پزشکان، پرستاران و مدیران در زمینه تحلیل داده و استفاده از فناوری‌های نوین، می‌تواند شکاف میان سیاست و اجرا را پر کند.

بیمارمحوری در عصر دیجیتال

تحول دیجیتال نه‌تنها در سطح ساختاری بلکه در سطح فرهنگی نیز تغییر ایجاد کرده است. در الگوی سنتی،

بیمار دریافت‌کننده منفعل خدمات بود، اما امروز در نظام‌های نوین سلامت، بیمار به شریک فعال در تصمیم‌گیری تبدیل شده است.
پرتال‌های سلامت شخصی، اپلیکیشن‌های پایش علائم حیاتی و برنامه‌های خودمدیریتی بیماری‌های مزمن، ابزارهایی هستند که به بیماران امکان می‌دهند درک بهتری از وضعیت خود داشته و در مسیر درمان مشارکت مؤثرتری کنند. در کودکان و بیماران خاص نیز، استفاده از سامانه‌های پایش از راه دور و ارتباطات تله‌مدیسین (**Telemedicine**)، سبب کاهش مراجعات غیرضروری و افزایش پیوستگی مراقبت‌ها شده است - موضوعی که به‌ویژه در مناطق محروم ایران اهمیت دوچندان دارد.

نقش سیاست‌گذاران در مدیریت تحول

تحول دیجیتال بدون حمایت سیاستی و بودجه‌ای امکان‌پذیر نیست. وزارت بهداشت ایران طی سال‌های اخیر گام‌های مهمی در تدوین نقشه راه تحول دیجیتال سلامت کشور برداشته است، اما اجرای مؤثر آن نیازمند هماهنگی میان نهادهای بیمه‌گر، دانشگاه‌های علوم پزشکی، بخش خصوصی و شرکت‌های دانش‌بنیان است.
سرمایه‌گذاری در زیرساخت‌های نرم‌افزاری، ایجاد چارچوب‌های اخلاقی برای تبادل داده، و استانداردسازی نظام‌های اطلاعاتی سلامت، سه محور اساسی در مسیر توسعه پایدار دیجیتال سلامت محسوب می‌شوند.

نقش سیاست‌گذاران در مدیریت تحول

تحول دیجیتال بدون حمایت سیاستی و بودجه‌ای امکان‌پذیر نیست. وزارت بهداشت ایران طی سال‌های اخیر گام‌های مهمی در تدوین نقشه راه تحول دیجیتال سلامت کشور برداشته است، اما اجرای مؤثر آن نیازمند هماهنگی میان نهادهای بیمه‌گر، دانشگاه‌های علوم پزشکی، بخش خصوصی و شرکت‌های دانش‌بنیان است.
سرمایه‌گذاری در زیرساخت‌های نرم‌افزاری، ایجاد چارچوب‌های اخلاقی برای تبادل داده، و استانداردسازی نظام‌های اطلاعاتی سلامت، سه محور اساسی در مسیر توسعه پایدار دیجیتال سلامت محسوب می‌شوند.

نتیجه‌گیری

تحول دیجیتال در نظام سلامت ایران، ضرورتی استراتژیک است که تحقق آن نیازمند همگرایی فناوری، سیاست و فرهنگ است. داده‌محوری باید به اصل حاکم در تصمیم‌سازی‌های سلامت تبدیل شود و بیماران به‌عنوان شرکای واقعی در فرآیند مراقبت شناخته شوند.
پیشنهاد می‌شود نظام سلامت ایران با تدوین چارچوب ملی تحول دیجیتال سلامت و سرمایه‌گذاری در آموزش، زیرساخت و امنیت داده‌ها، مسیر خود را به سمت بیمارمحوری و عدالت دیجیتال هدایت کند؛ مسیری که نه‌تنها به نفع بیماران، بلکه به سود کل جامعه خواهد بود.

منابع:

1. World Health Organization (WHO). Global strategy on digital health 2020–2025. Geneva: World Health Organization; 2021.
2. Ministry of Health and Medical Education of Iran. Iran Digital Health Transformation Roadmap. Tehran: MOHME Publications; 2023.
3. Sadoughi F, et al. Digital health in Iran: Challenges and opportunities. Iranian Journal of Public Health. 2020;49(6):1001–1012.
4. Khodaverdi M, et al. The role of eHealth infrastructure in improving healthcare delivery in Iran. Journal of Health Administration. 2022;25(4):45–59.
5. World Bank. The digital transformation of health systems in the Middle East and North Africa. Washington, DC: World Bank Group; 2022.
6. Rahimi F, Bahadori M. Barriers to implementation of digital health initiatives in developing countries: The case of Iran. Health Informatics Journal. 2021;27(2):14604582211010156.

فناوری دیپ‌فیک (DEEPFAKE)؛

بازتعریف واقعیت در عصر هوش مصنوعی و پیامدهای فناورانه، اجتماعی و اخلاقی آن

نویده خدائی
دانشجوی دکتری مدیریت فناوری اطلاعات

فناوری دیپ‌فیک به‌عنوان یکی از جلوه‌های پیشرفته هوش مصنوعی مبتنی بر یادگیری عمیق، توانایی تولید و دست‌کاری محتوای صوتی و تصویری بسیار واقع‌گرایانه را فراهم کرده است. این فناوری، که ابتدا در حوزه‌های پژوهشی و سرگرمی مطرح شد، به‌سرعت به عرصه‌های حساس‌تری همچون رسانه، سیاست، آموزش و سلامت نفوذ کرده است. مقاله حاضر با رویکردی توصیفی-تحلیلی، به معرفی جامع فناوری دیپ‌فیک، مبانی فنی، کاربردهای بالقوه، تهدیدها و چالش‌های اخلاقی و حقوقی آن می‌پردازد و بر ضرورت حکمرانی آگاهانه و مسئولانه این فناوری تأکید می‌کند.

مقدمه

در طول تاریخ، تصویر و صدا همواره از معتبرترین ابزارهای ثبت و انتقال واقعیت به‌شمار می‌رفته‌اند. با این حال، پیشرفت‌های شتابان در حوزه هوش مصنوعی، به‌ویژه یادگیری عمیق، این اعتبار سنتی را با چالشی جدی مواجه ساخته است. فناوری دیپ‌فیک (**Deepfake**) نمونه‌ای شاخص از این تحول است؛ فناوری‌ای که می‌تواند چهره، صدا و حرکات انسان را به‌گونه‌ای بازتولید کند که تشخیص محتوای واقعی از جعلی برای انسان عادی، و حتی متخصصان، دشوار باشد.
اهمیت دیپ‌فیک صرفاً در توان فنی آن خلاصه نمی‌شود، بلکه پیامدهای اجتماعی، اخلاقی و فرهنگی آن، این فناوری را به یکی از موضوعات محوری در بحث آینده حکمرانی دیجیتال تبدیل کرده است.

تعریف و سیر شکل‌گیری دیپ‌فیک

اصطلاح «دیپ‌فیک» ترکیبی از دو واژه **Deep Learning** و **Fake** است و به محتوایی اطلاق می‌شود که با استفاده از مدل‌های یادگیری عمیق تولید یا دست‌کاری شده باشد. نخستین نمونه‌های شناخته‌شده دیپ‌فیک در اواخر دهه ۲۰۱۰ و عمدتاً در فضای شبکه‌های اجتماعی ظهور کردند، اما به‌سرعت توجه پژوهشگران و سیاست‌گذاران را به خود جلب نمودند.
گسترش داده‌های دیجیتال، افزایش توان محاسباتی و متن‌باز شدن بسیاری از الگوریتم‌های هوش مصنوعی، باعث شد تولید دیپ‌فیک از یک فعالیت تخصصی به امری نسبتاً در دسترس تبدیل شود.

مبانی فنی فناوری دیپ‌فیک

در سطح فنی، دیپ‌فیک بر پایه شبکه‌های عصبی عمیق بنا شده است. مهم‌ترین معماری مورد استفاده در این

حوزه، شبکه‌های مولد تخاصمی (**GANs**) هستند. این شبکه‌ها از دو جزء اصلی تشکیل شده‌اند:

- مولد (**Generator**): که تلاش می‌کند داده‌ای مصنوعی اما شبیه به داده واقعی تولید کند.
- تمییزدهنده (**Discriminator**): که وظیفه تشخیص داده واقعی از جعلی را بر عهده دارد.

رقابت مستمر میان این دو شبکه، به بهبود تدریجی کیفیت خروجی منجر می‌شود. علاوه بر **GAN**ها، مدل‌های مبتنی بر **Auto encoder**ها و **Transformer**ها نیز در تولید دیپ‌فیک‌های پیشرفته به‌کار می‌روند.

انواع دیپ‌فیک

دیپ‌فیک‌ها را می‌توان بر اساس نوع محتوا به چند دسته تقسیم کرد:

- دیپ‌فیک تصویری: جایگزینی یا تغییر چهره در تصاویر
- دیپ‌فیک ویدیویی: بازسازی حرکات صورت، لب‌خوانی و حالات احساسی
- دیپ‌فیک صوتی: شبیه‌سازی صدای افراد واقعی
- دیپ‌فیک چندوجهی: ترکیب هم‌زمان تصویر، ویدیو و صدا

هر یک از این انواع، کاربردها و مخاطرات خاص خود را دارند.

کاربردهای بالقوه و مشروع دیپ‌فیک

برخلاف تصور عمومی، دیپ‌فیک صرفاً ابزاری برای جعل و فریب نیست. در صورت استفاده مسئولانه، این فناوری می‌تواند کاربردهای مثبتی داشته باشد، از جمله:

- آموزش و شبیه‌سازی (به‌ویژه در آموزش پزشکی و مهارت‌های ارتباطی)
- صنعت فیلم، بازی و رسانه‌های تعاملی
- دوبله هوشمند و ترجمه چندزبانه
- بازتوانی بیماران دچار اختلالات گفتاری
- آموزش الکترونیکی و تولید محتوای شخصی‌سازی‌شده

نقطه تمایز استفاده مشروع و نامشروع از دیپ‌فیک، شفافیت، رضایت و هدف کاربرد است.

تهدیدها و چالش‌های اجتماعی

در کنار مزایا، دیپ‌فیک تهدیدهای قابل توجهی به همراه دارد:

- انتشار اطلاعات نادرست و اخبار جعلی
- جعل هویت و کلاهبرداری دیجیتال
- نقض حریم خصوصی و آسیب به حیثیت افراد
- تضعیف اعتماد عمومی به رسانه‌ها
- ایجاد سردرگمی در تشخیص حقیقت از جعل

این تهدیدها به‌ویژه در شرایط بحرانی، مانند همه‌گیری‌ها یا بحران‌های سیاسی، می‌توانند آثار مخربی بر تصمیم‌گیری عمومی داشته باشند.

دیپ‌فیک و بحران اعتماد دیجیتال

یکی از پیامدهای کلیدی گسترش دیپ‌فیک، شکل‌گیری نوعی بی‌اعتمادی ساختاری به محتوای دیجیتال است. در چنین شرایطی، حتی شواهد واقعی نیز ممکن است مورد تردید قرار گیرند. این پدیده، چالش‌های عمیقی برای آموزش، سلامت، رسانه و نظام‌های حقوقی ایجاد می‌کند.

ملاحظات اخلاقی و حقوقی

بسیاری از نظام‌های حقوقی هنوز آمادگی لازم برای مواجهه با دیپ‌فیک را ندارند. مسائل کلیدی عبارت‌اند از:

- مالکیت داده و تصویر افراد
- رضایت آگاهانه
- مسئولیت تولیدکنندگان و پلتفرم‌ها
- مرز میان آزادی بیان و جلوگیری از سوءاستفاده

اخلاق فناوری در این حوزه نقشی محوری دارد و باید هم‌زمان با توسعه فنی پیش برود.

راهبردهای مواجهه و حکمرانی

برای مدیریت پیامدهای دیپ‌فیک، رویکردی چندلایه ضروری است:

۱. توسعه ابزارهای تشخیص محتوای جعلی
۲. ارتقای سواد رسانه‌ای و سواد هوش مصنوعی
۳. تدوین قوانین و مقررات شفاف
۴. نقش‌آفرینی دانشگاه‌ها و نشریات علمی
۵. ترویج اخلاق‌محوری در طراحی فناوری

جمع‌بندی

دیپ‌فیک نماد یکی از مهم‌ترین چالش‌های عصر هوش مصنوعی است؛ فناوری‌ای که هم‌زمان ظرفیت خلق ارزش و ایجاد تهدید را در خود دارد. آینده دیپ‌فیک نه به توان الگوریتم‌ها، بلکه به سطح آگاهی، مسئولیت‌پذیری و حکمرانی جوامع انسانی وابسته است. معرفی علمی و انتقادی این فناوری، گامی ضروری در مسیر استفاده آگاهانه و اخلاق‌محور از آن به‌شمار می‌رود.

منابع:

1. Goodfellow, I., et al. (2014). Generative Adversarial Networks. NeurIPS.
2. Westerlund, M. (2019). The emergence of deepfake technology. Technology Innovation Management Review.
3. Chesney, R., & Citron, D. (2019). Deepfakes and the new disinformation war. Foreign Affairs.
4. Kietzmann, J., et al. (2020). Deepfakes: Trick or treat?. Business Horizons.
5. Floridi, L., et al. (2018). AI4People—An ethical framework for a good AI society. Minds and Machines.
6. European Commission. (2023). Artificial Intelligence Act and synthetic media.

آموزش فناوری اطلاعات؛
مبانی هک اخلاقی(بخش ششم)

دکتر طاها صمدسلطانی
دانشیار انفورماتیک پزشکی
مدیرآمـــار، فنـــاوری اطلاعـــات و
امنیـــت فضـــای مجـــازی دانشـــگاه

طبق وعده‌ای که در انتهای آموزش قبلی داده شده بود در این نسخه به فاز **Enumeration** به عنوان یکی از مراحل کلیدی در فرآیند هک اخلاقی خواهیم پرداخت. **Enumeration** فازی است که پس از **Scanning** انجام می‌گیرد و هدف آن جمع‌آوری اطلاعات دقیق‌تر و جزئی‌تر از سیستم‌های هدف است. در هک اخلاقی، این مرحله برای شناسایی کاربران، گروه‌ها، منابع شبکه، سرویس‌های فعال و نقاط ضعف خاص استفاده می‌شود. اجرای این فاز کمک می‌کند تا هکر اخلاقی (یا متخصص تست نفوذ) بتواند نقشه دقیق‌تری از اکوسیستم سازمانی ترسیم کند و آماده مراحل بعدی مانند **Gaining Access** یا **Exploitation** شود. این فاز نیز باید با مجوز قانونی و در چارچوب تست نفوذ انجام شود تا از سوءاستفاده جلوگیری گردد.
Enumeration را می‌توان به دو دسته کلی **Active** و **Passive** تقسیم کرد، اما تمرکز اصلی بر روش‌های **Active** است که شامل تعامل مستقیم با سیستم هدف می‌شود. در این روش‌ها، ابزارهایی مانند **Nmap**، **Enum4linux**، **Metasploit** و **Hydra** برای استخراج اطلاعات استفاده می‌شوند. برخلاف **Scanning** که بیشتر بر شناسایی وجود سیستم‌ها و پورت‌ها تمرکز دارد، **Enumeration** به جزئیات مانند نام کاربران، نسخه سرویس‌ها و ساختار دایرکتوری‌ها می‌پردازد. البته این مرحله می‌تواند ترافیک شبکه ایجاد کند و ممکن است توسط سیستم‌های تشخیص نفوذ (**IDS**) شناسایی شود.

انواع Enumeration

در ادامه، به بررسی انواع رایج **Enumeration** می‌پردازیم که هر کدام بر روی پروتکل یا سرویس خاصی تمرکز دارند:

- نوع اول : NetBIOS Enumeration

NetBIOS یا (**Network Basic Input/Output System**) پروتکلی است که در شبکه‌های ویندوزی برای به اشتراک‌گذاری منابع استفاده می‌شود. در این روش، هکر اخلاقی نام کامپیوترها، کاربران، گروه‌ها و سرویس‌های به اشتراک گذاشته شده را استخراج می‌کند. ابزارهایی مانند **nbtstat** در ویندوز یا **enum4linux** در لینوکس برای این کار مناسب هستند.
مثال :
در **Kali Linux**، با استفاده از **enum4linux** می‌توانید اطلاعات **NetBIOS** را استخراج کنید:

```
enum4linux -a 192.168.1.100
```

این دستور لیستی از کاربران، گروه‌ها و منابع به اشتراک گذاشته شده را نمایش می‌دهد. برای نمونه، خروجی ممکن است شامل نام کاربران مانند "**Administrator**" یا "**Guest**" و گروه‌هایی مانند "**Domain Admins**" باشد. این اطلاعات برای حملات بعدی مانند **Brute Force** مفید است.
تصویر زیر نشان‌دهنده بخشی از خروجی **enum4linux** است که کاربران و گروه‌های سیستم هدف را لیست می‌کند، بدون اینکه نیاز به لاگین باشد.

```
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) at 2026

 ==========================
|    Target Information    |
 ==========================
Target ..... 192.168.1.100
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 =====================================================
|    Enumerating Workgroup/Domain on 192.168.1.100    |
 =====================================================
[+] Got domain/workgroup name: WORKGROUP


 ============================================
|    Nbtstat Information for 192.168.1.100    |
 ============================================
Looking up status of 192.168.1.100
    TESTSERVER      <00> -         B <ACTIVE>  Workstation Service
    TESTDOMAIN      <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
    TESTSERVER      <20> -         B <ACTIVE>  File Server Service
```

- **نوع دوم : SNMP Enumeration**

SNMP یا (**Simple Network Management Protocol**) برای مدیریت دستگاه‌های شبکه مانند روترها و سوئیچ‌ها استفاده می‌شود. در **Enumeration SNMP**، هکر اخلاقی با استفاده از **Community Strings** مانند "public" یا "**private**" به اطلاعات دستگاه دسترسی پیدا می‌کند، مانند لیست اینترفیس‌ها، روتینگ تیبل و حتی کاربران لاگین شده.
(ابزارهای قابل استفاده: **snmpwalk** یا **snmpenum**)

```
snmpwalk -v1 -c public 192.168.1.1
```

این دستور تمام **OID** یا (**Object Identifiers**) دستگاه را استخراج می‌کند و اطلاعاتی مانند نسخه سیستم عامل یا نام دستگاه را نشان می‌دهد. اگر **Community String** پیش‌فرض باشد، این روش بسیار مؤثر است اما ریسک شناسایی دارد.

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux router 5.10.0-1-amd64 #1 SMP Debian 5.10.1-1 (20
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (12345678) 1 day, 10:17:36.78
SNMPv2-MIB::sysContact.0 = STRING: admin@example.com
SNMPv2-MIB::sysName.0 = STRING: TestRouter
SNMPv2-MIB::sysLocation.0 = STRING: Data Center, Room 101
SNMPv2-MIB::sysServices.0 = INTEGER: 72

IF-MIB::ifNumber.0 = INTEGER: 3
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifDescr.1 = STRING: lo
IF-MIB::ifDescr.2 = STRING: eth0
IF-MIB::ifDescr.3 = STRING: eth1
IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifMtu.1 = INTEGER: 65536
IF-MIB::ifMtu.2 = INTEGER: 1500
IF-MIB::ifMtu.3 = INTEGER: 1500
IF-MIB::ifSpeed.1 = Gauge32: 10000000
IF-MIB::ifSpeed.2 = Gauge32: 1000000000
IF-MIB::ifSpeed.3 = Gauge32: 1000000000
IF-MIB::ifPhysAddress.1 = STRING:
IF-MIB::ifPhysAddress.2 = STRING: 00:11:22:33:44:55
IF-MIB::ifPhysAddress.3 = STRING: 00:aa:bb:cc:dd:ee
```

خروجی معمولا شامل بخش های زیر می باشد

SYS: اطلاعات سیستم مانند توصیف، نام، مکان و زمان آپ تایم.

IF: جزئیات اینترفیس‌های شبکه مانند نوع، سرعت، وضعیت و آدرس **MAC**

IP: آمار **IP** مانند **forwarding**، تعداد پکت‌های دریافتی/ارسال‌شده و آدرس‌های **IP**

TCP/UDP: آماری از پروتکل‌های **TCP** و **UDP**

- نوع سوم : **LDAP Enumeration**

LDAP یا (**Lightweight Directory Access Protocol**) برای مدیریت دایرکتوری‌ها در شبکه‌های بزرگ مانند **Active Directory** استفاده می‌شود. در این روش، اطلاعات کاربران، گروه‌ها و ساختار سازمانی استخراج می‌شود. ابزارها شامل **ldapsearch** یا **JXplorer** می باشند که در مثال مشاهده می کنید.

```
ldapsearch -h 192.168.1.50 -x -b "dc=example,dc=com'
```

این دستور لیستی از کاربران و گروه‌ها به همراه اطلاعات تماس مثل ایمیل و نقش‌هایشان نشان می دهد. این روش برای شناسایی نقاط ضعف در **Active Directory** حیاتی است.

```
# Administrator, people, example, com
dn: cn=Administrator,ou=people,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Administrator
givenName: Admin
sn: User
mail: admin@example.com
userPrincipalName: admin@example.com
description: Built-in administrator account

# tahasoltany, people, example, com
dn: cn=tahasoltany,ou=people,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: tahasoltany
givenName: Taha
sn: Soltany
mail: taha@tbzmed.ac.ir
userPrincipalName: tahasoltany@example.com
description: IT Specialist at Tabriz University of Medical Sciences
telephoneNumber: +98-123-456789
```

بحث انواع **Enumeration** ادامه دارد....

پیام مخاطب

دکتر سینا قرطاسی اسکویی
دکترای حرفه‌ای دندان‌پزشکی، فلوشیپ انفورماتیک بالینی
مسئول تحقیق و توسعه بخش دندانپزشکی دیجیتال
معاون سردبیر JAPID و مدیر سابق دفتر نشر دانشگاه

با سلام و احترام

خدمت دست‌اندرکاران محترم نشریه «پالسی نو»

ضمن عرض تبریک بابت راه‌اندازی و انتشار نشریه «پالسی نو» به‌عنوان ماهنامه فناوری اطلاعات دانشگاه علوم پزشکی تبریز، بدین‌وسیله بازخورد و نکاتی با هدف ارتقای هرچه بیشتر کیفیت این نشریه ارزشمند معروض می‌دارد.

در ابتدا، شایسته است از انتخاب هوشمندانه و به‌روز موضوعات در حوزه‌هایی نظیر سلامت دیجیتال، امنیت سایبری، حکمرانی داده، هوش مصنوعی و سایر فناوری‌های نوین اطلاعات در نظام سلامت قدردانی گردد. تنوع موضوعی، عناوین مسئله‌محور، ارتباط مستقیم مطالب با چالش‌ها و نیازهای روز نظام سلامت، همچنین انتشار منظم ماهنامه و دسترسی به شماره‌های منتشرشده از طریق وب‌سایت نشریه، از نقاط قوت قابل توجه «پالسی نو» به شمار می‌روند و جایگاه این نشریه را به‌عنوان یک رسانه تخصصی و آینده‌نگر تقویت می‌کند.

پیشنهادهایی جهت بهبود و توسعه:

- **افزایش انسجام ساختاری مقالات:** پیشنهاد می‌شود مقالات از چارچوب نسبتاً ثابتی شامل مقدمه، بدنه تحلیلی و جمع‌بندی پیروی کنند تا خوانایی، انسجام محتوایی و اثرگذاری مطالب برای طیف متنوعی از مخاطبان افزایش یابد.
- **افزودن خلاصه مدیریتی (Executive Summary)**: درج یک خلاصه کوتاه در ابتدای برخی مقالات، به‌ویژه مطالب تحلیلی و راهبردی، می‌تواند برای مدیران، تصمیم‌گیران و مخاطبانی که محدودیت زمانی دارند، بسیار مفید باشد.
- **توجه بیشتر به مصادیق و تجربیات بومی:** بهره‌گیری از نمونه‌های داخلی، پروژه‌های دانشگاهی یا تجربه‌های اجرایی در کشور، به افزایش کاربردپذیری مطالب و ایجاد پیوند مؤثرتر میان محتوا و واقعیت‌های اجرایی نظام سلامت کمک خواهد کرد.
- **تعریف و درج بیانیه هدف و مخاطبان نشریه:** با وجود آن‌که عنوان نشریه تا حد زیادی حیطه موضوعی آن را مشخص می‌کند، به نظر می‌رسد جای یک بخش کوتاه تحت عنوان «درباره نشریه» یا «بیانیه هدف» در صفحه شناسنامه هر شماره خالی است. درج چنین بیانیه‌ای می‌تواند به تبیین مأموریت نشریه، رویکرد محتوایی و همچنین معرفی صریح‌تر مخاطبان هدف (مانند مدیران سلامت، کارشناسان فناوری اطلاعات، اعضای هیئت علمی، دانشجویان و علاقه‌مندان حوزه سلامت دیجیتال) کمک کند.
- **گسترش شیوه‌های انتشار و حضور رسانه‌ای:** انتشار بخشی از محتوا در قالب‌های متناسب با شبکه‌های اجتماعی (مانند معرفی کوتاه مقالات، نکات کلیدی یا اینفوگرافیک) می‌تواند به افزایش دیده‌شدن نشریه کمک کند.
- همچنین، ارائه مقالات به‌صورت صفحات **HTML** مجزا در وب‌سایت نشریه در کنار نسخه **PDF**، موجب بهبود دسترسی‌پذیری، قابلیت اشتراک‌گذاری و نمایه‌شدن محتوا در موتورهای جست‌وجو خواهد شد.
- **به‌روزرسانی صفحه‌آرایی و طراحی بصری نسخه PDF:** با توجه به ماهیت نوآورانه و به‌روز موضوعات نشریه، به‌روزرسانی صفحه‌آرایی، استفاده از فونت‌های امروزی‌تر و طراحی بصری منسجم‌تر می‌تواند هماهنگی فرم و محتوا را افزایش داده و تجربه مطالعه مخاطب را بهبود بخشد.
- **تقویت ویراستاری زبانی و یکدستی نگارشی:** توجه بیشتر به ویراستاری زبانی، روان‌سازی جملات، یکدست‌سازی اصطلاحات تخصصی و کاهش ناهماهنگی‌های نگارشی در برخی مطالب، می‌تواند کیفیت کلی محتوا و اعتبار حرفه‌ای نشریه را بیش از پیش ارتقا دهد.

در مجموع، نشریه «پالسی نو» را می‌توان اقدامی ارزشمند و آینده‌نگر در راستای توسعه گفتمان فناوری اطلاعات در نظام سلامت دانست و امید است با تداوم انتشار و اعمال بهبودهای تدریجی، بیش از پیش به مرجعی اثرگذار در این حوزه تبدیل شود.

با سپاس از تلاش‌های ارزشمند شما و آرزوی توفیق روزافزون
دکتر سینا قرطاسی اسکوئی

دکتر طاها صمد سلطانی
دانشیار انفورماتیک پزشکی
مدیرآمار، فناوری اطلاعات و امنیت
فضای مجازی دانشگاه

نویده خدائی
دانشجوی دکتری مدیریت فناوری
اطلاعات
کارشناس فناوری اطلاعات

دکترامیر تراب میاندوآب
استادیار مدیریت اطلاعات سلامت
مرکز تحقیقات آموزش پزشکی

دکتر سعید سقطی‌زاد
دکتری حرفه‌ای پزشکی
رئیس دبیرخانه هیأت امنای
دانشگاه

جواد فرهادی
کارشناس ارشد نرم افزار

وحید عباس‌زاده
دانشجوی PHD الکترونیک
کارشناس شبکه

جواد ملکی
کارشناس ارشد مهندسی شبکه
کارشناس فناوری اطلاعات
شبکه بهداشت و درمان جلفا

دکتر آیدین محمدعلیلو
فلوشیپ فوق‌تخصص
طب اورژانس کودکان
مرکز آموزشی درمانی
فوق‌تخصصی زهرا مردانی آذر

سیدمحمدحسن الهی

سوگند حبیبی
کارشناس ارشد فناوری اطلاعات سلامت
کارشناس فناوری اطلاعات سلامت
معاونت درمان

مدیریت آمار، فناوری اطلاعات و امنیت فضای مجازی
دانشگاه علوم پزشکی تبریز

A New Pulse

anp.tbzmed.ac.ir

anp@tbzmed.ac.ir

anew_pulse