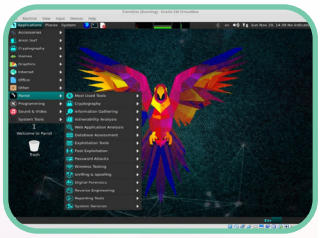
ماهنامه
پالسی نو
A New Pulse
First year - September 2025 No:02
سال اول – شماره دوم – شهریور ۱۴۰۴



... سیستم عامل دیگر که نسبت به Kali سبک تر و ساده تر بوده و قابلیت های مناسبی ارائه می کند Parrot می باشد ...

... دیجیتال توئین به یک نسخه دیجیتال یا شبیه‌سازی مجازی از یک شیء، سیستم، فرآیند یا حتی یک انسان در دنیای واقعی اشاره دارد ...

کلمه متاورس (Metaverse) از دو بخش تشکیل شده است: "متا" (Meta) به معنای فراتر یا ماورا، و "ورس" (Verse) که به معنای جهان یا کیهان است...

ویکی واژه
WIKIWORD

... ویکی‌واژه مجموعه‌ای منتخب از مفاهیم را معرفی می‌کند که با دقت به دلیل ارتباط، عمق و تأثیرشان انتخاب شده‌اند. این بخش از طریق ...

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 صابر درسخوان، مهندس وحید عباس‌زاده، مهندس جواد فرهادی، سیدمحمدحسن الهی، سوگند حبیبی، الهام منقش، مهندس فریبا اسماعیلی، مهندس رقیه سیدنژاد، نرگس نجفی، مهندس سمیه کرد

مدیر اجرایی: دکتر سعید سقطی زاد

طراح و برنامه نویس: سیدمحمدحسن الهی

روابط عمومی: الناز هوشیان

سرمقاله

نویده خدائی
دانشجوی دکتری مدیریت فناوری اطلاعات

دانشگاهی فراتر از آموزش و پژوهش: فناوری اطلاعات راهی به‌سوی دانشگاه نسل پنجم

تحول نقش دانشگاه در جهان امروز، ضرورتی انکارناپذیر است. در مواجهه با چالش‌های پیچیده اجتماعی، اقتصادی و فناورانه، دیگر نمی‌توان دانشگاه را صرفاً نهادی آموزشی یا پژوهشی تلقی کرد. روندهای جهانی نشان می‌دهند که دانشگاه‌ها باید از قالب‌های سنتی فراتر روند و در مسیر ارزش‌آفرینی، نوآوری و اثرگذاری مستقیم بر جامعه گام بردارند. در این چارچوب، مفاهیم «دانشگاه نسل چهارم» و به‌ویژه «دانشگاه نسل پنجم»، به‌عنوان مدل‌های پیشرو، در مرکز توجه نظام‌های علمی و سیاست‌گذاران آموزشی قرار گرفته‌اند.

دانشگاه‌های نسل چهارم با تأکید بر نوآوری، تعاملات بین‌رشته‌ای، مشارکت در توسعه منطقه‌ای و پیوند عمیق با جامعه، توانستند مرزهای سنتی آموزش و پژوهش را درنوردند. در این میان، فناوری اطلاعات به مثابه پیشران اصلی این تحول، نقشی کلیدی ایفا کرده است. از زیرساخت‌های آموزش هوشمند گرفته تا تحلیل کلان‌داده‌ها، از سیستم‌های تصمیم‌یار مدیریتی تا پلتفرم‌های هوش مصنوعی؛ همگی نشانه‌هایی از باز تعریف کارکرد دانشگاه در بستر دنیای دیجیتال هستند. حضور سیستم‌های یادگیری الکترونیکی، پلتفرم‌های تعاملی آموزش مجازی، ابزارهای تحلیل داده‌های پژوهشی، سامانه‌های هوشمند مدیریت منابع و تصمیم‌یارهای پیشرفته، گواهی روشن بر این نقش زیرساختی است. فناوری حتی در طراحی محتوا، روش‌های تدریس، شبیه‌سازی‌های پیشرفته، مسیر تازه‌ای برای آموزش گشوده و در پژوهش نیز با فراهم‌سازی امکان تحلیل کلان‌داده‌ها و شبکه‌سازی علمی، افق‌های تازه‌ای را پیش روی دانشگاهیان قرار داده است.

از سوی دیگر، در حوزه مدیریت دانشگاهی، فناوری اطلاعات امکان یکپارچه‌سازی داده‌ها، ارزیابی اثربخش عملکرد، شفاف‌سازی فرآیندها، و ارائه بینش‌های تحلیلی برای تصمیم‌گیری راهبردی را فراهم کرده است. در ارتباط با جامعه نیز، فناوری به دانشگاه‌ها این توان را داده تا با شیوه‌هایی نوین در تعامل باشند، محتوا تولید کنند، خدمات مشاوره‌ای ارائه دهند، در حل مسائل واقعی ایفای نقش کنند و بستری برای نوآوری و کارآفرینی دانش‌بنیان فراهم آورند.

دانشگاه نسل پنجم، فراتر از مأموریت‌های سنتی خود، به‌مثابه یک کنشگر فناورانه و اجتماعی ظاهر می‌شود؛ نهادی یادگیرنده، مسئله‌محور، و مسئول در برابر تحولات محیطی. چنین دانشگاهی، یک زیست‌بوم پویا و داده‌محور است که در آن آموزش شخصی‌سازی‌شده، پژوهش کاربردی، نوآوری مشارکتی و تعامل مستمر با جامعه در هم تنیده‌اند.

امروز، دانشگاهی می‌تواند مدعی نسل پنجم بودن باشد که نه‌تنها آموزش و پژوهش را بازآفرینی می‌کند، بلکه به عنوان یک کنشگر اجتماعی فناورانه، نقش مستقیم در آینده‌سازی ایفا می‌نماید. دانشگاه نسل پنجم یک «زیست‌بوم دانایی‌محور» است؛ جایی که آموزش شخصی‌سازی‌شده، پژوهش مسئله‌محور، نوآوری کاربرمحور و حکمرانی داده‌محور، هسته‌های اصلی آن را شکل می‌دهند.

در این مسیر، فناوری اطلاعات نه صرفاً ابزار، بلکه یک بنیان‌گذار جدید تفکر سیستمی است. تحول در مدیریت داده‌ها، ظهور دانشگاه‌های هوشمند، توسعه مدل‌های یادگیری تطبیقی، طراحی پلتفرم‌های تعاملی برای سیاست‌گذاری، و هوش مصنوعی به عنوان مشاور آموزشی و پژوهشی، همه و همه از فناوری اطلاعات ریشه می‌گیرند.

«پالسی‌نو» در تلاش است با نگاهی آینده‌نگر و تحلیلی، بستری برای گفت‌وگو پیرامون این تحولات فراهم آورد. رسالت ما آن است که این دگردیسی را نه به‌عنوان یک رویداد فناورانه، بلکه به مثابه یک گذار اندیشه‌ای درک و ترویج کنیم.

امید است این نشریه، با مشارکت ارزشمند همکاران دانشگاهی و بهره‌گیری از تازه‌ترین دیدگاه‌ها و منابع علمی، بتواند سهمی در ترسیم چشم‌انداز آینده دانشگاه‌ها داشته باشد؛ دانشگاه‌هایی که با بهره‌گیری هوشمندانه از ابزارهای نوین، به تعالی علمی، نوآوری و پاسخگویی مؤثر به نیازهای جامعه نزدیک‌تر می‌شوند.

متاورس درمانی

گامی نوین در تحول خدمات سلامت

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

کلمه متاورس (**Metaverse**) از دو بخش تشکیل شده است: "متا" (**Meta**) به معنای فراتر یا ماورا، و "ورس" (**Verse**) که به معنای جهان یا کیهان است. در نتیجه، متاورس به معنای یک جهان فراتر یا یک دنیای دیجیتال و مجازی است که در آن افراد می‌توانند با استفاده از فناوری‌هایی مثل واقعیت مجازی (**VR**)، واقعیت افزوده (**AR**) یا حتی صفحه‌نمایش‌های ساده، به‌صورت تعاملی فعالیت کنند. این فضا شبیه یک دنیای سه‌بعدی است که افراد در آن می‌توانند حرکت کنند، با دیگران ارتباط برقرار کنند، کار کنند، بازی کنند یا حتی خدمات مختلفی دریافت کنند، انگار که در یک دنیای واقعی هستند، اما همه‌چیز در محیط دیجیتال اتفاق می‌افتد. در سال‌های اخیر، فناوری متاورس از حوزه سرگرمی و بازی‌های دیجیتال فراتر رفته و به بخش‌های مهمی مانند آموزش، تجارت و به‌ویژه مراقبت‌های بهداشتی وارد شده است. متاورس درمانی یک دنیای مجازی سه‌بعدی است که در آن بیماران، پزشکان و متخصصان از طریق ابزارهایی مانند هدست‌های واقعیت مجازی، گوشی‌های هوشمند یا کامپیوتر با یکدیگر تعامل می‌کنند. تصور کنید وارد یک کلینیک مجازی می‌شوید، با پزشک خود گفت‌وگو می‌کنید، تمرینات توان‌بخشی انجام می‌دهید یا در جلسات گروهی برای حمایت روانی شرکت می‌کنید، بدون اینکه از خانه خارج شوید. این فناوری، که ترکیبی از واقعیت مجازی (**VR**)، واقعیت افزوده (**AR**) و محیط‌های سه‌بعدی تعاملی است، توانایی حذف موانع جغرافیایی و فیزیکی را دارد و دسترسی به خدمات سلامت را برای افراد در مناطق دورافتاده یا با محدودیت‌های حرکتی تسهیل می‌کند. به بیان ساده، متاورس درمانی مانند یک بازی ویدئویی پیشرفته است که برای درمان، آموزش و مراقبت طراحی شده و با رعایت حریم خصوصی و ایمنی، اثربخشی بالایی دارد.

اهداف متاورس درمانی

هدف اصلی متاورس درمانی، افزایش دسترسی به خدمات سلامت برای همه، در هر زمان و مکان است. این فناوری با اهداف زیر طراحی شده است:

- کاهش هزینه‌های درمان:
  حذف نیاز به سفر یا استفاده از تجهیزات گران‌قیمت.
- افزایش تعامل بیمار و پزشک:
  ارائه درمان‌های شخصی‌سازی‌شده با ارتباط نزدیک‌تر.
- بهبود آموزش پزشکی:
  شبیه‌سازی‌های واقعی برای یادگیری بهتر پزشکان و دانشجویان.
- حمایت از بیماران مزمن:
  ایجاد گروه‌های مجازی برای مشاوره و پشتیبانی عاطفی.

به طور کلی، متاورس درمانی قصد دارد مراقبت‌های بهداشتی را دیجیتال، فراگیر و کارآمد کند.

کاربردهای متاورس درمانی

متاورس درمانی در زمینه‌های متعددی کاربرد دارد و می‌تواند خدمات سلامت را متحول کند. مهم‌ترین کاربردها عبارتند از:

- روان‌درمانی و درمان اضطراب:
  شبیه‌سازی محیط‌های کنترل‌شده برای درمان فوبیا یا اختلال استرس پس از سانحه (**PTSD**)، که اضطراب را بدون خطر واقعی کاهش می‌دهد.
- توان‌بخشی حرکتی و نورولوژیک:
  تمرینات مجازی برای بیماران سکته مغزی یا آسیب نخاعی با بازخورد آنی، که انگیزه بیماران را از طریق بازی‌وارسازی افزایش می‌دهد.
- آموزش پزشکی:
  شبیه‌سازی جراحی‌ها و سناریوهای بالینی برای دانشجویان پزشکی، که امکان تمرین ایمن بدون نیاز به بیمار واقعی را فراهم می‌کند.
- حمایت از بیماران مزمن:
  گروه‌های مجازی برای بیماران مبتلا به بیماری‌هایی مانند سرطان، که حس انزوا را کاهش می‌دهد.
- مشاوره و تشخیص از راه دور:
  ملاقات مجازی با پزشکان برای بررسی علائم یا پیگیری درمان، که دسترسی به متخصصان را به‌ویژه در بحران‌هایی مثل همه‌گیری‌ها تسهیل می‌کند.

این کاربردها نشان می‌دهند که متاورس درمانی نه تنها برای درمان جسمی، بلکه برای سلامت روان، پیشگیری و آموزش

نیز مؤثر است.

چگونه از متاورس درمانی استفاده کنیم؟

استفاده از متاورس درمانی ساده است، اما نیاز به ابزارها و مراحل مشخصی دارد:

۱. تجهیزات مورد نیاز: استفاده از هدست‌های واقعیت مجازی ایده‌آل هستند، اما گوشی‌های هوشمند یا کامپیوتر با اپلیکیشن‌های واقعیت افزوده و اینترنت پرسرعت نیز کافی است.
۲. ورود به محیط مجازی: کاربران از طریق اپلیکیشن یا وب‌سایت وارد متاورس شده و یک آواتار برای خود می‌سازند تا حس راحتی بیشتری داشته باشند.
۳. فعالیت‌های درمانی: در کلینیک مجازی، بیمار می‌تواند با پزشک گفت‌وگو کند، تمرینات حرکتی انجام دهد یا در جلسات گروهی شرکت کند. درمانگر از راه دور داده‌هایی مانند ضربان قلب یا حرکات بیمار را تحلیل می‌کند.
۴. پایش و امنیت: داده‌های پزشکی با رعایت حریم خصوصی (مانند رمزنگاری) جمع‌آوری می‌شوند و جلسات معمولاً ۳۰ تا ۶۰ دقیقه طول می‌کشند.

آموزش اولیه برای آشنایی با ابزارها ضروری است، اما فرآیند برای کاربران عادی نیز قابل فهم است.

نمونه‌های موفق جهانی

تجربه‌های جهانی نشان‌دهنده اثربخشی متاورس درمانی هستند:

- انگلستان: شرکت **Oxford VR** از واقعیت مجازی برای درمان اضطراب اجتماعی و فوبیا استفاده می‌کند و کاهش ۶۸ درصدی اضطراب را گزارش کرده است.
- کره جنوبی: شرکت **TechVillage** برنامه‌های واقعیت مجازی برای توان‌بخشی بیماران سکته مغزی طراحی کرده و دستکش هوشمند **Neofect** حرکت دست بیماران را بهبود داده است.
- ایالات متحده: دانشگاه‌های **Stanford** و **Ohio State** از متاورس برای آموزش پزشکی استفاده می‌کنند و شرکت **XRHealth** مشاوره‌های مجازی ارائه می‌دهد.
- استرالیا: انجمن **Cancer Council** از فضاهای مجازی برای گروه‌های حمایتی بیماران سرطانی استفاده می‌کند، که حس انزوا را کاهش داده است.

این پروژه‌ها نشان می‌دهند که متاورس می‌تواند هزینه‌های درمان را تا ۳۰ درصد کاهش دهد و مشارکت بیماران را افزایش دهد.

مسیر پیاده‌سازی متاورس درمانی در ایران

ایران با زیرساخت‌های دیجیتال رو به رشد (مانند اینترنت ۵G) و نیروی انسانی متخصص، پتانسیل بالایی برای متاورس درمانی دارد. این فناوری می‌تواند در گردشگری سلامت نیز نقش داشته باشد. برای پیاده سازی این فناوری اجرای گام های زیر ضروری بنظر می رسد:

۱. آموزش و آگاهی: برگزاری کارگاه‌های آموزشی برای پزشکان و مدیران سلامت.
۲. حوزه‌های اولویت‌دار: شروع با روان‌درمانی آنلاین و توان‌بخشی نورولوژیک.
۳. توسعه زیرساخت: بهبود دسترسی به اینترنت پرسرعت، ایجاد اپلیکیشن‌های بومی واقعیت مجازی و مراکز داده امن.
۴. پروژه‌های آزمایشی: آزمایش فناوری در بیمارستان‌های پایلوت، با تمرکز بر بیماران مناطق روستایی.
۵. حمایت قانونی: تدوین قوانین برای حفظ حریم خصوصی، پوشش بیمه‌ای و جلوگیری از نابرابری در دسترسی.

متاورس درمانی نمادی از ترکیب فناوری و مراقبت‌های بهداشتی است که می‌تواند محدودیت‌های جغرافیایی و مالی را کاهش دهد و کیفیت زندگی را بهبود ببخشد. نمونه‌های موفق جهانی اثربخشی این فناوری را تأیید می‌کنند. در ایران نیز، با همکاری دانشگاه‌ها و شرکت‌های دانش‌بنیان و با برنامه‌ریزی دقیق و تمرکز بر آموزش، توسعه زیرساخت و مسائل اخلاقی، متاورس درمانی می‌تواند دسترسی به خدمات سلامت را افزایش داده و نظام سلامت را مدرن‌تر کند.

منابع:

1. Mesk ó , B., & G□r□g, M. (2022). A short guide for medical professionals in the era of the metaverse. Journal of Medical Internet Research, 24(3), e34653.
2. Thomason, J. (2021). MetaHealth: How will the metaverse change healthcare? Journal of Metaverse, 1(1), 13-18.
3. Skalidis, I., et al. (2022). The metaverse in cardiovascular healthcare: Opportunities and challenges. Frontiers in Cardiovascular Medicine, 9, 1011910.
4. Yang, D., et al. (2022). Metaverse in medicine: Opportunities, challenges, and future. Frontiers in Medicine, 9, 1038902.
5. Wang, G., et al. (2023). Metaverse-based telemedicine: Feasibility and challenges. Telemedicine and e-Health, 29(4), 567-575.
6. Bansal, G., et al. (2022). Healthcare in metaverse: A survey on current applications. IEEE Access, 10, 112345-112360.
7. Kye, B., et al. (2021). Medical education in the metaverse: A new era of training. Medical Education Online, 26(1), 1993956.
8. Stanford Medicine. (2023). Virtual reality in medical training. Retrieved from https://med.stanford.edu/news/vr-training.html
9. XRHealth. (2023). Virtual clinics in the metaverse. Retrieved from https://www.xr.health/virtual-clinics
10. TechVillage. (2022). VR rehabilitation programs. Retrieved from https://www.techvillage.co.kr/rehabilitation
11. Ghanbarzadeh, R., et al. (2023). Digital health in Iran: Challenges and opportunities. Iranian Journal of Public Health, 52(5), 897-905.
12. Cancer Council Australia. (2023). Virtual support groups for cancer patients. Retrieved from https://www.cancer.org.au/virtual-support
13. Oxford VR. (2023). Virtual reality therapy outcomes. Retrieved from https://www.oxfordvr.org/outcomes

یو پی اس در اتاق سرور و نحوه محاسبه توان مورد نیاز

وحید عباس‌زاده
دانشجوی PHD الکترونیک
کارشناس شبکه

در حوزه فناوری اطلاعات (IT)، یو پی اس (UPS) یک جزء حیاتی است که برای محافظت از تجهیزات و داده‌ها در برابر اختلالات برق ضروری است. یو پی اس با تأمین برق بدون وقفه و پایدار، از تجهیزات حساس مانند سرورها، سوئیچ‌ها، و سایر تجهیزات شبکه در برابر قطعی برق، نوسانات ولتاژ و سایر مشکلات الکتریکی محافظت می‌کند. این امر به ویژه در اتاق‌های سرور و دیتاسنترها که تجهیزات حیاتی در آن قرار دارند، اهمیت بیشتری پیدا می‌کند.

اهمیت یو پی اس در IT

- جلوگیری از از دست رفتن داده‌ها
- حفاظت از تجهیزات
- تداوم عملکرد
- کاهش هزینه‌ها

انواع یو پی اس در IT

- یو پی اس آنلاین
- یو پی اس لاین اینتراکتیو
- یو پی اس آفلاین

با توجه به اهمیت یو پی اس در IT و مزایای فراوانی که به همراه دارد، انتخاب و استفاده از یو پی اس مناسب برای هر سازمان و شرکت ضروری است.

راهنمای انتخاب یو پی اس

- ظرفیت: ظرفیت یو پی اس باید بر اساس توان مصرفی تجهیزات و مدت زمان مورد نیاز برای پشتیبانی از برق اضطراری انتخاب شود.
- نوع یو پی اس: نوع یو پی اس باید با توجه به نوع تجهیزات و نیازهای پایداری و کیفیت برق انتخاب شود.
- ویژگی‌های اضافی: برخی از یو پی اس‌ها دارای ویژگی‌های اضافی مانند مدیریت از راه دور، حفاظت از نوسانات ولتاژ و قابلیت مقیاس‌پذیری هستند که باید با توجه به نیازهای سازمان انتخاب شوند.

نحوه محاسبه توان مورد نیاز

برای محاسبه توان مورد نیاز برای یک یو پی اس (**UPS**)، باید مجموع توان مصرفی تمام دستگاه‌هایی که قرار است توسط یو پی اس تغذیه شوند محاسبه شود و سپس با در نظر گرفتن ضریب توان و یک حاشیه ایمنی، توان مناسب انتخاب گردد.

مراحل محاسبه

۱. تعیین توان مصرفی دستگاه‌ها:
- توان مصرفی هر دستگاه را بر حسب وات (**W**) یا ولت-آمپر (**VA**) از روی برچسب یا دفترچه راهنمای آن پیدا شود.
- اگر توان مصرفی بر حسب وات است، می‌توان آن را با استفاده از فرمول **VA = W / PF** که در آن **PF** ضریب توان است به ولت-آمپر تبدیل کرد.

۲. محاسبه مجموع توان مصرفی:
- توان‌های مصرفی تمام دستگاه‌ها با هم جمع می گردد تا مجموع توان مصرفی کل دستگاه‌ها بدست آید.

محاسبه KVA با در نظر گرفتن ضریب توان

- اگر مجموع توان مصرفی بر حسب وات است، بر ضریب توان (معمولاً ۰.۸ یا ۰.۷ برای یو پی اس) تقسیم می گردد تا توان بر حسب **VA** بدست آید.
- اگر مجموع توان مصرفی بر حسب **VA** است، این مقدار به **KVA** تبدیل می شود (تقسیم بر ۱۰۰۰).

اضافه کردن حاشیه ایمنی

- توصیه می‌شود که توان یو پی اس کمی بیشتر از مقدار محاسبه شده انتخاب شود تا در صورت افزایش بار یا نوسانات، یو پی اس بتواند عملکرد مناسبی داشته باشد.
- حاشیه ایمنی ۲۰ تا ۳۰ درصدی در نظر گرفته می شود.

مثال

با فرض نیاز به یک یو پی اس برای ۲ کامپیوتر با توان ۲۵۰ وات و یک سرور با توان ۱۵۰۰ وات

۱. توان هر کامپیوتر: ۲۵۰ وات
۲. مجموع توان مصرفی کامپیوترها: ۲ * ۲۵۰ = ۵۰۰ وات
۳. توان مصرفی سرور: ۱۵۰۰ وات
۴. اگر ضریب توان ۰.۸ در نظر گرفته شود، توان بر حسب **VA** برابر است با ۰.۸ / ۲۰۰۰ = ۲۵۰۰
۵. با در نظر گرفتن ٪۲۰ حاشیه ایمنی، توان مورد نیاز برابر است با: ۲۵۰۰ * ۱.۲ = ۳۰۰۰ ولت آمپر یا ۳ کیلو ولت آمپر
۶. بنابراین، یک یو پی اس ۳ کیلو ولت آمپر برای این منظور مناسب است.

مینیمالیسم دیجیتال: رویکردی نوین برای ارتقای کیفیت زندگی فردی، اجتماعی و حرفه‌ای

نویده خدائی
دانشجوی دکتری مدیریت فناوری اطلاعات

مقدمه

در عصر ارتباطات دیجیتال، حضور مستمر در فضای مجازی فرصت‌ها را هم افزایش داده و هم چالش‌های جدیدی ایجاد کرده است. مینیمالیسم دیجیتال رویکردی است که استفاده‌ی هوشمندانه و هدفمند از فناوری‌ها را ترویج می‌دهد تا کیفیت زندگی فردی، روابط اجتماعی و بهره‌وری شغلی ارتقا یابد.

مفهوم مینیمالیسم دیجیتال

Cal Newport در کتاب خود این مفهوم را چنین تعریف می‌کند:
« مینیمالیسم دیجیتال فلسفه‌ای است برای تجدیدنظر نسبت به ابزارهای ارتباطی دیجیتال — و رفتارهای پیرامون آنها — که بیشترین ارزش را به زندگی‌تان اضافه می‌کنند.»
او پیشنهاد می‌کند که با حذف «سر و صداهای دیجیتال» کم‌ارزش و بهینه‌سازی استفاده از ابزارهایی که ارزش واقعی دارند، می‌توان کیفیت زندگی را به طرز قابل‌توجهی ارتقا داد . رویکرد او شامل فرآیند سی روزه‌ای است که در آن ابتدا ابزارهای غیرضروری حذف شده و جایگزین‌هایی معنادار در زندگی جایگزین می‌شوند .

تأثیرات در زندگی فردی

- آرامش روانی و تمرکز بیشتر: خاموش‌کردن اطلاع‌رسان‌ها (**notifications**) باعث کاهش حواس‌پرتی و تمرکز بهتر می‌شود .
- مدیریت بهتر زمان: تمرکز بر ابزارهای ضروری و کاهش پراکندگی دیجیتال، موجب صرفه‌جویی در زمان و افزایش کارایی می‌شود .
- افزایش خودآگاهی و رشد شخصی: زمانی برای تفکر عمیق و فعالیت‌های غیر دیجیتال باقی می‌ماند که به رشد فردی کمک می‌کند .
- سلامت جسمانی بهتر: کاهش استفاده از صفحه‌نمایش‌ها می‌تواند کیفیت خواب و سلامت چشم را بهبود بخشد .

تأثیرات در زندگی اجتماعی

- ارتباطات حضوری با کیفیت‌تر: کاهش تمرکز بر فضای مجازی، افراد را به تعامل واقعی و حضور آگاهانه در جمع‌ها سوق می‌دهد .
- افزایش سرمایه اجتماعی: برگزاری نشست‌های بدون تلفن یا حضور حضوری ارزش روابط انسانی را تقویت می‌کند .
- کاهش تنهایی و انزوا: دوری از مقایسه‌های مجازی کمک می‌کند احساس تعلق و ارتباط واقعی افزایش یابد .
- افزایش سواد رسانه‌ای: استفاده هوشمندانه از رسانه‌ها منجر به فرهنگ‌سازی مثبت و کاهش آسیب‌های اجتماعی می‌شود .

تأثیرات در محیط کار

- بهره‌وری بیشتر با تمرکز عمیق: حذف حواس‌پرتی‌های دیجیتال مانند ایمیل‌های لحظه‌ای امکان انجام کار عمیق (**Deep Work**) را فراهم می‌کند (**Newport**)
- کاهش فرسودگی شغلی (**Technostress**): فشار ناشی

از استفاده‌ی زیاد از فناوری در کار به نام تکنواسترس شناخته شده که می‌تواند با استراتژی‌های مینیمالیسم دیجیتال کنترل شود .

- ارتباطات شفاف‌تر: استفاده از یک پلتفرم مشخص ارتباطی نظم کاری را افزایش داده و سردرگمی را کاهش می‌دهد .
- حفظ خلاقیت و نوآوری: فضای آرام به تفکر خلاق و برنامه‌ریزی جدید کمک می‌کند .
- تعهد سازمانی و کاهش اضطراب دیجیتال: تعهد سازمانی قوی همراه با فرهنگ اخلاقی می‌تواند اضطراب ترک اتصال دیجیتال (**nomophobia**) را کاهش دهد .

راهکارهای عملی اجرای مینیمالیسم دیجیتال

در زندگی فردی

۱. زمان‌بندی مشخص برای استفاده از دستگاه‌های دیجیتال.
۲. غیرفعال کردن اعلان‌های غیرضروری.
۳. اجرای فرآیند سی‌روزه برای حذف اپ‌ها و جایگزینی فعالیت‌های معنادار .
۴. تعیین مناطق بدون فناوری (مثل اتاق خواب یا زمان غذا).

در زندگی اجتماعی

۱. برگزاری نشست‌های بدون تلفن همراه.
۲. طرح «ساعات دیجیتال آزاد» برای تفکر و تعامل حضوری.
۳. آموزش سواد دیجیتال و ترویج استفاده آگاهانه در خانواده و جامعه.

در محیط کار

۱. تعیین یک کانال ارتباطی استاندارد (مثلاً ایمیل رسمی یا پیام‌رسان واحد).
۲. زمان‌بندی «کار عمیق» بدون دخل و تصرف دیجیتال .
۳. پیاده‌سازی سیاست‌های سازمانی در استفاده از فناوری (مثلاً محدودیت استفاده از شبکه‌های اجتماعی در ساعات کاری).
۴. ایجاد محیط‌های فیزیکی و دیجیتال آرام مانند بازه‌های تمرکز.
۵. تقویت تعهد اخلاقی و سازمانی برای کاهش اضطراب دیجیتال.

نتیجه‌گیری

مینیمالیسم دیجیتال بیش از یک سبک زندگی است؛ در واقع یک فلسفه برای بازسازی کیفیت زندگی در جهت سلامت روانی، تعاملات انسانی و بهره‌وری سازمانی است. با انتخاب آگاهانه فناوری، افراد و سازمان‌ها می‌توانند از چرخه فشار دیجیتال به تعادل حقیقی بازگردند.

منابع:

1. Newport, C. (2019). Digital Minimalism: Choosing a Focused Life in a Noisy World. Portfolio/Penguin.
2. Pielot, M., & Rello, L. (2016). Productive, Anxious, Lonely – 24 Hours without Push Notifications. arXiv.
3. Atrian, A., & Ghobbeh, S. (2023). Technostress and Job Performance: Understanding the Negative Impacts and Strategic Responses in the Workplace. arXiv.
4. Bai, A., & Vahedian, M. (2023). Beyond the Screen: Safeguarding Mental Health in the Digital Workplace through Organizational Commitment and Ethical Environment. arXiv.
5. VirtualStaff.ph (2024). The Role of Digital Minimalism in Remote Work: Focus on What Matters.
6. UpriseHealth (2025). From Overwhelm to Balance: Leveraging Digital Minimalism.

ویکی واژه

در عصری که تهدیدهای 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.

ویکی واژه
WIKIWORD

سید محمدحسن الهی

اکسپلویت

اکسپلویت یک تکنیک یا قطعه نرم‌افزاری است که از آسیب‌پذیری‌های موجود در یک سیستم، برنامه یا شبکه برای دسترسی غیرمجاز یا ایجاد رفتار ناخواسته استفاده می‌کند. اکسپلویت‌ها اغلب توسط مهاجمان برای نقض دفاع امنیتی و به خطر انداختن دارایی‌های دیجیتال استفاده می‌شوند.

EXPLOIT
EXPLOIT

دانلود کننده‌ها

دانلودکننده نوعی نرم‌افزار مخرب است که برای بازیابی و نصب مخفیانه برنامه‌های مضر اضافی بر روی یک سیستم آسیب‌دیده طراحی شده است.

این نرم‌افزار به عنوان یک مکانیسم تحویل عمل می‌کند و مهاجمان را قادر می‌سازد تا کنترل خود را گسترش داده و تهدیدات پیچیده‌تری را به کار گیرند.

DOWNLOADER
DOWNLOADER

کلید نگارها

کلیدنگار نوعی نرم‌افزار یا سخت‌افزار نظارتی است که هر ضربه کلید انجام شده توسط کاربر را ثبت می‌کند. کلیدنگارها که اغلب به صورت مخفیانه نصب می‌شوند، اطلاعات حساس مانند رمزهای عبور و داده‌های شخصی را ضبط می‌کنند و در نتیجه حریم خصوصی و امنیت کاربر را تهدید می کنند.

KEYLOGGER
KEYLOGGER

جاسوس افزارها

جاسوس‌افزار نرم‌افزار مخربی است که برای نظارت مخفیانه و جمع‌آوری اطلاعات در مورد فعالیت‌های کاربر بدون رضایت او طراحی شده است. این نرم‌افزار داده‌ها را به اشخاص ثالث منتقل می‌کند، حریم خصوصی را به خطر می‌اندازد و به طور بالقوه حملات بیشتر را تسهیل می‌کند.

باج افزارها

باج‌افزار نوعی بدافزار شدید است که داده‌های قربانی را رمزگذاری می‌کند یا دسترسی به سیستم‌ها را قفل می‌کند و در ازای بازگرداندن دسترسی، درخواست باج می‌کند. این یک تهدید مهم و رو به رشد برای افراد و سازمان‌ها است و می‌تواند عواقب ویرانگری داشته باشد.

فلادر یا سِیل‌سازها

فلادر ابزاری یا اسکریپتی است که برای تحت الشعاع قرار دادن یک شبکه، سرور یا سرویس شبکه با حجم بیش از حد ترافیک یا درخواست‌ها استفاده می‌شود و منجر به انکار سرویس DoS می‌شود. حملات سیل‌آسا عملکرد و در دسترس بودن سیستم را کاهش می‌دهد و تهدیدات جدی برای قابلیت اطمینان شبکه ایجاد می‌کند.

آگهی‌افزار

نرم‌افزاری است که به طور خودکار، اغلب بدون رضایت صریح کاربر، مطالب تبلیغاتی را نمایش یا دانلود می‌کند. اگرچه همیشه مخرب نیست، اما نرم‌افزارهای تبلیغاتی مزاحم می‌توانند تجربه کاربری را خراب کنند و گاهی اوقات به عنوان مجرایی برای برنامه‌های مضرتر عمل کنند.

تحول در امنیت سایبری سازمان‌ها با AI و GENERATIVE AI

فریبا اسماعیلی
کارشناس ارشد مهندسی نرم افزار
کارشناس فناوری اطلاعات دانشکده پرستاری و مامایی

مقدمه

«تحول»، همان اصلاح و یا بهبود نیست. «تحول» یعنی تغییر بزرگ و شگرف. «تحول» یعنی تغییر در ماهیت و منطق یک پدیده.
تحول با هوش مصنوعی، تغییری شگرف در عملکرد یک سازمان و یا یک کشور با محوریت فناوری‌های تحول‌آفرین است. تحول دیجیتال سازمانی به معنای ساخت سازمانی در تراز عصر دیجیتال می‌باشد.. در دنیای دیجیتال، با رشد تکنولوژی، هوش مصنوعی (**AI**) به یکی از ابزارهای کلیدی در بهبود امنیت سایبری تبدیل شده و به عنوان یک ابزار تحول‌آفرین، قابلیت‌های بی‌سابقه‌ای را برای شناسایی، پیشگیری و پاسخ به تهدیدات سایبری فراهم کرده است. بدین ترتیب، امنیت سایبری وحفاظت از داده‌ها و اطلاعات به یکی از بزرگترین چالش‌های سازمان ها تبدیل شده است.

بحث

بر اساس گزارش علمی و تحقیقی جدید موسسه تحقیقاتی **Cap Gemini** پیرامون تهدیدات جدید و دفاع‌های جدید در مقابل تهدیدهای سایبری نشان داده شد که خطرات جدید امنیت سایبری به دلیل گسترش هوش مصنوعی(**AI**) و هوش مصنوعی مولد (**Gen AI**) در حال ظهور هستند، این فناوری‌ها یک تغییرات اساسی در جهت تقویت استراتژی‌های دفاع سایبری اعم از: پیش‌بینی، شناسایی و پاسخ به تهدیدات، برای بلندمدت ایجاد می‌نمایند. همچنین نتایج آن تحقیق نشان داده که دو سوم سازمان‌ها اکنون استفاده از هوش مصنوعی را در عملیات امنیتی خود در اولویت قرار می‌دهند. از طرفی افزایش پذیرش هوش مصنوعی نسل جدید (**Gen AI**) در صنایع مختلف، باعث افزایش خطر آسیب‌پذیری در سه حوزه عمده زیر برای سازمان‌ها نیز گردیده است:
حملات پیچیده‌تر با دشمنان بیشتر، گسترش سطح حملات سایبری، رشد آسیب‌پذیری‌ها، در کل چرخه عمرهوش مصنوعی.
نتایج یک نظرسنجی جدید دیگر از افسران ارشد امنیت اطلاعات (**CISOs**) در ایالات متحده و بریتانیا نشان داد آنها نسبت به احتمال نقض امنیتی ناشی از فناوری‌های هوش مصنوعی مولد (**Gen AI**) نگران هستند. این تحقیق نشان داد که تعداد فزاینده‌ای از نقض داده ها در صنایع مختلف رخ می دهد و ۷۲ درصد از پاسخ دهندگان نسبت به این تهدید جدید ابراز نگرانی کرده‌اند.
هوش مصنوعی(**AI**) با استفاده از الگوریتم‌ها و تکنیک‌های یادگیری ماشین (**Machine Learning**)، همچنین تحلیل پیش‌بینانه به سازمان‌ها اجازه می‌دهد تا با سرعت بیشتری به تهدیدات پاسخ دهند و زمان و هزینه‌های مربوط به مدیریت رخدادهای امنیتی را کاهش دهند و در تحلیل داده‌های بزرگ و شناسایی الگوهای پنهان نقش حیاتی ایفا می‌کند، که به روش‌های سنتی قابل دسترسی نیست.
سازمانها در ایران نیز از این قاعده مستثنی نمی باشد. با وجود مزایای هوش مصنوعی، نبود استراتژی امنیتی مبتنی بر هوش مصنوعی در این کشور چالش‌های متعددی در مسیر پیاده‌سازی آن برای سازمانها به وجود آورده است.

چالشها و تهدیدات

کشورهای پیشرفته، با استفاده از سیستم‌هایی همچون **XDR** (**Extended Detection and Response**) و **SIEM (Security Information and Event Management)** مجهز به هوش مصنوعی، تهدیدات را شناسایی و پیش از وقوع، آن‌ها را خنثی می‌کنند. اما در ایران، بسیاری از سازمان‌ها حتی از نسخه‌های استاندارد این ابزارها نیز استفاده نمی‌کنند! این عدم آمادگی، ضمن به خطر انداختن زیرساخت‌های حیاتی کشور، باعث بوجود آمدن چالشهایی مانند: کمبود داده‌های باکیفیت، کاهش دقت سیستم‌ها، تحریم و محدودیت دسترسی سازمانهای ایرانی به برخی از پیشرفته‌ترین ابزارهای هوش مصنوعی و سخت‌افزارهای مورد نیاز، گردیده است. همچنین استفاده اغلب سازمان‌ها از فایروال‌های قدیمی و سیستم‌های تشخیص نفوذ (**IDS**) غیرهوشمند و نبود سرمایه‌گذاری روی امنیت سایبری در بسیاری از سازمانهای دولتی و خصوصی داخل کشور راهکارهای امنیتی سازمانها را در برابر حملات نوین بی‌اثر نموده است.
عدم آموزش نیروهای متخصص به دلیل نبود برنامه‌های آموزشی جامع، عدم آشنایی کافی با ابزارهای مدرن، منجر به عدم پیاده سازی راهکارهای پیشرفته می‌گردد. بر اساس گزارش‌ها، کشورهای پیشرفته بیش از ٪۷۰ از نیروی متخصص جهانی را در اختیار دارند،

درحالی‌که ایران با کمبود جدی در این زمینه مواجه است. از طرفی نبود قوانین و سیاست‌های امنیت سایبری جامع در ایران بر چالش های هوش مصنوعی در سازمانها نیز افزوده است.
نتایج تحقیق **CISO** ها همچنان نشان داد که حفظ و ایجاد یک فرهنگ امنیتی قوی بسیار برای سازمانها لازم و ضروری است، در حالی که آنها در تدوین و حفظ یک فرهنگ امنیتی مؤثر با مشکلات متعددی روبرو هستند. بیش از ۵۰ درصد از پاسخ دهندگان به نظرسنجی در آن تحقیق از حملات بدافزار یا فیشینگ، به صورت پراکنده یا منظم، لذت برده‌اند. در سازمان‌ها با سوءاستفاده از هوش مصنوعی (**AI**) و هوش مصنوعی نسل جدید (**Gen AI**) توسط کارمندان، از طریق طراحی بدافزارهای پیشرفته، شخصی‌سازی حملات فیشینگ، تولید محتوای مغرضانه، مضر یا نامناسب، خطر نشت داده‌ها را به میزان قابل توجهی افزایش می دهد.

نقش AI بر روی تهدیدات سایبری

با توجه به اینکه بدافزارهای مبتنی بر هوش مصنوعی (**Gen AI**) به قابلیت تطبیق رفتار مجهز هستند و به این ترتیب می‌توانند خود را از سیستم‌های امنیتی پنهان کنند و نقش بسیار پررنگتری در تهدیدات سایبری ایجاد نمایند. در فضای پرتلاطم جنگ سایبری، امنیت تنها در صورتی پیروز میدان خواهد بود که پیشرفت‌های فناوری و استراتژی‌های هوشمندانه در کنار هم قرار گیرند. ابزارهایی مانند **FortiAI**، با استفاده از قدرت هوش مصنوعی، توانایی شناسایی سریع تهدیدات، تجزیه وتحلیل الگوهای مشکوک و خنثی‌سازی حملات سایبری را به طور چشمگیری افزایش داده‌اند. این دستیار هوشمند همراه با به‌روزرسانی همیشگی بانک اطلاعاتی **FortiGuard**، امکان دسترسی به جدیدترین داده‌ها و الگوهای تهدیدات سایبری را فراهم می‌آورد. ترکیب چنین فناوری‌هایی با آموزش مستمر متخصصان و همکاری‌های جهانی می‌تواند امنیت را به قهرمان بی‌چون‌وچرای این میدان تبدیل کند.

راهکارها

توسعه سیستم‌های امنیتی مجهز به هوش مصنوعی، که علاوه بر استفاده از فناوری‌های خارجی، با محیط سایبری کشور نیز سازگار باشد. همچنین سرمایه‌گذاری در فناوری‌های پیشرفته، آموزش و ارتقای دانش متخصصان امنیت سایبری و ایجاد چارچوب‌های قانونی سخت‌گیرانه برای امنیت سایبری.

نتیجه‌گیری

در جهانی که مهاجمان از پیشرفته‌ترین تکنولوژی‌ها برای نفوذ به سیستم‌ها استفاده می‌کنند، در دنیای هوش مصنوعی محور امروز، عدم بهره‌گیری از هوش مصنوعی در امنیت سایبری یک خودکشی دیجیتال محسوب می‌شود. سازمان‌های ایرانی نیز باید درک کنند که ابزارهای امنیتی دهه گذشته، برای مقابله با تهدیدات امروز کافی نیستند. چالش‌های پیش رو تنها با یک تغییر رویکرد اساسی قابل‌حل هستند. امنیت سایبری نیازمند یک انقلاب فناورانه است و اولین گام آن، پذیرش این واقعیت است که بدون هوش مصنوعی، آینده تاریک خواهد بود.
مارکو پریرا، رئیس جهانی امنیت سایبری، خدمات زیرساخت ابری موسسه تحقیقاتی **Cap Gemini** می‌گوید: ((سازمان ها باید برای پذیرش هوش مصنوعی زیرساخت‌های مدیریت داده‌ها، چارچوب‌ها و دستورالعمل‌های اخلاقی را ایجاد کنند و برنامه‌های آموزشی و آگاهی‌بخشی قوی برای کارکنان ایجاد کنند)).

منابع:

[1] https://www.capgemini.com/researchinstitute
[2] Nearly one-quarter (24%) of organizations have enabled Gen AI capabilities in some or most of their functions and locations – Cap Gemini Research Institute, "Harnessing the value of generative AI 2nd edition: Top use cases across sectors," July 2024.
[3] This involves using malicious inputs to manipulate AI and Gen AI models, compromising their integrity.
[4] 1,000 organizations across 12 sectors and 13 countries in Asia Pacific, Europe, and North America, with annual revenues of $1 billion and over.
[5] https://www.msn.com/en-us/news/technology/generative-ai-poses-new-threats-to-cybersecurity-cisos-report/ar-AA1nAL5X
[6] https://business-reporter.co.uk/2021/05/27/ai-enhancing-the-future-of-digital-transformation
[7]https://rastaksv.com/2022/03/30/%D9%87%D9%88%D8%B4/

یک اتاق سرور حرفه‌ای؛
ترکیب امنیت، کارایی و پایداری

صابر درس‌خوان
کارشناس ارشد شبکه
کارشناس مسئول زیرساخت

در حوزه فناوری اطلاعات، اتاق سرور به عنوان ستون فقرات زیرساخت دیجیتال یک سازمان عمل می‌کند. اتاق سرور یک فضای اختصاصی است که در آن سرورها و تجهیزات شبکه قرار می‌گیرند و طراحی و ویژگی‌های آن برای تضمین عملکرد بهینه، امنیت و قابلیت اطمینان بسیار مهم است. در این مطلب به معرفی و بررسی حداقل نیازهای یک اتاق سرور خواهیم پرداخت. بدیهیست موارد ذکر شده فقط بیانگر حداقل‌ها می باشد و در صورت نیاز می توان با مراجعه به منابع معتبر و نیز واحدهای بالادستی اتاق‌های سرور بهتر و مناسبتری طراحی و اجرا نمود.

۱. کنترل محیطی

یک اتاق سرور مناسب باید شرایط محیطی دقیقی را برای محافظت از تجهیزات حساس حفظ کند.مهمترین گزینه ها شامل موارد زیر است:

- تنظیم دما: دمای ایده‌آل برای عملکرد سرور معمولاً بین ۶۸ درجه فارنهایت و ۷۲ درجه فارنهایت (۲۰ درجه سانتیگراد تا ۲۲ درجه سانتیگراد) است. حفظ این محدوده به جلوگیری از گرمای بیش از حد که می‌تواند منجر به خرابی سخت‌افزار شود، کمک می‌کند.
- کنترل رطوبت: سطح رطوبت باید بین ۴۵% و ۵۵% نگه داشته شود تا از الکتریسیته ساکن و میعان جلوگیری شود، که هر دو می‌توانند به قطعات الکترونیکی آسیب برسانند.
- مدیریت جریان هوا: جریان هوای مناسب ضروری است. اتاق باید به گونه‌ای طراحی شود که گردش هوای بدون مانع را تسهیل کند، که اغلب از طریق کفپوش مرتفع یا دریچه‌های قرار داده شده در موقعیت استراتژیک (مثلا سقفی) حاصل می‌شود.

۲. امنیت فیزیکی

امنیت در اتاق سرور بسیار مهم است، زیرا داده‌ها و زیرساخت‌های حیاتی را در خود جای داده است. ویژگی‌های کلیدی امنیت فیزیکی عبارتند از:

- کنترل دسترسی: پیاده‌سازی کنترل‌های دسترسی دقیق، مانند سیستم‌های کارت کلید یا اسکنرهای بیومتریک، تضمین می‌کند که فقط پرسنل مجاز می‌توانند وارد اتاق سرور شوند.
- سیستم‌های نظارتی: نصب دوربین‌ها می‌تواند به نظارت بر فعالیت‌ها و جلوگیری از دسترسی غیرمجاز کمک کند.
- سیستم‌های اطفاء حریق: یک اتاق سرور مناسب باید به سیستم‌های اطفاء حریقی که از آب استفاده نمی‌کنند، مانند سیستم‌های مبتنی بر گاز، مجهز باشد تا از تجهیزات در برابر آسیب آتش‌سوزی محافظت کند.

۳. طراحی زیرساخت

طرح و طراحی فیزیکی اتاق سرور نقش مهمی در عملکرد آن ایفا می‌کند. ملاحظات مهم عبارتند از:
- تخصیص فضا: باید فضای کافی برای نصب تجهیزات، نگهداری و توسعه‌های آینده وجود داشته باشد. این گزینه شامل فضای قفسه‌ها، واحدهای خنک‌کننده و کابل‌کشی نیز می‌شود.
- مدیریت کابل: سیستم‌های مدیریت کابل مناسب به سازماندهی و ایمن‌سازی کابل‌ها، کاهش بی‌نظمی و بهبود جریان هوا کمک می‌کنند.
- عایق صدا: اقدامات عایق صدا می‌تواند نویز تجهیزات را به حداقل برساند و محیط کاری مناسب‌تری را برای پرسنل ایجاد کند.

۴. منبع تغذیه و پشتیبان

یک منبع تغذیه قابل اعتماد برای عملکرد سرور بسیار مهم است. ویژگی‌هایی که باید در نظر گرفته شوند عبارتند از:
- منبع تغذیه بدون وقفه (**UPS**): یک سیستم **UPS** در هنگام قطع برق، برق پشتیبان را فراهم می‌کند و تضمین می‌کند که سرورها عملیاتی باقی می‌مانند و داده‌ها از بین نمی‌روند.
- منابع تغذیه اضافی: داشتن چندین منبع تغذیه می‌تواند در صورت خرابی یک منبع، از خرابی جلوگیری کند.
- واحدهای توزیع برق (**PDU**): **PDU**ها به مدیریت توزیع برق به دستگاه‌های مختلف در اتاق سرور کمک می‌کنند و استفاده بهینه از برق را تضمین می‌کنند.

۵. سیستم‌های نظارت و مدیریت

سیستم‌های نظارت مؤثر برای حفظ شرایط بهینه در اتاق سرور ضروری هستند. این سیستم‌ها باید شامل موارد زیر باشند:
- نظارت محیطی: حسگرهایی که دما، رطوبت و جریان هوا را ردیابی می‌کنند، می‌توانند داده‌های بلادرنگ ارائه دهند و امکان پاسخ سریع به هرگونه مشکل را فراهم کنند.
- سیستم‌های هشدار: هشدارهای خودکار می‌توانند پرسنل را از هرگونه تغییر محیطی یا خرابی تجهیزات مطلع کنند و امکان اقدام سریع برای کاهش خطرات را فراهم کنند.
- ابزارهای مدیریت از راه دور: این ابزارها به کارکنان فناوری اطلاعات اجازه می‌دهند تا سرورها را از مکان‌های خارج از سایت نظارت و مدیریت کنند و بهره‌وری عملیاتی را افزایش دهند.

به طور خلاصه، یک اتاق سرور مناسب با توانایی آن در حفظ شرایط محیطی بهینه، تضمین امنیت فیزیکی، تأمین برق قابل اعتماد و تسهیل نظارت مؤثر مشخص می‌شود. با گنجاندن این ویژگی‌ها، سازمان‌ها می‌توانند از زیرساخت‌های حیاتی فناوری اطلاعات خود محافظت کنند و از عملکرد کارآمد و ایمن آن اطمینان حاصل کنند. طراحی و مدیریت دقیق یک اتاق سرور برای پشتیبانی از نیازهای فناوری هر سازمان مدرنی ضروری است.

دیجیتال توئین در سلامت: تحولی در مراقبت‌های پزشکی

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

کلمه دیجیتال توئین (**Digital Twin**) به معنای "دوقلوی دیجیتال" است. این اصطلاح از دو بخش تشکیل شده: دیجیتال که به دنیای دیجیتال و فناوری اشاره دارد، و توئین (**Twin**) که به معنای دوقلو یا نسخه‌ای مشابه است. در نتیجه، دیجیتال توئین به یک نسخه دیجیتال یا شبیه‌سازی مجازی از یک شیء، سیستم، فرآیند یا حتی یک انسان در دنیای واقعی اشاره دارد. این نسخه دیجیتال با استفاده از داده‌های واقعی ساخته می‌شود و رفتار، ویژگی‌ها و عملکرد شیء واقعی را در محیط مجازی بازسازی می‌کند. دیجیتال توئین (**Digital Twin**) به‌عنوان یکی از فناوری‌های نوظهور در حوزه سلامت، با ایجاد مدل‌های مجازی پویا از موجودیت‌های فیزیکی نظیر بیماران، اندام‌ها یا تجهیزات پزشکی، امکان ارائه مراقبت‌های دقیق‌تر و شخصی‌سازی‌شده را فراهم می‌کند. دیجیتال توئین یک مدل مجازی پویا است که با استفاده از فناوری‌های پیشرفته مثل اینترنت اشیا (**IoT**)، هوش مصنوعی (**AI**) و حسگرها، اطلاعات لحظه‌ای از یک شیء یا سیستم واقعی (مثل یک ماشین، ساختمان یا حتی بدن انسان) جمع‌آوری می‌کند و آن را در دنیای دیجیتال شبیه‌سازی می‌کند. این مدل مجازی به‌گونه‌ای طراحی شده که با تغییرات در دنیای واقعی به‌روز می‌شود و می‌تواند رفتار، وضعیت یا مشکلات احتمالی شیء واقعی را پیش‌بینی یا تحلیل کند. در حوزه درمان، دیجیتال توئین می‌تواند برای شبیه‌سازی بدن بیمار یا یک عضو خاص استفاده شود تا پزشکان بتوانند درمان را دقیق‌تر برنامه‌ریزی کنند.دیجیتال توئین مانند یک آینه دیجیتال است که رفتار و وضعیت یک شیء یا سیستم واقعی را نشان می‌دهد. می تواند، یک موجودیت فیزیکی مانند قلب بیمار یا تجهیزات پزشکی نظیر دستگاه **MRI** را بازنمایی می‌کند. این مدل با استفاده از داده‌های بلادرنگ (مانند نتایج آزمایش‌های پزشکی یا داده‌های سنسورهای پوشیدنی) به‌روز می‌شود و امکان پیش‌بینی وضعیت بیمار یا عملکرد تجهیزات را فراهم می‌کند. به‌عنوان مثال، دیجیتال توئین قلب بیمار می‌تواند، بدون نیاز به انجام آزمایش‌های واقعی اثرات یک دارو یا جراحی را پیش‌بینی کند،که این امر خطرات را کاهش می‌دهد.

اهداف دیجیتال توئین

هدف اصلی دیجیتال توئین ارتقای کیفیت مراقبت‌های پزشکی است. این فناوری به دنبال دستیابی به اهداف زیر است:

- تشخیص زودهنگام بیماری‌ها: شناسایی سریع بیماری‌ها برای بهبود نتایج درمانی.
- درمان‌های شخصی‌سازی‌شده: ارائه راهکارهای درمانی متناسب با ویژگی‌های منحصربه‌فرد هر بیمار.
- کاهش هزینه‌ها: بهینه‌سازی هزینه‌های درمان و نگهداری تجهیزات پزشکی.
- بهبود آموزش پزشکی: استفاده از شبیه‌سازی‌های واقعی برای آموزش پزشکان و دانشجویان.

این اهداف در راستای افزایش دقت، کاهش هزینه‌ها و دسترسی‌پذیری خدمات سلامت طراحی شده‌اند.

کاربردها و پتانسیل‌ها

دیجیتال توئین در حوزه سلامت کاربردهای متنوعی دارد که در جدول زیر خلاصه شده‌اند:

کاربرد	توضیح	پتانسیل
مدیریت بیماری‌های مزمن	شبیه‌سازی بیماری‌هایی مانند دیابت برای پیش‌بینی عوارض و مدیریت بهتر.	بهبود کیفیت زندگی و کاهش نیاز به بستری.
برنامه‌ریزی جراحی	شبیه‌سازی جراحی‌های پیچیده مانند قلب یا مغز برای بررسی گزینه‌های مختلف.	کاهش خطاها و افزایش نرخ موفقیت جراحی‌ها.
مدیریت تجهیزات پزشکی	پیش‌بینی خرابی دستگاه‌هایی مانند ونتیلاتور یا اسکنرها.	کاهش هزینه‌های تعمیر و افزایش کارایی تجهیزات.
پژوهش دارویی	آزمایش داروها روی مدل‌های مجازی به جای آزمایش‌های بالینی واقعی.	تسریع توسعه دارو و کاهش هزینه‌های پژوهشی.

این کاربردها در ایران، به‌ویژه برای بیماری‌های شایع مانند دیابت و بیماری‌های قلبی‌عروقی، پتانسیل بالایی دارند.

فرآیند پیاده‌سازی

پیاده‌سازی دیجیتال توئین شامل مراحل زیر است:

۱. جمع‌آوری داده‌ها: گردآوری داده‌های بلادرنگ از منابع مختلف مانند آزمایش‌های پزشکی، تصاویر تشخیصی یا سنسورهای **IoT**.
۲. ساخت مدل مجازی: استفاده از هوش مصنوعی و نرم‌افزارهای شبیه‌سازی برای ایجاد مدل دیجیتال.
۳. به‌روزرسانی و تحلیل: به‌روزرسانی مدل با داده‌های جدید و تحلیل برای تصمیم‌گیری‌های پزشکی.
۴. امنیت داده‌ها: حفاظت از داده‌ها با استفاده از رمزنگاری و پروتکل‌های امنیتی.

این فرآیند نیازمند زیرساخت‌های فناوری پیشرفته و آموزش تخصصی است.

نمونه‌های موفق جهانی

دیجیتال توئین در سطح جهانی دستاوردهای قابل‌توجهی داشته است:

- ایالات متحده: شرکت **Philips** با استفاده از دیجیتال توئین قلب (**HeartNavigator**) دقت جراحی‌های قلب را تا ۳۰ درصد افزایش داده است.
- آلمان: **Siemens Healthineers** با بهره‌گیری از دیجیتال توئین برای دستگاه‌های **MRI**، هزینه‌های تعمیر را تا ۲۰ درصد کاهش داده است.
- انگلستان: بیمارستان **Great Ormond Street** از دیجیتال توئین برای شبیه‌سازی جراحی‌های قلب کودکان استفاده می‌کند، که نتایج درمانی را بهبود بخشیده است.

مزایا و چالش‌ها

مزایای دیجیتال توئین شامل افزایش دقت تشخیص و درمان، کاهش هزینه‌ها و بهبود آموزش پزشکی است. بااین‌حال، چالش‌هایی مانند هزینه‌های اولیه بالا، نیاز به زیرساخت‌های ارتباطی پیشرفته (مانند اینترنت **5G**) و نگرانی‌های مرتبط با حریم خصوصی داده‌ها وجود دارد. در ایران، محدودیت دسترسی به اینترنت پرسرعت در مناطق روستایی می‌تواند مانع پیاده‌سازی این فناوری شود.

مسیر پیاده‌سازی در ایران

ایران با توجه به جمعیت جوان و پیشرفت زیرساخت‌های دیجیتال، ظرفیت بالایی برای بهره‌گیری از دیجیتال توئین دارد. پیشنهادات برای پیاده‌سازی عبارت‌اند از:

۱. آموزش تخصصی: برگزاری دوره‌های آموزشی در دانشگاه‌های علوم پزشکی.
۲. تمرکز بر اولویت‌ها: هدف‌گذاری روی بیماری‌های شایع مانند دیابت و بیماری‌های قلبی.
۳. توسعه زیرساخت‌ها: گسترش اینترنت ۵G و ایجاد پلتفرم‌های بومی.
۴. پروژه‌های آزمایشی: اجرای طرح‌های اولیه در بیمارستان‌های تخصصی مانند بیمارستان قلب شهید مدنی تبریز.
۵. تدوین قوانین: تنظیم استانداردهای حریم خصوصی و پوشش بیمه‌ای برای فناوری‌های دیجیتال توئین.

دیجیتال توئین با ایجاد مدل‌های مجازی دقیق از بیماران و تجهیزات پزشکی، پتانسیل تحول در نظام سلامت را دارد. تجربه‌های موفق جهانی نشان‌دهنده اثربخشی این فناوری است. در ایران، با رفع چالش‌های زیرساختی و سرمایه‌گذاری در پژوهش‌های بومی، می‌توان از این فناوری برای بهبود تشخیص، درمان و مدیریت منابع سلامت بهره برد. انجام مطالعات بومی برای ارزیابی اثربخشی دیجیتال توئین در نظام سلامت ایران ضروری است.

منابع:

1. Coorey, G., Figtree, G. A., Fletcher, D. F., & Redfern, J. (2021). The health digital twin: Advancing precision cardiovascular medicine through dynamic modelling and simulation. European Heart Journal - Digital Health, 2(4), 617-626. https://doi.org/10.1093/ehjdh/ztab087
2. Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital Twin: Enabling Technologies, Challenges and Open Research. IEEE Access, 8, 108952-108971. https://doi.org/10.1109/ACCESS.2020.2998358
3. Gartner. (2021). Top Strategic Technology Trends for 2022: Digital Twins. Gartner Research.
4. Liu, M., Fang, S., Dong, H., & Xu, C. (2021). Review of digital twin about concepts, technologies, and industrial applications. Journal of Manufacturing Systems, 58, 346-361. https://doi.org/10.1016/j.jmsy.2020.06.017
5. NHS. (2022). Great Ormond Street Hospital: Annual Report 2021-2022. National Health Service.
6. Philips. (2021). HeartNavigator: Enhancing Cardiac Interventions. Philips Healthcare.
7.Rasheed, A., San, O., & Kvamsdal, T. (2020). Digital Twin: Values, Challenges and Enablers From a Modeling Perspective. IEEE Access, 8, 21980-22012. https://doi.org/10.1109/ACCESS.2020.2970143
8. Siemens Healthineers. (2020). Digital Twin Technology in Medical Imaging. Siemens Healthineers.
9. World Health Organization. (2021). Digital Health: Opportunities and Challenges. WHO Report.

چت بات ها در خدمت سلامت

نرگس نجفی
دانشجوی کارشناسی فناوری اطلاعات سلامت

چت بات یک "برنامه کامپوتری شبیه سازی ارتباطی" است که برای تقلید از مکالمه انسان با انسان با تجزیه و تحلیل ورودی متنی کاربر و ارائه پاسخ های هوشمند و مرتبط طراحی شده است.چت بات ها به عنوان یکی از کاربرد های متعدد هوش مصنوعی،به عوامل گفت وگوی مجازی اشاره دارند که کاربران را قادر می سازند تا از طریق روش های شنیداری یا متنی با برنامه های کامپیوتری مبتنی بر هوش مصنوعی تعامل داشته باشند.

طیف گسترده ای از چت بات ها در بسیاری از حوزه ها وجود دارند که شامل کسب و کار،بازار سهام،مراقبت از مشتری،مشاوره،سرگرمی،روزنامه نگاری،چت بات های بانکی،مسافرتی،خرید آنلاین غذا و لوازم جانبی و نیز مراقب های بهداشتی میشود.معروف ترین چت بات ها مانند الکسا یا دستیار گوگل،بهترین نمونه هایی هستند که میتوان برای چت بات های ارتباطی هوشمند ارائه داد.اینها چت بات های عمومی هستند که خدماتی را برای همه ی حوزه ها ارائه میدهند و محدود به یک حوزه خاص نیستند.

همچنین چت بات های مختص حوزه نیز وجود دارند که قابلیت هایی را برای حوزه های ذکر شده در بالا ارائه میدهند. برخی از آنها به شرح زیر است: **Botsify** یک چت بات است که به توسعه دهندگان کمک میکند تا چت بات های هوشمند پیام رسان فیس بوک ایجاد کنند و برای جمع آوری اطلاعات از کاربران فیس بوک استفاده میشود. **Imperson** یک چت بات است که به توسعه دهندگان کمک میکند تا چت بات های تجاری ایجاد کنند و خدمات پشتیبانی از مشتری را ارائه میدهند. **NBC** یک چت بات است که به گویندگان خبر کمک میکند تا به سرعت در میان عناوین مهم حرکت کنند.

ورود چت بات ها به دنیای درمان

ارائه دهندگان خدمات مراقبت های بهداشتی همچنین به پذیرش فناوری های جدید برای بهبود خدمات خود علاقه مند هستند و شروع به پذیرش چت بات های پزشکی برای عملکردهایی مانند پاسخ دادن یا پرسیدن سوالات،ایجاد سوابق سلامت و سابقه استفاده،ارائه اطلاعات مربوط به بیماری ها،بحث در مورد نتایج آزمایشگاه های بالینی یا حتی انجام اقدامات مناسب براساس پاسخ های کاربران کرده اند.

چت بات های موجود زیادی برای حوزه مراقبت های بهداشتی وجود دارد که عملکردهای مختلفی را ارائه میدهند. **Endurance** یک چت بات است که با کاربرانی که از زوال عقل رنج میبرند سروکار دارد.**Casper** به افرادی که از بیخوابی رنج میبرند کمک میکند تا شب های خود را که به دلیل تنهایی بیخواب هستند سپری کنند.**Medwhat** یک چت بات پاسخ دهنده به سوالات متداول مراقبت های بهداشتی است و همچنین اطلاعاتی را در مورد بیماری های مختلف و علائم آن ارائه میدهد.

مزایای چت بات های پزشکی

مطالعات موجود اثربخشی چت بات های پزشکی را در کارهایی مانند اطمینان از پایبندی کافی به دارو گزارش کرده اند.مشاهده شده است که رضایت بیماران سرطانی پس از گفت و گو با یک چت بات بهبود یافته است.تعامل با یک چت بات همدل،تاثیر تسکین دهنده ای بر سلامت روان بیماران دارد.تعامل با چت بات های پزشکی علائم افسردگی و اضطراب را تسکین میدهد.با کمک چت بات های پزشکی میتوان حجم کار متخصصان مراقبت های بهداشتی را کاهش داد و ساده کرد.همانطور که برای مبارزه با بیماری همه گیر کووید_۱۹،چت بات های پزشکی بیش از ۹۶ درصد از بیماران آلوده را به طور دقیق شناسایی کردند.چت بات های پزشکی ممکن است نقش مهم دیگری در سلامت و رفاه داشته باشند. بسیاری از بیماری ها وجود دارند که به دلیل احساس انگ خوردن و یا خجالت افراد،کمتر تشخیص داده میشوند و درمان نمیشوند.وقتی افراد در پاسخ به افشای علائم خود،انگ یا شرمساری پیش بینی میکنند،به اشتراک گذاشتن اطلاعات و بحث آشکار در مورد سلامت خود با متخصصان پزشکی میتواند دشوار باشد.بسیاری از افراد ممکن است،فرصت درمان زود هنگام را از دست بدهند که منجر به کاهش قابل توجه سلامت و تندرستی میشود.چت بات های پزشکی میتوانند مشاوره اولیه قابل دسترس تری را برای کاربران فراهم کنند و برای تشویق کاربران به صحبت در مورد علائم خود در یک محیط آرام استفاده شوند که میتوان به عنوان «اولین قدم» مثبت برای کمک به آنها در مسیرسلامتشان عمل کند. چت بات ها همچنین میتوانند پس از تشخیص اولیه مفید باشند و برای کمک به افراد در مدیریت سلامت طولانی مدت خود استفاده شوند.پیش بینی میشود که در آینده،بیماران این توانایی را خواهند داشت که سوابق اطلاعات مراقبت های بهداشتی خود را با چت بات های پزشکی به اشتراک بگذارند

تا به بهبود بیشتر کاربرد و دقت آنها کمک کنند.

آینده ای هوشمند اما نه بی چالش!

با وجود همه ی این ویژگی های امیدوارکننده،چت بات های پزشکی هنوز با چالش های متعددی روبه رو هستند و مطالعات مختلف در منابع موجود نشان میدهند که فضای زیادی برای مطالعات بیشتر در زمینه چت بات های پزشکی وجود دارد.
چت بات های پزشکی معمولا برپایه الگوریتم های ازپیش تعریف شده و داده های آموزشی عمل میکنندکه این ساختار باعث میشود در مواجهه با موارد پیچیده،چندوجهی و نادر پزشکی،توانایی تحلیل و تصمیم گیری آنها محدود باشد.برخلاف پزشکان انسانی که میتوانند با تکیه بر شهود،تجربه و بررسی چند جانبه در چنین موضع هایی به نتیجه برسند،چت بات ها ممکن است پاسخ های سطحی یا حتی نادرستی ارائه دهند.
چت بات ها به رغم تلاش برای شبیه سازی زبان انسانی، فاقد توانایی واقعی در درک احساسات،اضطراب یا نگرانی های بیمار هستند.این ضعف میتواند منجر به کاهش رضایت بیماران و احساس بی توجهی در تعامل با سیتم های هوشمند شود.
دسترسی به اطلاعات حساس بیماران برای عملکرد صحیح چت بات های پزشکی،چالش های جدی در زمینه امنیت داده ها و حفظ حریم خصوصی ایجاد میکند.در صورت نفوذ یا سواستفاده از این اطلاعات،پیامد های حقوقی و اخلاقی سنگینی متوجه سیستم های درمانی خواهد شد.
بسیاری ازمراکز درمانی هنوز از سیستم های سنتی یا نیمه دیجیتال استفاده میکنند که این عمر ادغام چت بات های پزشکی با این زیرساخت ها را دچار چالش هایی از قبیل نیاز به هزینه،آموزش و باز طراحی فرایند ها میکند.از سوی دیگر اتکای بیش از حد به هوش مصنوعی ممکن اسن منجر به حذف نقش پزشک در فرایند های حیاتی و تضعیف مسئولیت پذیری شود.
در مجموع چت بات های پزشکی اگرچه نوید بخش تحول در ارائه خدمات سلامت هستند اما بدون توجه به چالش های فوق ممکن است به جای تسهیل درمان،موجب اختلال آن شوند.توسعه این فناوری ها باید با رویکردی اخلاق محور،انسان محور و مبتنی برنظارت دقیق همراه باشد تا بتوان از ظرفیت های آن ها به صورت ایمن و موثر بهره برداری کرد.

چت بات های درمان گر؛چشم انداز آینده و ضرورت نگاه انتقادی

از نظر آماری،روند رشد بازار جهانی چت بات های سلامت بسیار چشمگیر است.طبق مقاله **Makebot.ai** ،ارزش این بازار از ۲.۱۵ میلیارد دلار در سال ۲۰۲۵ به ۱۷.۷۴ میلیارد دلار تا سال ۲۰۳۵ خواهد رسید_نشان دهنده رشد بیش از ۷ برابر در یک دهه_که این رشد عمدتا ناشی از پیشرفت در فناوری های پردازش زبان طبیعی (**NLP**) ، یادگیری ماشین و افزایش تقاضا برای خدمات سلامت دیجیتال است.چت بات های پزشکی نه تنها ابزاری برای تسهیل ارتباط بیمار و پزشک هستند، بلکه به عنوان بخشی از زیرساخت آینده ی سلامت دیجیتال، نقش کلیدی در شخصی سازی مراقبت،کاهش هزینه ها و افزایش بهره وری ایفا خواهند کرد.موفقیت این مسیر نیازمند تعامل میان فناوری ، اخلاق پزشکی و سیاست گذاری هوشمندانه برای تحقق پتانسیل کامل چت بات های پزشکی میباشد.

منابع:

1. https://doi.org/10.1016/j.ijmedinf.2022.104827
2. https://www.viit.ac.in/images/Quality/NAAC/NAAC-Data/Criteria-3/Research-Journal-Paper/JP-AY-2019-20-PART-1.pdf
3. https://softteco.com/blog/chatbots-in-healthcare
4. https://www.makebot.ai/blog-en/future-of-chatbots-in-healthcare-innovations-and-patient-care-transformation

چالش‌های اخلاقی و امنیتی استفاده از هوش مصنوعی در داده‌های سلامت در ایران

رقیه سیدنژاد
کارشناس ارشد مهندسی نرم افزار
مدیر وب‌سایت مدیریت اطلاع‌رسانی پزشکی و منابع علمی

مقدمه

فناوری هوش مصنوعی (AI) در حوزه سلامت در حال تحول است؛ از تشخیص تصویری تا تصمیم‌گیری بالینی و تحلیل داده‌ها. در عین حال، داده‌های سلامت جزو حساس‌ترین اطلاعات فردی محسوب می‌شوند و حفاظت ناکافی از آن‌ها می‌تواند پیامدهای اجتماعی، اقتصادی و امنیتی عمیقی در پی داشته باشد . با دیجیتالی شدن نظام سلامت ایران-در قالب پرونده الکترونیک سلامت(مانند سپاس)، نسخه‌نویسی الکترونیک، و سامانه‌های بیمه‌ای- حجم عظیمی از داده‌های پزشکی تولید و پردازش می‌شود. در این زمینه، استفاده از AI فرصت‌هایی برای بهبود سلامت فراهم می‌آورد؛ اما مخاطرات اخلاقی و امنیتی جدی‌ای نیز به همراه دارد.

اهمیت داده‌های سلامت در ایران

سامانه‌هایی مانند سپاس و دیگر سامانه‌های الکترونیک در ایران موجب جمع‌آوری داده‌های متعدد مانند سوابق بیماری، تصاویر پزشکی و نوع درمان شده‌اند. این داده‌ها به‌عنوان دارایی ملی برای تحقیقات پزشکی و توسعه هوش مصنوعی ارزشمندند، اما در صورت سوءاستفاده، می‌توانند محرمانگی افراد را به خطر اندازند.

چالش‌های اخلاقی استفاده از AI در داده‌های سلامت

۱. حریم خصوصی و کنترل داده‌ها: نگرانی‌هایی درباره امکان خنثی شدن ناشناس‌سازی یا ردیابی مجدد افراد از طریق داده‌های AI مطرح است.
۲. رضایت آگاهانه و شفافیت: استفاده از داده‌ها بدون اطلاع صریح بیماران چالش‌های حقوقی و اخلاقی مهمی را ایجاد می‌کند.
۳. اصول اخلاق پزشکی: استقلال تصمیم‌گیرنده، انصاف، جلوگیری از آسیب و ارتقای خیر عمومی باید لحاظ شود.
۴. سوگیری و تبعیض الگوریتمی: آموزش بر داده‌های غیرنماینده می‌تواند نتایج تبعیض‌آمیز ایجاد کند.
۵. مسئولیت و پاسخگویی: تعیین مسئولیت در خطاهای AI هنوز مشخص نیست.
۶. چالش‌های امنیتی استفاده از AI در داده‌های سلامت
۱.حملات سایبری و نشت داده‌ها: حملات باج‌افزاری مراکز درمانی را تهدید می‌کند.
۲.فقدان چارچوب قانونی جامع: قوانین ایران پراکنده و ناکافی هستند.
۳.وابستگی به فناوری‌های خارجی: اعتماد به زیرساخت‌های خارجی تهدید امنیت ملی است.
۴.تهدیدهای نوظهور: مدل‌های AI خود می‌توانند آلوده یا آسیب‌پذیر باشند.

وضعیت قوانین و سیاست‌ها در ایران

قوانین فعلی ایران در حوزه حفاظت از داده شخصی شامل قانون تجارت الکترونیک و قانون جرایم رایانه‌ای هستند اما چارچوب یکپارچه و مشخصی برای استفاده از داده‌های سلامت در AI وجود ندارد. در مقابل، قوانین بین‌المللی مانند GDPR اروپا و HIPAA آمریکا چارچوب‌های دقیقی دارند.

راهکارهای پیشنهادی

- تدوین چارچوب اخلاقی-حقوقی ملی
- بومی‌سازی تکنولوژی و داده‌ها
- استفاده از فناوری‌های حفظ حریم خصوصی مانند یادگیری فدرال
- تقویت زیرساخت‌های امنیتی در مراکز درمانی
- ایجاد کمیته‌های اخلاق داده
- آموزش و فرهنگ‌سازی پزشکان و مدیران

جمع‌بندی

هوش مصنوعی می‌تواند تحولات شگرفی در نظام سلامت ایران ایجاد کند؛ اما این پیشرفت اگر بدون توجه به اخلاق و امنیت انجام شود، می‌تواند منجر به کاهش اعتماد عمومی و آسیب جدی به بیماران شود.

منابع:

1. Morley J, Machado CCV, Burr C, Cowls J, Joshi I, Taddeo M, Floridi L. The ethics of AI in health care: A mapping review. BMC Med Ethics. 2020;21(1):14.
2. Beauchamp TL, Childress JF. Principles of biomedical ethics. Oxford University Press; 2019.
3. European Union. General Data Protection Regulation (GDPR). Official Journal of the European Union. 2016.
4. U.S. Department of Health & Human Services. Health Insurance Portability and Accountability Act of 1996 (HIPAA).
5. Abbasgholizadeh Rahimi S, L é gar é F, Sharma G, et al. Application of artificial intelligence in primary health care: A scoping review. Int J Med Inform. 2021;149:104414.

۶. وزارت بهداشت، درمان و آموزش پزشکی ایران. سامانه پرونده الکترونیک سلامت (سپاس)
۷. قانون جرائم رایانه‌ای جمهوری اسلامی ایران (۱۳۸۸)

8. Generis Online. Understanding Data Protection and Privacy Laws in Iran. 2023.
9. Shamsi A, Asghari H, Kiani M. Ethical challenges of artificial intelligence in healthcare: A focus on Iran. Iranian Journal of Medical Ethics. 2021;14(2):45-56.

10. Xu J, Glicksberg BS, Su C, Walker P, Bian J, Wang F. Federated learning for healthcare informatics. arXiv preprint arXiv:2007.11621. 2020.

دل نوشت

برای خوانندگان پالسی نو

سید محمدحسن الهی

کارکنان خاموش واحد IT

در تشکیلات عظیم دانشگاه ما، هر بخش و واحد با نتیجه کار خود قابل مشاهده است مثلا کارگزینی را به صدور حکم می بینند و امور مالی را به پرداخت ها و حقوق و دستمزد و ... به جز یک واحد.

بخش فناوری اطلاعات نه در صحنه عملیات روزانه قرار دارد و نه به دنبال تشویق برای کاری که انجام می دهد. این بخش همواره در پس‌زمینه وجود دارد و بی‌سروصدا وزنی بزرگ و مسئولیتی سنگین را حمل می‌کند که کمتر کسی آن را تشخیص می‌دهد، اما همه به آن وابسته هستند.

برای کارکنان فناوری اطلاعات، هر روز کاری یک فعالیت بین دقت و فشار کاری است. پیروزی‌های آنها به ندرت جشن گرفته می‌شود، زیرا در سکوت سنجیده می‌شوند و نتایج آن را دیگر واحدها استفاده می کنند: سیستمی که از کار نمی‌افتد، سروری که متزلزل نمی‌شود، شبکه‌ای که فرو نمی‌ریزد.

کارکنان فناوری اطلاعات نه به خاطر ساعت‌های بی‌شماری که صرف جلوگیری از مشکلات کرده‌اند، بلکه فقط برای لحظاتی که مشکلی پیش می‌آید، به یاد آورده می‌شوند. زمانی که واحدی دیگر نمی تواند فعالیت های خود را به درستی انجام دهد، آن وقت زمانی است که همه به یاد می آورند واحدی هم در دانشگاه وجود دارد که نام آن فناوری اطلاعات است.

و اما با این حال...

پشت تمام آن فعالیت‌ها در واحد فناوری اطلاعات، انسانها - نه ماشین‌ها - نشسته اند. کارشناسانی که مدت‌ها پس از اتمام فعالیت دیگران، در واحد خود هستند تا نوار موفقیت عملکرد دیگران قطع نشود.

افرادی که در لحظات شکست، بار انتظارات کل سازمان را بر دوش خود حمل می‌کنند. افرادی که گاهی اوقات احساس می‌کنند دیده نمی‌شوند، زیرا کارشان زمانی که نامرئی است، موفق‌تر است.

چالش‌های آنها صرفاً فنی نیست. آنها با وقفه‌های مداوم، با فشار مطالبات فوری، با خستگی ناشی از دانستن اینکه خدمتشان مورد انتظار است اما همیشه درک نمی‌شود، زندگی و کار می‌کنند.

با وجود این، آنها همواره ادامه می‌دهند؛ زیرا می‌دانند که بدون هوشیاری آنها، ضربان قلب سازمان، پالس سازمان متزلزل می‌شود.

شاید زمان آن رسیده باشد که همه ما، به عنوان همکار سازمانی، اندکی مکث کنیم و بیندیشیم. نه تنها سیستم‌هایی را که آنها حفظ می‌کنند، بلکه فداکاری‌هایی را که انجام می‌دهند را نیز ببینیم. درک کنیم که کار آنها فقط در ماشین‌ها و کدها نیست، بلکه در صبر، استقامت و حس عمیق وظیفه‌شناسی است.

بخش فناوری اطلاعات صرفاً تیمی از کارشناس‌ها نیست. این واحد قدرت نامرئی دانشگاه ماست.

بدون شک فناوری اطلاعات، پالسی نو است.

بیست انتظار اصلی از پرسنل دانشگاه در حوزه امنیت اطلاعات

جواد فرهادی
کارشناس ارشد نرم افزار

در عصری که اطلاعات به عنوان شریان حیاتی هر نهادی جریان دارد، مسئولیت حفاظت از آن نمی‌تواند صرفاً بر عهده فناوری یا بخش‌های تخصصی باشد. امنیت واقعی محصول هوشیاری جمعی است، جایی که هر عضو یک سازمان نقشی ایفا می‌کند. برای حفظ محرمانگی، یکپارچگی و در دسترس بودن، باید همه پرسنل اصول خاصی را رعایت کنند. این اصول را می‌توان در بیست انتظار اصلی خلاصه کرد که هر کدام برای تاب‌آوری سازمان در زمان‌های بحرانی لازم و حیاتی هستند.

۱. پایبندی به سیاست‌های امنیتی

از پرسنل انتظار می‌رود که با سیاست‌های امنیتی تعیین‌شده توسط دانشگاه کاملاً آشنا باشند و بدون استثنا از آنها پیروی کنند. سیاست‌ها نه به عنوان محدودیت، بلکه به عنوان سپرهای محافظ وجود دارند و تضمین می‌کنند که اقدامات هر کارمند با استراتژی امنیتی گسترده‌تر همسو باشد. هنگامی که سیاست‌ها نادیده گرفته می‌شوند، کل ساختار سازمانی آسیب‌پذیر می‌شود.

۲. شیوه‌های قوی رمز عبور

رمز عبور اغلب اولین خط دفاعی است. از همکاران انتظار می‌رود رمزهای عبور پیچیده و منحصر به فردی ایجاد کنند و از سادگی که مهاجمان به راحتی از آن سوءاستفاده می‌کنند، اجتناب کنند. آنها همچنین باید از نوشتن رمزهای عبور یا به اشتراک گذاشتن آنها با همکاران دیگر خودداری کنند، زیرا حتی کوچکترین خطا می‌تواند دروازه‌ها را برای نفوذ باز کند.

۳. استفاده از احراز هویت چند عاملی در سامانه های مورد لزوم

فراتر از رمزهای عبور، لایه‌های اضافی محافظتی مانند کدهای یکبار مصرف، توکن‌ها یا بررسی‌های بیومتریک، محافظت‌های حیاتی بیشتر را فراهم می‌کنند. از کارمندان انتظار می‌رود که این اقدامات را بپذیرند و درک کنند که اگرچه ممکن است کمی دردسر ایجاد کنند، اما به طور قابل توجهی دفاع در برابر دسترسی غیرمجاز را تقویت می‌کنند.

۴. محرمانگی اطلاعات

پرسنل باید اطلاعات حساس را به عنوان یک امانت تلقی کنند. اسناد، ارتباطات و سوابق نباید به طور اتفاقی فاش شوند یا بدون مراقبت رها شوند. محرمانگی نه تنها موضوع رعایت قوانین است، بلکه به صداقت و احترام به همکاران، بیماران یا مشتریانی که اطلاعات آنها به دانشگاه سپرده شده است نیز مربوط می‌شود.

۵. هوشیاری در مورد ایمیل

ایمیل همچنان یکی از رایج‌ترین مسیرهای حمله است. از کارمندان انتظار می‌رود که با احتیاط، به لینک‌ها یا پیوست‌های ناآشنا

اعتماد نکنند و قبل از پاسخ دادن به پیام‌های مشکوک مکث کنند. با برخوردی سالم و شکاکانه با هر ایمیل، پرسنل می‌توانند از گسترش تهدیدات در دانشگاه جلوگیری کنند.

۶. استفاده ایمن از اینترنت

گشت و گذار بی‌دقت در وب، خطرات فراوان را به همراه دارد. از پرسنل انتظار می‌رود از سایت‌های غیرقابل اعتماد دوری کنند، از دانلود مطالب غیرمجاز خودداری کنند و هنگام استفاده از سرویس‌های آنلاین خارجی احتیاط کنند. رفتار دیجیتال مسئولانه، یکپارچگی سازمان را حفظ کرده و از نفوذ نرم‌افزارهای مخرب جلوگیری می‌کند.

۷. نحوه صحیح استفاده از دستگاه‌ها

لپ‌تاپ‌ها، تلفن‌های همراه و درایوهای قابل حمل، داده‌های حساسی را حمل می‌کنند و باید با همان دقتی که با اسناد طبقه‌بندی شده رفتار می‌شود، با آنها رفتار شود. انتظار می‌رود دستگاه‌های خود را با رمز عبور یا رمزگذاری ایمن کنند، از رها کردن آنها بدون مراقبت خودداری کنند و در خارج از محل کار با احتیاط با آنها کار کنند.

۸. به‌روزرسانی‌های به موقع

آسیب‌پذیری‌های نرم‌افزاری روزانه کشف می‌شوند و وصله‌هایی برای رفع آنها صادر می‌شود. پرسنل باید با تیم‌های فناوری اطلاعات همکاری کنند تا اطمینان حاصل شود که سیستم‌ها، برنامه‌ها و دستگاه‌ها به سرعت به‌روزرسانی می‌شوند. تأخیر در به‌روزرسانی ممکن است کل شبکه را در معرض سوءاستفاده قرار دهد.

۹. آگاهی از پشتیبان‌گیری از داده‌ها

هر عضو دانشگاه نقشی منحصر بفرد در حفظ داده‌ها دارد. چه از طریق ذخیره کار در سیستم‌های تأیید شده و چه با رعایت برنامه‌های پشتیبان‌گیری، پرسنل باید درک کنند که پشتیبان‌گیری‌ها از خطاهای انسانی و فاجعه جلوگیری می‌کنند. داده‌هایی که از دست می‌روند ممکن است هرگز بازیابی نشوند.

۱۰. گزارش فعالیت‌های مشکوک

از تمامی همکاران انتظار می‌رود که به عنوان چشم و گوش امنیت عمل کنند. هر رویداد غیرعادی - یک ایمیل غیرمعمول، یک سیستم معیوب یا رفتار مشکوک - باید فوراً گزارش شود. سکوت یا تردید ممکن است باعث شود یک حادثه کوچک به یک بحران کامل تبدیل شود.

۱۱. فقط استفاده از نرم‌افزارهای مجاز

نرم‌افزار غیرمجاز، حتی اگر به ظاهر بی‌ضرر باشد، ممکن است حاوی تهدیدات پنهان باشد. پرسنل هرگز نباید برنامه‌هایی را که توسط سازمان تأیید نشده‌اند نصب یا استفاده کنند. ابزارهای مجاز از نظر امنیتی بررسی می‌شوند؛ ابزارهای غیرمجاز کل زیرساخت را در معرض خطر قرار می‌دهند.

۱۲. احترام به کنترل‌های دسترسی

مجوزهای دسترسی با دقت طراحی شده‌اند تا افشای داده‌های حساس را محدود کنند. از همکاران انتظار می‌رود که به این مرزها

احترام بگذارند و فقط به اطلاعات لازم برای نقش خود دسترسی داشته باشند. درخواست یا اعطای دسترسی غیرضروری، هم نقض اعتماد و هم تهدیدی برای امنیت است.

۱۳. محافظت در برابر مهندسی اجتماعی

همه حملات به شکل کد نیستند. بسیاری از آنها از طریق ترغیب و فریب انجام می‌شوند. از همکاران انتظار می‌رود که در برابر تلاش‌های دستکاری، چه از طریق تلفن، ایمیل یا حتی حضوری، هوشیار باشند. آگاهی و شک و تردید قوی‌ترین دفاع آنها است.

۱۴. مراقبت در فضاهای عمومی

کار اغلب فراتر از دیوارهای دفتر است. کارمندان باید در مکان‌های عمومی احتیاط کنند مشارکت در بحث‌های بلند در مورد موضوعات حساس، محافظت از صفحه نمایش لپ‌تاپ از چشمان کنجکاو و هرگز در معرض دید قرار ندادن اسناد. دنیای بیرون نباید به دریچه‌ای به اسرار سازمان تبدیل شود.

۱۵. دفع ایمن اطلاعات

اطلاعات دیجیتال و فیزیکی باید مسئولانه دور ریخته شوند. اسناد چاپی باید خرد شوند، در حالی که ذخیره‌سازهای دیجیتال باید قبل از دفع به طور ایمن پاک شود. بی‌احتیاطی در استفاده از مواد منسوخ می‌تواند منجر به نقض‌های شدید شود.

۱۶. آگاهی از مسئولیت شخصی

هر کارمند باید تشخیص دهد که امنیت اطلاعات وظیفه شخص دیگری نیست. هر کلیک، هر ورود به سیستم، هر تصمیمی عواقبی دارد. از پرسنل انتظار می‌رود که خود را به عنوان نگهبانان فعال ببینند و درک کنند که امنیت از خود فرد شروع می‌شود.

۱۷. احترام به استانداردهای قانونی و اخلاقی

امنیت اطلاعات به صورت جداگانه وجود ندارد. این امر به قوانین، مقررات و ضوابط اخلاقی وابسته است. پرسنل باید همیشه در این چارچوب‌ها عمل کنند و به یاد داشته باشند که رعایت آنها اختیاری نیست، بلکه برای صداقت حرفه‌ای اساسی است.

۱۸. مشارکت در آموزش امنیت

دانش بزرگترین دفاع در برابر تهدیدهای در حال تحول است. از کارمندان انتظار می‌رود در جلسات آگاهی‌بخشی امنیتی شرکت کنند، فعالانه مشارکت کنند و درس‌های آموخته شده را به کار گیرند. آموزش بار اضافی نیست، بلکه سپری است که کارکنان را برای چالش‌هایی که ممکن است روزی با آن مواجه شوند، مجهز می‌کند.

۱۹. آمادگی برای شرایط اضطراری

هنگام بروز بحران، هر ثانیه اهمیت دارد. پرسنل باید با پروتکل‌های واکنش، چه برای حملات سایبری، نقض داده‌ها یا بلایای طبیعی، آشنا باشند. آمادگی تضمین می‌کند که هنگام وقوع غیرمنتظره، وحشت جایگزین رویه نشود.

۲۰. تعهد به هوشیاری مداوم

بالاتر از همه، از کارمندان انتظار می‌رود هوشیار بمانند. تهدیدها روزانه در حال تکامل هستند و بی‌خیالی بزرگترین دشمن امنیت است. پرسنل با حفظ آگاهی، نظم و تعهد، نه تنها سیستم‌های دانشگاه، بلکه اعتبار، اعتماد و ماموریت آن را نیز حفظ می‌کنند.

این بیست انتظار تنها در تئوری وجود ندارند؛ آنها فرهنگ زنده امنیت اطلاعات را تشکیل می‌دهند. هر کارمند، از جدیدترین کارمند گرفته تا بالاترین مقام اجرایی، در دفاع از موسسه مشارکت دارد. وقتی این انتظارات برآورده شود، سازمان مقاوم می‌ماند، از داده‌های آن محافظت می‌شود و اعتماد آن خدشه‌دار نمی‌شود. در حوزه امنیت، فناوری ممکن است چارچوب باشد - اما کاربران پایه و اساس هستند.

سلامت دیجیتال؛ افق نوین در تحول نظام سلامت

الهام منقش
دانشجوی دکتری تخصصی مدیریت اطلاعات سلامت اطلاعات

در دهه اخیر، همگرایی فناوری اطلاعات و علوم پزشکی، مفهوم «سلامت دیجیتال» را از یک ایده نوظهور به یک ضرورت استراتژیک بدل کرده است. از پرونده الکترونیک سلامت تا هوش مصنوعی در تشخیص بیماری‌ها، هر روز شاهد نفوذ عمیق فناوری در فرآیندهای بهداشت و درمان هستیم. سلامت دیجیتال تنها یک ابزار فناورانه نیست؛ بلکه یک پارادایم تحول‌آفرین است که می‌تواند عدالت در دسترسی، کیفیت خدمات و بهره‌وری نظام سلامت را متحول سازد. با این حال، تحقق این چشم‌انداز در بستر بومی کشور، نیازمند آمادگی زیرساختی، سرمایه انسانی توانمند و چارچوب‌های حقوقی و اخلاقی شفاف است. این مقاله با رویکرد تحلیلی، به بررسی ابعاد کلیدی سلامت دیجیتال و الزامات موفقیت آن در نظام سلامت ایران می‌پردازد.

زیرساخت و حکمرانی داده

پایه هر سیستم سلامت دیجیتال موفق، حکمرانی داده است. این شامل ایجاد استانداردهای تبادل داده، پلتفرم‌های امن ذخیره‌سازی و الگوریتم‌های تحلیلی برای استخراج دانش از کلان‌داده‌های سلامت می‌شود. تجربه جهانی نشان می‌دهد که بدون معماری یکپارچه اطلاعات، پروژه‌های سلامت دیجیتال به پراکندگی و موازی‌کاری دچار خواهند شد. بنابراین، ایجاد «پایگاه ملی داده‌های سلامت» می‌تواند گام مهمی برای هم‌افزایی میان بیمارستان‌ها، مراکز پژوهشی و سیاست‌گذاران باشد.

امنیت سایبری؛ خط مقدم اعتماد عمومی

بخش سلامت یکی از اهداف اصلی حملات سایبری است. حفاظت از داده‌های بیماران و استمرار خدمات درمانی نیازمند استراتژی‌های امنیتی چندلایه، ارزیابی منظم آسیب‌پذیری‌ها و آموزش مداوم کارکنان است. حملات باج‌افزاری، فیشینگ و تهدیدات داخلی از جمله خطرات رایج هستند که باید با آمادگی سازمانی پاسخ داده شوند. تجربه کشورهایی که دچار اختلالات سایبری در بیمارستان‌ها شده‌اند نشان می‌دهد که غفلت در این حوزه می‌تواند حتی جان بیماران را به خطر بیندازد.

هوش مصنوعی و پزشکی دقیق

از تحلیل تصاویر پزشکی تا پیش‌بینی سیر بیماری، هوش مصنوعی در حال تغییر رویکردهای تشخیصی و درمانی است. برای بهره‌برداری مؤثر از این فناوری، علاوه بر الگوریتم‌های بومی‌سازی‌شده، نیاز به چارچوب‌های اخلاقی و نظارتی قوی برای جلوگیری از سوگیری و حفظ حریم خصوصی وجود دارد. هوش مصنوعی همچنین می‌تواند به «پزشکی دقیق» کمک کند؛ جایی که درمان‌ها بر اساس ویژگی‌های ژنتیکی، سبک زندگی و محیط فرد شخصی‌سازی می‌شوند. این رویکرد می‌تواند نتایج درمانی را به شکل چشمگیری بهبود بخشد.

اینترنت اشیای پزشکی (IoMT)

یکی از روندهای نوظهور، گسترش دستگاه‌های پوشیدنی و حسگرهای متصل به اینترنت است که داده‌های حیاتی بیمار را در لحظه ثبت و به پزشک منتقل می‌کنند. ساعت‌های هوشمند، مانیتورهای قند خون و دستگاه‌های کنترل ضربان قلب، نمونه‌هایی از این فناوری‌اند. در ایران، استفاده گسترده از چنین ابزارهایی می‌تواند بار مراجعات غیرضروری به مراکز درمانی را کاهش دهد و مدیریت بیماری‌های مزمن مانند دیابت و فشار خون را بهبود بخشد.

تله‌مدیسین و دسترسی عادلانه

مشاوره پزشکی از راه دور یا تله‌مدیسین، یکی از کاربردهای پررنگ سلامت دیجیتال است. این فناوری امکان ارائه خدمات پزشکی به مناطق محروم و دورافتاده را فراهم می‌سازد و می‌تواند نابرابری در دسترسی به خدمات درمانی را کاهش دهد. البته موفقیت این حوزه در ایران نیازمند توسعه زیرساخت اینترنت پرسرعت و فرهنگ‌سازی میان پزشکان و بیماران است.

چالش‌ها و ملاحظات بومی

در ایران، محدودیت منابع مالی، پراکندگی سیستم‌های اطلاعاتی و مقاومت فرهنگی در برابر تغییر، موانع اصلی پیاده‌سازی سلامت دیجیتال هستند. غلبه بر این موانع مستلزم ترکیب اقدامات فنی (ارتقای زیرساخت) و اجتماعی (آموزش و فرهنگ‌سازی) است. همچنین، قوانین روشن در زمینه مالکیت داده‌ها، مسئولیت‌پذیری در خطاها و تضمین حفظ حریم خصوصی بیماران از الزامات حیاتی محسوب می‌شود.

آینده سلامت دیجیتال در ایران

چشم‌انداز آینده نشان می‌دهد که سلامت دیجیتال تنها به یک ابزار کمکی محدود نخواهد ماند، بلکه به هسته اصلی نظام سلامت تبدیل خواهد شد. آموزش دانشگاهی در حوزه انفورماتیک پزشکی، سرمایه‌گذاری در استارتاپ‌های سلامت دیجیتال و همکاری میان وزارت بهداشت و بخش خصوصی می‌تواند این آینده را تسریع کند.

نتیجه‌گیری

سلامت دیجیتال فرصتی تاریخی برای بهبود کیفیت، کارایی و عدالت در نظام سلامت کشور فراهم می‌آورد. اما تحقق این فرصت نیازمند رویکردی جامع است که از سطح سیاست‌گذاری تا اجرای عملیاتی، بر مبنای داده و شواهد علمی پیش رود. همان‌طور که قلب تپنده نظام سلامت، داده‌های دقیق و قابل‌اعتماد هستند، امنیت و یکپارچگی این داده‌ها شرط بقای این زیست‌بوم دیجیتال است. آینده سلامت ایران در گرو آن است که فناوری نه به عنوان ابزاری تزئینی، بلکه به عنوان موتور محرک تحول درک و پیاده‌سازی شود.

آموزش تبدیل گفتار به نوشتار در GOOGLE DOCS

سمیه کرد
کارشناس ارشد مهندسی مواد گرایش شناسایی
کارشناس تحلیل‌گر سیستم معاونت آموزشی

مقدمه

در دنیای امروز که سرعت و دقت در انتقال اطلاعات حرف اول را می‌زند، استفاده از تکنولوژی‌هایی مانند تبدیل گفتار به نوشتار نه‌تنها یک گزینه، بلکه یک ضرورت است. این ابزارها به کاربران کمک می‌کنند تا از زمان خود بهینه‌تر استفاده کنند، خطاها را کاهش دهند، و در نهایت، بهره‌وری خود را افزایش دهند. یکی از ابزارهای قدرتمند در این زمینه، قابلیت تبدیل گفتار به نوشتار **Speech-to-Text** در **Google Docs** است. این تکنولوژی به کاربران این امکان را می‌دهد تا به سادگی و با استفاده از میکروفون دستگاه خود، گفتار را به متن تبدیل کنند. این ویژگی نه‌تنها در صرفه‌جویی زمان مؤثر است، بلکه برای افرادی که در تایپ مهارت ندارند یا به دلایلی نمی‌توانند از صفحه‌کلید استفاده کنند، یک راه‌حل ایده‌آل محسوب می‌شود.

همچنین این قابلیت می‌تواند به نویسندگان، روزنامه‌نگاران و محققان کمک کند تا ایده‌ها و مطالب خود را به سرعت و با کمترین خطا ثبت کنند و همچنین، این تکنولوژی می‌تواند برای مصاحبه‌ها یا سخنرانی‌هایی که نیاز به **transcript** دارند، بسیار مفید باشد. تبدیل گفتار به نوشتار تنها یک ابزار راحت نیست، بلکه یک نیاز اساسی برای ایجاد جامعه‌ای فراگیر و در دسترس است. این تکنولوژی با از بین بردن موانع فیزیکی و زمانی، به افراد کمک می‌کند تا پتانسیل‌های خود را به طور کامل محقق سازند. با توجه به رشد سریع هوش مصنوعی، انتظار می‌رود در آینده شاهد سیستم‌های دقیق‌تر و کاربرپسندتری باشیم که زندگی را برای همه افراد، به ویژه افراد با نیازهای ویژه، ساده‌تر کنند.

فواید و ضرورت نیاز به این تکنولوژی

صرفه‌جویی در زمان: تبدیل گفتار به نوشتار به صورت خودکار انجام می‌شود و نیاز به تایپ دستی را کاهش می‌دهد. این امر به ویژه برای افرادی که حجم زیادی از متن را باید ثبت کنند، بسیار کاربردی است. ثبت سریع اطلاعات بدون نیاز به تایپ دستی، به ویژه برای افرادی که با محدودیت‌های حرکتی مواجه هستند، یک مزیت کلیدی است. این تکنولوژی به کاربران اجازه می‌دهد تا در زمان کمتر، حجم بیشتری از کارها را انجام دهند.

استفاده مؤثر از تکنولوژی تبدیل گفتار به نوشتار برای نابینایان و افراد با توانمندی کمتر: این تکنولوژی برای افراد دارای معلولیت جسمی یا کسانی که در تایپ مشکل دارند، یک ابزار ضروری محسوب می‌شود. تبدیل گفتار به نوشتار (و بالعکس) یکی از ابزارهای تحول‌آفرین برای افراد نابینا یا کم‌بینا و همچنین افرادی است که به دلایل مختلف (مانند معلولیت‌های جسمی یا حرکتی) در استفاده از صفحه‌کلید یا ماوس محدودیت دارند. این تکنولوژی نه‌تنها دسترسی‌پذیری را بهبود می‌بخشد، بلکه استقلال و مشارکت این افراد را در فعالیت‌های روزمره، تحصیلی و حرفه‌ای افزایش می‌دهد. برای افراد نابینا یا کم‌بینا، تایپ کردن متون اغلب چالشی بزرگ است. تبدیل گفتار به نوشتار این امکان را فراهم می‌کند تا این افراد بتوانند ایده‌ها، یادداشت‌ها، و حتی مستندات رسمی خود را به راحتی تولید کنند. این امر نه‌تنها استقلال آن‌ها را افزایش می‌دهد، بلکه فرصت‌های برابر در آموزش و اشتغال را نیز فراهم می‌سازد. این افراد می‌توانند با استفاده از این تکنولوژی، متون خود را به‌صورت شفاهی دیکته کنند و نیازی به تایپ دستی ندارند. برای مطالعه متون، ترکیب این ابزار با تبدیل نوشتار به گفتار (**Text-to-Speech**) امکان‌پذیر است. به این ترتیب، کاربران می‌توانند متون تولیدشده را نیز بشنوند. دانش‌آموزان و دانشجویان نابینا می‌توانند تکالیف، مقالات، یا یادداشت‌های درسی خود را به‌راحتی ثبت کنند. در محیط‌های کاری، این افراد می‌توانند ایمیل‌ها، گزارش‌ها، یا مستندات را بدون وابستگی به دیگران تهیه کنند. این تکنولوژی به افراد با توانمندی کمتر

کمک می‌کند تا در گفتگوهای آنلاین، شبکه‌های اجتماعی، یا حتی پیام‌رسانی سریع‌تر و مؤثرتر مشارکت کنند. ثبت فوری ایده‌ها، لیست خرید، یا برنامه‌ریزی روزانه بدون نیاز به تایپ. سازماندهی و جستجوی اسناد با استفاده از دستورات صوتی. برای افرادی هم که در گفتار مشکل دارند (مانند افراد با اختلالات گفتاری)، تبدیل نوشتار به گفتار می‌تواند به عنوان یک واسطه عمل کند.

کاهش خطاهای انسانی: با وجود پیشرفت‌های اخیر در هوش مصنوعی، دقت سیستم‌های تبدیل گفتار به نوشتار به‌طور چشمگیری افزایش یافته است. این امر باعث کاهش خطاهای ناشی از تایپ دستی می‌شود.

کاربرد در محیط‌های حرفه‌ای: نشریات و رسانه‌ها: برای ثبت سریع مصاحبه‌ها یا سخنرانی‌ها.

تحقیقات علمی: برای ثبت نتایج آزمایش‌ها یا ایده‌های پژوهشی با سرعت و دقت بیشتر.

تجارت و کسب‌وکار: برای تهیه گزارش‌ها یا مستندسازی جلسات.

انعطاف‌پذیری: کاربران می‌توانند در هر زمان و مکان از این قابلیت استفاده کنند، به شرطی که به اینترنت و یک دستگاه مجهز به میکروفون دسترسی داشته باشند.

پشتیبانی از چند زبان: **Google Docs** از زبان‌های متعددی پشتیبانی می‌کند، که این ویژگی آن را به ابزاری جهانی تبدیل کرده است.

یکپارچه‌سازی با ابزارهای کمکی: این تکنولوژی می‌تواند با ابزارهای دیگر مانند صفحه‌خوان‌ها (**Screen Readers**) یا نرم‌افزارهای کنترل صوتی مانند **Dragon NaturallySpeaking** ترکیب شود تا تجربه کاربری بهتری فراهم کند.

در **Google Docs** امکان ذخیره خودکار متون و همگام‌سازی آن با سایر دستگاه‌ها وجود دارد، که برای کاربران نابینا بسیار مفید است.

چالش‌ها و راهکارها

دقت: گاهی اوقات سیستم در تشخیص کلمات یا لهجه‌های خاص دچار مشکل می‌شود. استفاده از میکروفون‌های باکیفیت و آموزش سیستم به صدای کاربر می‌تواند کمک‌کننده باشد.

آموزش: برخی کاربران ممکن است در ابتدا با این تکنولوژی راحت نباشند. برگزاری کارگاه‌های آموزشی می‌تواند به آن‌ها کمک کند تا از حداکثر پتانسیل آن استفاده کنند.

گوگل داکس (**Google Docs**) با ارائه قابلیت تایپ صوتی (**Voice Typing**)یکی از بهترین ابزارهای رایگان برای تبدیل گفتار به نوشتار است. در این راهنما، به طور کامل مراحل فعال‌سازی میکروفون، تنظیمات آن و نحوه استفاده از این ابزار را توضیح می‌دهیم.

مراحل استفاده از تایپ صوتی در Google Docs

۱. ورود به **Google Docs**: مرورگر خود را باز کنید و به آدرس **docs.google.com** بروید و وارد حساب گوگل خود شوید و یک سند جدید ایجاد کنید یا سند قبلی را باز کنید.

۲. فعال‌سازی تایپ صوتی: از منوی بالای صفحه، روی **Tools** کلیک کنید و گزینه **Voice typing** را انتخاب کنید. یا از کلیدهای میانبر استفاده کنید:

ویندوز/کروم: **Ctrl + Shift + S**

مک: **Command + Shift + S**

آیکون میکروفون در سمت چپ صفحه ظاهر می‌شود.

۳. تنظیم و انتخاب میکروفون:

اجازه دسترسی به میکروفون: با کلیک روی آیکون میکروفون، پیامی برای دسترسی به میکروفون نمایش داده می‌شود و روی **Allow** کلیک کنید تا گوگل داکس بتواند از میکروفون استفاده کند. اگر به اشتباه دسترسی را رد کردید، روی علامت قفل در نوار آدرس مرورگر کلیک کنید و مجدداً تنظیمات را تغییر دهید.

انتخاب میکروفون مناسب: اگر از چند میکروفون (مثلاً داخلی لپ‌تاپ، هندزفری یا میکروفون اکسترنال) استفاده می‌کنید، مطمئن شوید میکروفون موردنظر انتخاب شده است.

برای بررسی یا تغییر میکروفون: روی آیکون میکروفون در نوار آدرس مرورگر (کنار علامت قفل) کلیک کنید.

میکروفون دلخواه را از لیست انتخاب کنید.

با صحبت کردن، تست کنید که صدای شما به درستی ثبت می‌شود.

۴. شروع تایپ صوتی: روی آیکون میکروفون در گوگل داکس کلیک کنید. رنگ آن به قرمز تغییر می‌کند، یعنی فعال است. واضح و با سرعت معمولی صحبت کنید. متن شما به صورت خودکار تایپ می‌شود. برای فرمت‌دهی، از دستورات صوتی استفاده کنید، مثلاً:

"نقطه" (برای گذاشتن نقطه)

"خط جدید" (برای رفتن به خط بعد)

"ویرگول" (برای گذاشتن ویرگول)

۵. توقف یا ادامه تایپ صوتی: برای توقف، دوباره روی آیکون میکروفون کلیک کنید.

برای ادامه، مجدداً آن را فعال کنید.

۶. ویرایش متن: پس از اتمام تایپ صوتی، متن را بررسی و ویرایش کنید.

از ابزارهای فرمت‌دهی گوگل داکس (مثل پررنگ کردن، تغییر فونت و...) استفاده کنید.

نکات کلیدی برای بهبود عملکرد

۱. کیفیت میکروفون

میکروفون اکسترنال یا هندزفری باکیفیت، نتیجه بهتری دارد.

میکروفون را در فاصله ۱۵ – ۳۰ سانتی‌متری دهان خود قرار دهید.

۲. محیط مناسب

در محیطی کم‌صدا صحبت کنید تا نویز کمتری ثبت شود.

اگر محیط شلوغ است، از میکروفون‌های دارای نویزگیر استفاده کنید.

۳. زبان و لهجه

گوگل داکس از زبان فارسی پشتیبانی می‌کند. برای تغییر زبان:

روی آیکون میکروفون کلیک کنید.

زبان فارسی را از لیست انتخاب کنید.

اگر لهجه خاصی دارید، شمرده‌تر صحبت کنید.

۴. دستورات صوتی

برای کارایی بیشتر، از دستوراتی مثل "پاراگراف جدید" یا "انتخاب کن" استفاده کنید.

لیست کامل دستورات را با کلیک روی علامت ? کنار میکروفون ببینید.

رفع مشکلات رایج

۱. میکروفون کار نمی‌کند

تنظیمات: مرورگر را بررسی کنید و مطمئن شوید به میکروفون دسترسی دارد.

میکروفون را در دستگاه دیگری تست کنید تا از سالم بودن آن اطمینان حاصل کنید.

مرورگر را به روز رسانی یا ریستارت کنید.

۲. متن به درستی ثبت نمی‌شود: شمرده‌تر و واضح‌تر صحبت کنید.

از اصطلاحات ساده‌تر استفاده کنید.

در صورت امکان، از هدست استفاده نمایید.

۳. تاخیر در ثبت متن: اینترنت خود را بررسی کنید. این قابلیت نیاز به اتصال پایدار دارد.

برنامه‌های دیگر را ببندید تا منابع سیستم آزاد شود.

جمع‌بندی

تایپ صوتی گوگل داکس ابزاری فوق‌العاده برای افزایش سرعت و راحتی در تایپ است. با رعایت نکات گفته شده، می‌توانید به بهترین نتیجه برسید. این ویژگی برای دانشجویان، نویسندگان، و کسانی که با تایپ طولانی مشکل دارند و همچنین افرادی که مشکلات جسمی داشته و امکان تایپ برایشان فراهم نیست، بسیار کاربردی است.

منابع:

مستندات رسمی گوگل

Google Docs Help Center:Voice typing in Google Docs

این صفحه راهنمای رسمی گوگل برای استفاده از قابلیت تایپ صوتی است و تمام دستورات صوتی و تنظیمات را پوشش می‌دهد.

آموزش فناوری اطلاعات:
مبانی هک اخلاقی
بخش دوم

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

این بخش از مجله به مباحث آموزشی با محوریت موضوعات جذاب در زمینه فناوری اطلاعات خواهد پرداخت. هر مبحث متشکل از مجموعه اپیزودهایی خواهد بود که سلسله وار تا اتمام آن به مخاطب انتقال داده خواهد شد.

مبحث دوم :

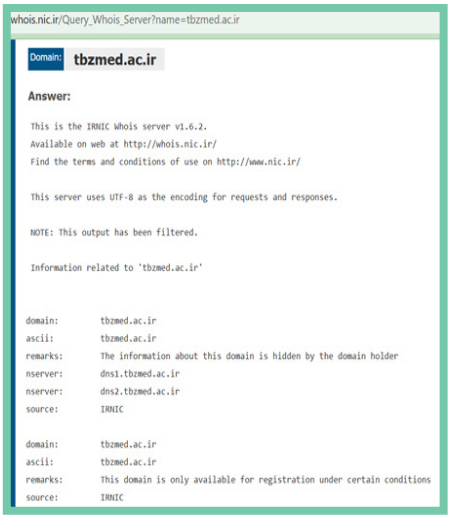
در ادامه مباحث مرتبط با هک اخلاقی (Ethical Hacking) به روشهای تست نفوذ(Pen-etration Tests) می پردازیم. این روشها بر اساس میزان اطلاعات فرد از هدف دارد دسته بندی می شوند. سه دسته بندی کلی جعبه سیاه(Blackbox) و جعبه سفید(WhiteBox) در این باره مرسوم می باشد.

در روشهای جعبه سیاه هکر اطلاعاتی راجع به هدف و شبکه آن ندارد و باید با استفاده از ردیابی و شناسایی اطلاعات اولیه را به دست آورد. این رویکرد مورد استفاده هکرهای کلاه سیاه(Black Hat) است و به دلیل آزمون و خطاهای مکرر توسط هکر روش زمانبری می باشد.

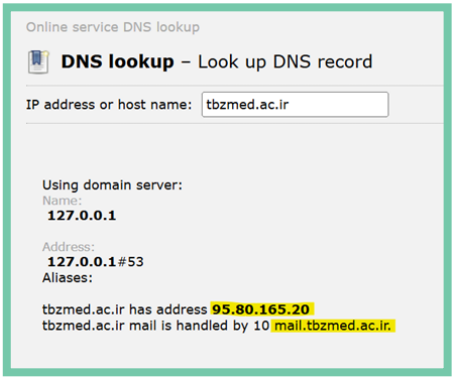
در روش جعبه سفید، هکر اطلاعات اولیه راجع به هدف و شبکه دارد و بر اساس اطلاعات ارائه شده توسط مالک سامانه ها و طبق قراردادهایی برای نفوذ به شبکه اقدام می کند. لذا این روش مورد استفاده هکرهای کلاه سفید(White Hat) است. هکر به کد برنامه، معماری و مستندات دسترسی دارد و بصورت عمیق و دقیق و عمدتا شبیه سازی حملات اقدام می کند. یکی از مفاهیم مرتبط با تست نفوذ مفهوم آسیب پذیری(Vulnerability) می باشد که به نقاط ضعف سیستم از ابعاد نرم افزاری یا سخت افزاری اشاره دارد. هکرها از این نقاط ضعف جهت نفوذ استفاده می کنند.

حال با مراحل و فازهای هک اخلاقی آشنا می شویم. در هک اخلاقی عمدتا چهارفاز جمع آوری اطلاعات(Foot printing)، اسکن(Scanning)، شمارش و استخراج اطلاعات(Enumera-tion) و نفوذ به سیستم(System Hacking) مطرح می شوند. در فاز Footprinting هکر با گردآوری اطلاعاتی از جمله شناسایی دامنه ها(Domain) ، آدرس های IP، اطلاعات مدیر سیستم(Administrator) و جمع آوری اطلاعات از طریق موتورهای جستجو و شبکه های اجتماعی در مورد هدف اقدام می کند. یکی از ابزارهای مفید در این زمینه Whois می باشد که اطلاعاتی در مورد دامنه ها و صاحبان آن ارائه می کند. برای مثال جهت بررسی زیرساخت دانشگاه علوم پزشکی تبریز، دامنه tbzmed.ac.ir به عنوان سایت اصلی و زیر سامانه هایی مثل sama.tbzmed.ac.ir و didgah.tbzmed.ac.ir از طریق

موتورهای جستجو به سادگی قابل شناسایی هستند. با ورود عنوان دامنه اصلی در سایت nic.ir به عنوان مرجع Whois دامنه های ایرانی، اطلاعاتی مشابه شکل زیر حاوی نام صاحب دامنه و سرورهای اصلی دامنه نمایش داده می شود.



در اقدام بعدی شناسایی بازه آدرسهای IP می تواند بسیار مهم باشد. برای این منظور نیز ابزارهای متنوعی عمدتا مبتنی بر سیستم عامل لینوکس(Linux) توسعه یافته اما ابزارهای محدود و آنلاینی نیز می توانند کمک کننده باشند. برای نمونه با ورود دامنه دانشگاه در سایت های nslookup به اطلاعاتی بیشتر از سایت دانشگاه مطابق تصویر زیر دست پیدا می کنیم که حاوی آدرس IP اصلی و دامنه ایمیل دانشگاه می باشد.

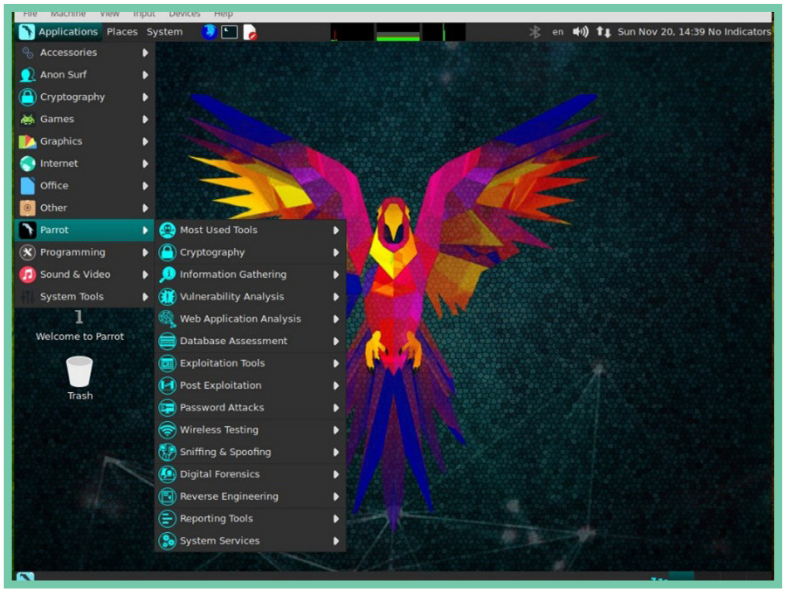


همانطور که مشاهده می کنید اطلاعات بسیارکلی و با ابزارهای متنوع قابل استحصال هستند اما ابزارهای منسجمی در قالب سیستم عامل های اختصاصی هک و امنیت نیز توسعه یافته اند که قبل از ورود تخصصی به فازهای هک اخلاقی آن را معرفی می نماییم.

سیستم‌عامل‌های اختصاصی هک اخلاقی همچون سیستم عامل ویندوز بصورت قابل نصب روی رایانه ارائه می‌شوند و شامل مجموعه‌ای از ابزارهای از پیش نصب‌شده برای تست نفوذ، امنیت شبکه، تحلیل آسیب‌پذیری‌ها و رمزنگاری هستند. در ادامه معروف‌ترین این سیستم‌عامل‌ها را معرفی می‌کنیم:

محبوب ترین سیستم عامل هک اخلاقی Kali Linux می باشد. Kali بصورت رایگان و با هدف تست نفوذ، مهندسی معکوس و کشف دیجیتال(Forensic digital) توسعه یافته و دارای محیط کاربری گرافیکی می باشد. این سیستم عامل بیش از ۶۰۰ ابزار هک اخلاقی دارد که در ادامه آموزشها به برخی از آنها اشاره خواهد شد. تصویری از محیط آن را در شکل زیر مشاهده می کنید. پیچیدگی زیاد و مصرف منابع سخت افزاری بالا از چالش های استفاده از این سیستم عامل می باشد.

سیستم عامل دیگر که نسبت به **Kali** سبک تر و ساده تر بوده و قابلیت های مناسبی ارائه می کند **Parrot** می باشد. این سیستم عامل نیز ابزارهای مشابه **Kali** ارائه می کند اما جامعه پشتیبان و کاربران آن محدودتر می باشد. تصویر زیر نمایی از سیستم عامل را نمایش می دهد.



سیستم عامل بسیار حرفه ای تر برای هکرهای حرفه ای و پرتجربه **BlackArch Linux** می باشد که بیش از ۲۵۰۰ ابزار تست و شناسایی را در خود جای داده. نصب آن پیچیده و کار با آن زمانبر می باشد. تصویر زیر نمایی از این سیستم عامل را نشان می دهد.

سیستم عامل های دیگری همچون **BackBox**، **Fedora Security Lab** و **Pentoo** برای تحلیل های تخصصی تر استفاده می شوند. برای مثال **Pentoo** ابزارهای اختصاصی شبکه های بی سیم **Wireless** را در اختیار متخصصین مخابراتی می گذارد. در ادامه به صورت تخصصی به فازهای هک اخلاقی خواهیم پرداخت.

ادامه دارد...

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
مرکزتحقیقات آموزش پزشکی

دکتر سعید سقطی‌زاد

دکتری حرفه‌ای پزشکی
رئیس دبیرخانه هیأت امنای دانشگاه

سوگند حبیبی

کارشناس ارشد فناوری اطلاعات سلامت
کارشناس فناوری اطلاعات سلامت معاونت درمان

وحید عباس‌زاده

دانشجوی PHD الکترونیک
کارشناس شبکه

فریبا اسماعیلی

کارشناس ارشد مهندسی نرم افزار
کارشناس فناوری اطلاعات
دانشکده پرستاری و مامایی

صابر درس‌خوان

کارشناس ارشد شبکه
کارشناس مسئول زیرساخت

نرگس نجفی

دانشجوی فناوری اطلاعات سلامت

رقیه سیدنژاد

کارشناس ارشد مهندسی نرم افزار
مدیر وب‌سایت مدیریت اطلاع‌رسانی پزشکی و منابع علمی

الهام منقش

دانشجوی دکتری تخصصی مدیریت اطلاعات سلامت اطلاعات سلامت

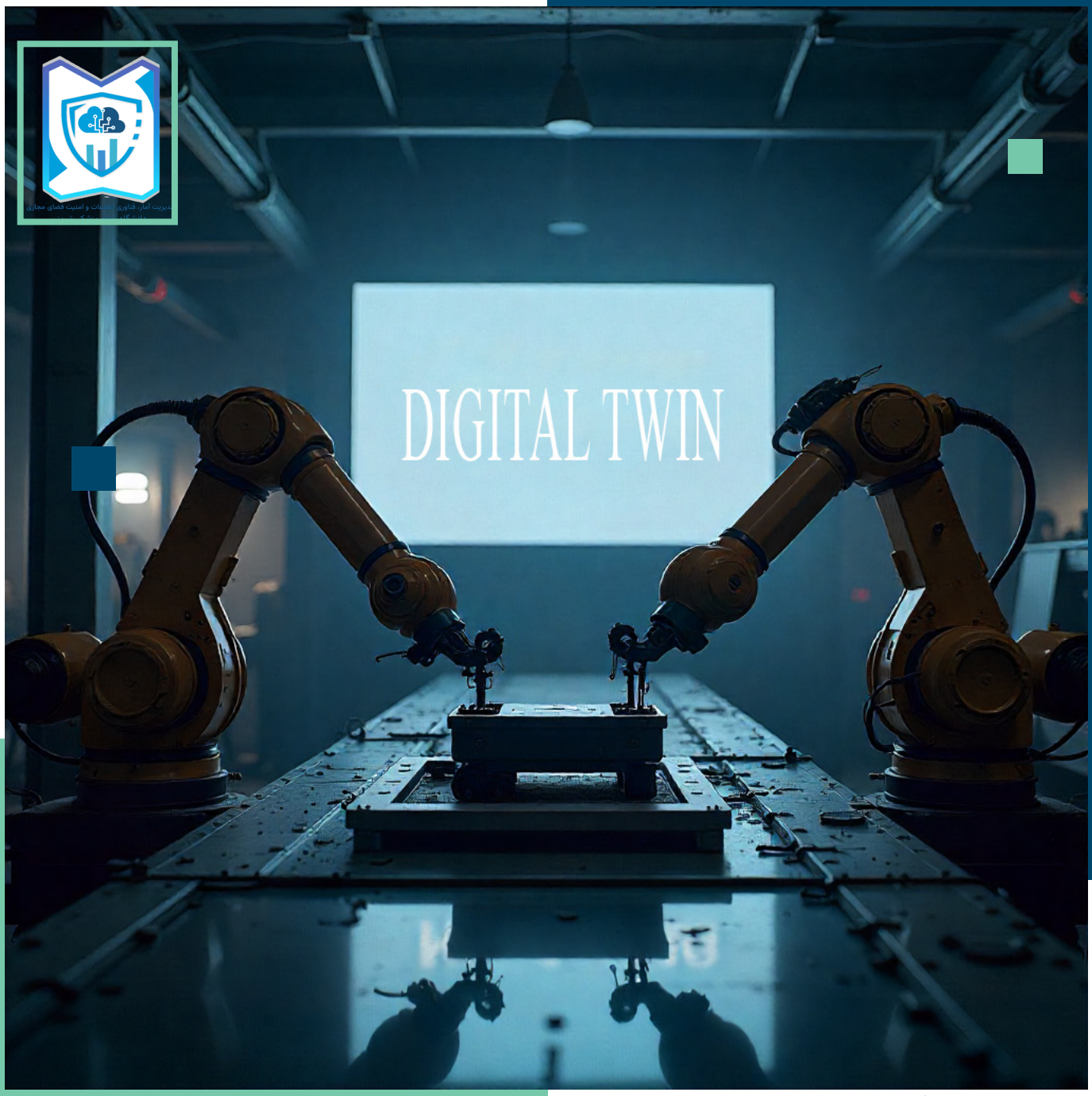
سمیه کرد

کارشناس ارشد مهندسی مواد گرایش شناسایی
کارشناس تحلیل‌گر سیستم معاونت آموزشی

جواد فرهادی

کارشناس ارشد نرم افزار

سیدمحمدحسن الهی



A New Pulse

anew_pulse