ماهنامه
پالسی نو
سال اول – شماره سوم – مهر ۱۴۰۴

A New Pulse
First year - October 2025 No:03

... آشنایی با فناوری‌ها و تجهیزات دوران پیش از ظهور نیمه‌رساناها می‌تواند به ما کمک کند تا اهمیت و نقش کلیدی نیمه‌رساناها را در دنیای الکترونیک و کامپیوتر ...

... یک کابل فیبر نوری از یک رشته نازک شیشه یا پلاستیک تشکیل شده است که توسط یک روکش محافظ، یک پوشش...

منظور از آمادگیِ الکترونیکی در حوزه اسناد، اصولاً فرآیندی است که طی آن اسناد و مدارکی که دیگر مورد استفاده قرار نمی‌گیرند ...

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: دکتر زینب جوادی والا، مهندس صابر درسخوان، مهندس وحید عباس‌زاده، مهندس جواد فرهادی، سیدمحمدحسن الهی، الهام منقش، بابک زارع‌آبادی، رقیه قاسمپور

مدیر اجرایی: دکتر سعید سقطی زاد

طراح و برنامه نویس: سیدمحمدحسن الهی

روابط عمومی: الناز هوشیان

سرمقاله

نویده خدائی
دانشجوی دکتری مدیریت فناوری اطلاعات

تفکر سیستمی در مواجهه با هوش مصنوعی

هوش مصنوعی به‌ویژه در شکل مولد آن، به‌سرعت وارد فضای دانشگاهی شده است؛ چه در قالب ابزارهای کمکی برای پژوهشگران، چه دستیاران هوشمند برای دانشجویان، و چه سامانه‌هایی که به‌طور مستقیم در آموزش و ارزیابی نقش ایفا می‌کنند. ورود این فناوری‌ها، نه محصول انتخاب آگاهانه دانشگاه‌ها، بلکه نتیجه جریانی جهانی است که دیوارهای علمی را درنوردیده است. واکنش‌ها نیز همان‌قدر متنوع است: گروهی با اشتیاق و هیجان به استقبال می‌روند، گروهی دیگر با نگرانی و بدبینی نگاه می‌کنند، و بسیاری هم هنوز در حیرت و تردید باقی مانده‌اند. اما پرسش مهم اینجاست: آیا دانشگاه‌های ما، و به‌ویژه دانشگاه‌های علوم پزشکی، این پدیده را در چارچوبی سیستمی درک می‌کنند؟ یا همچنان نگاه‌ها پراکنده و بخشی‌نگر است؟

امروز اگر پای صحبت اساتید برویم، برخی از خطر تقلب در امتحان‌ها می‌گویند؛ اگر به پژوهشگران گوش بسپاریم، دغدغه اصلی‌شان تغییر در فرآیند تولید مقاله است؛ بخش‌های فناوری اطلاعات بر کمبود زیرساخت تأکید می‌کنند و متخصصان اخلاق پزشکی از تهدید هویت علمی و مرزهای صداقت پژوهشی سخن می‌گویند. همه این نگرانی‌ها واقعی‌اند، اما مسئله اینجاست که هرکدام تنها گوشه‌ای از واقعیت را بازتاب می‌دهند. تصویر کلی هنوز شکل نگرفته است.

اینجاست که مفهوم «تفکر سیستمی» اهمیت پیدا می‌کند. تفکر سیستمی به ما یادآور می‌شود که دانشگاه فقط مجموعه‌ای از واحدهای جداگانه نیست؛ بلکه سیستمی پویاست که آموزش، پژوهش، فرهنگ سازمانی، اخلاق، سیاست‌گذاری و فناوری در آن به‌طور درهم‌تنیده عمل می‌کنند. تغییری که در یک بخش رخ می‌دهد، دیر یا زود بر دیگر بخش‌ها اثر خواهد گذاشت. پرسش این است: آیا فرهنگ دانشگاهی ما به‌اندازه کافی آماده است که چنین ارتباطات پیچیده‌ای را ببیند و بپذیرد؟

در همین‌جا بعد فرهنگی ماجرا پررنگ می‌شود. شاید فناوری را بتوان در قالب نرم‌افزار یا سخت‌افزار خرید و به کار گرفت، اما فرهنگ را نمی‌توان یک‌شبه تغییر داد. فرهنگ دانشگاهی ما سال‌ها بر ارزش‌هایی چون استقلال علمی، اصالت پژوهش، و روش‌های سنتی آموزش تکیه داشته است. اکنون، هوش مصنوعی این ارزش‌ها را به چالش کشیده: آیا مقاله‌ای که با کمک یک ابزار هوشمند نگاشته شده، همان وزن و اعتبار سنتی را دارد؟ آیا یادگیری که به واسطه پاسخ‌های یک ربات انجام می‌شود، به‌اندازه مطالعه و تجربه مستقیم ارزشمند است؟ و آیا می‌توان مرز روشنی میان «یادگیری اصیل» و «یادگیری مصنوعی» ترسیم کرد؟

و نهایتاً، آیا ما به‌عنوان یک نهاد فرهنگی، می‌خواهیم صرفاً مصرف‌کننده فناوری باشیم یا شکل‌دهنده رابطه میان فرهنگ و فناوری؟

پاسخ روشن و قطعی به این پرسش‌ها شاید هنوز در دسترس نباشد. اما طرح آن‌ها، قدم نخست برای بازاندیشی است. شاید بتوان گفت چالش اصلی دانشگاه در مواجهه با هوش مصنوعی، نه فنی است و نه حتی آموزشی؛ بلکه فرهنگی و سیستمی است. مسئله این نیست که چه ابزاری به‌کار گیریم یا چه آیین‌نامه‌ای تدوین کنیم، بلکه اینکه چگونه می‌خواهیم جایگاه خود را در این تغییر بزرگ بازتعریف کنیم؛ اینجاست که سیاست‌گذاران و نهادهای مرتبط می‌توانند با تصمیم گیری، مسیر نگاه به هوش مصنوعی را مشخص نمایند. اینکه آن را مجموعه‌ای از اقدامات پراکنده بدانیم یا بخشی از یک رویکرد سیستمی و فرهنگی، پرسشی است که شاید پاسخ آن آینده دانشگاه را شکل خواهد داد.

نیمه‌هادی ها در علوم کامپیوتر

وحید عباس‌زاده
دانشجوی PHD الکترونیک
کارشناس شبکه

مقدمه

نیمه‌هادی‌ها به عنوان یکی از شگفتی‌های تاریخ علم و فناوری، مسیر تحولی جذاب و پرچالش را طی کرده‌اند. آغاز این فناوری به دهه ۱۹۴۰ میلادی برمی‌گردد، هنگامی که دو مهندس آلمانی، والتر براتین و جان باریدین، در آزمایشگاه‌های بل موفق به کشف نخستین نیمه‌هادی شدند. این کشف، تحت عنوان ترانزیستور شناخته شد و نقطه عطفی در دنیای الکترونیک به شمار آمد، جایی که انقلابی بی‌سابقه در طراحی و تولید دستگاه‌های الکترونیکی آغاز شد. در ابتدای راه، کاربرد ترانزیستورها محدود به چند دستگاه الکترونیکی بود، اما با پیشرفت‌های سریع تکنولوژی و نوآوری در روش‌های ساخت، تراشه‌های نیمه‌هادی به تدریج کوچک‌تر و کارآمدتر شدند. با ورود مدارهای مجتمع در دهه‌های بعدی، این تراشه‌ها جایگزین تعداد زیادی از قطعات الکترونیکی شدند که پیش‌تر بر پایه ترانزیستورهای مستقل عمل می‌کردند. این تحول باعث افزایش کارایی دستگاه‌ها، کاهش هزینه‌های تولید و کوچک‌تر شدن ابعاد آن‌ها شده و در عین حال قابلیت اعتماد بیشتری را نیز به همراه داشت.

با پیشرفت سریع تکنولوژی در حوزه‌های الکترونیک و علوم کامپیوتر، نیاز به به‌روز نگه‌داشتن اطلاعات و آگاهی از نحوه عملکرد و دانش مرتبط با آن‌ها بیش از پیش احساس می‌شود. به همین دلیل، در این مقاله تلاش شده تا با نقش نیمه‌هادی‌ها در دنیای کامپیوتر آشنا شویم.

پیش از هر چیز، آشنایی با فناوری‌ها و تجهیزات دوران پیش از ظهور نیمه‌رساناها می‌تواند به ما کمک کند تا اهمیت و نقش کلیدی نیمه‌رساناها را در دنیای الکترونیک و کامپیوتر بهتر درک کنیم.

لامپ خلا یک ابزار الکترونیکی است که با اعمال ولتاژ به الکترودهای آن، امکان کنترل حرکت الکترون‌ها را در محیطی تقریبا خالی از هوا (داخل محفظه شیشه‌ای) فراهم می‌کند.

اجزای یک لامپ خلا

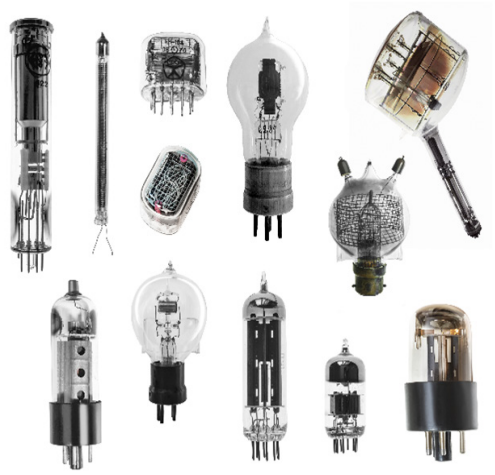
۱. سیستم تغذیه لامپ: لامپ خلا برای عملکرد صحیح به منبع تغذیه الکتریکی نیاز دارد تا جریان الکتریکی موردنیاز الکترودها را تامین کند.
۲. الکترودها: هر لامپ خلا دارای دو الکترود است که روبه‌روی هم قرار دارند. جنس این الکترودها معمولا از فلز تنگستن است که وظیفه تولید و هدایت الکترون‌ها را در لامپ بر عهده دارند.

۳. خلا: اصلی‌ترین عامل مقاومت و استحکام لامپ خلا، عاری بودن آن از هواست. با پمپاژ و تخلیه هوای درون حباب، فضای خلا ایجاد می‌شود که باعث افزایش کارایی لامپ می‌گردد.
۴. ماده تخلیه: بیشتر لامپ‌های خلا با گازی خاص پر می‌شوند تا با عبور جریان الکترون‌ها، تخلیه الکتریکی لازم را ایجاد کنند.

نحوه کار لامپ خلا

در لامپ خلا، الکترون‌ها از کاتد (**Cathode**) به سمت آند (**Anode**) حرکت می‌کنند. به دلیل وجود خلا در لامپ و نبود مولکول‌های هوا، الکترون‌های آزاد شده بدون توقف منتشر می‌شوند. سطح کاتد به اکسید فلزات قلیایی آغشته می‌شود و با گرمای تولیدشده توسط فیلامان تنگستنی، الکترون‌ها آزاد می‌شوند.

انواع لامپ‌های خلا

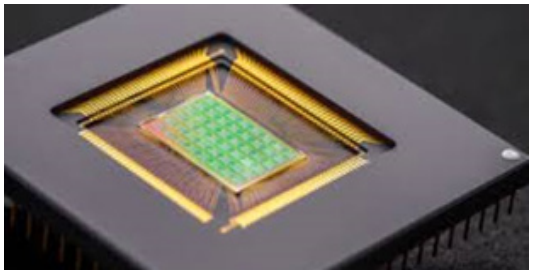


لامپ‌های خلا در انواع مختلفی تولید می‌شدند:

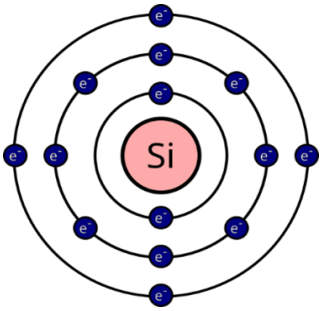
- لامپ دیود (**Diode**)
- لامپ ترایود (**Triode**)
- لامپ تترود (**Tetrode**)
- لامپ پنتود (**Pentode**)
- لامپ هگزود (**Hexode**)
- لامپ هپتود (**Heptode**)

لامپ‌های خلا با ایراداتی مانند حجم زیاد، عدم اطمینان در عملکرد، تولید گرمای بالا و اتلاف انرژی روبه‌رو هستند. این مشکلات عمدتا ناشی از رشته‌ی گرم شونده در داخل آن است، که در مقایسه با افزاره‌های نیمه هادی نظیر ترانزیستور، بهره‌وری کمتری دارد.

نیمه هادی‌ها

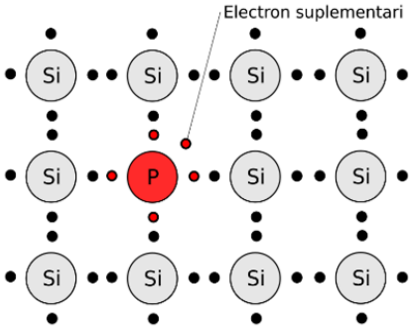


نیمه هادی‌ها موادی هستند که از نظر هدایت الکتریکی، بین هادی‌ها (مثل فلزات) و عایق‌ها (مثل شیشه) قرار دارند. در شرایط عادی، این مواد هدایت الکتریکی کمی دارند اما با اعمال انرژی (مثل حرارت یا نور) می‌توانند رسانایی بالاتری پیدا کنند.
مواد نیمه‌رسانا به دلیل ویژگی‌های خاص خود در بسیاری از حوزه‌های علمی و صنعتی مورد توجه قرار گرفته‌اند. هسته اتم این مواد شامل نوترون‌های خنثی و پروتون‌هایی با بار مثبت است. از آنجایی که تعداد پروتون‌ها و الکترون‌ها در یک اتم برابر هستند، مجموع بار اتم به صورت خنثی باقی می‌ماند. در ساختار الکترونی سیلیکون، مدار نزدیک به هسته دو الکترون دارد، مدار میانی دارای هشت الکترون است، و مدار خارجی آن چهار الکترون را در خود جای داده است. این آرایش خاص، خواص نیمه‌رسانایی سیلیکون را تعیین می‌کند.

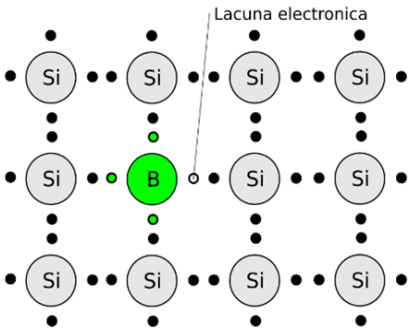


برای اینکه بتوانیم از سیلیکون یا دیگر عناصر نیمه هادی در صنایع الکترونیک بهره ببریم، لازم است که مقدار اندکی ناخالصی را به آنها اضافه کنیم. اگر ماده ای که به عنوان ناخالصی اضافه می‌کنیم دارای ۵ الکترون در آخرین مدار اتمی خود باشد، می تواند در شبکه کریستالی با سیلیکون ترکیب شده و یک الکترون آزاد نیز باقی بماند.

این الکترون برای انتقال جریان الکتریکی استفاده می‌شود، به شرطی که اختلاف پتانسیل مناسب در آن ماده ایجاد شود. حالتی که ناخالصی باعث به وجود آمدن الکترون اضافه می‌شود را نیمه هادی نوع **n** یا (**n type**) می‌نامند و مواد مورد استفاده در این روش معمولا فسفر و آرسنیک هستند.



در نقطه مقابل میتوان ماده ناخالصی که ۳ الکترون در مدار خارجی اش دارد را به نیمه هادی افزود، که با این‌کار حفره‌ای(فقدان جفت الکترونی) در شبکه کریستالی ایجاد شده که باعث آزاد شدن الکترون در نیمه هادی می‌شود. این نوع نیمه هادی ها را نوع **p** یا (**p type**) می‌نامند و معمولا از بور و آلومینیوم به عنوان ناخالصی استفاده می شود.



کاربرد نیمه هادی ها

شاید بتوان گفت که امروزه هیچ دستگاه الکترونیکی را پیدا نمی کنید که در آن از نیمه هادی استفاده نشده باشد.
کاربردهای نیمه هادی شامل ترانزیستورها برای کنترل جریان و ولتاژ در مدارات الکترونیکی، دیودها برای تبدیل جریان AC به DC و انتقال انرژی الکتریکی، LEDها برای تولید نور و سنسورها برای تشخیص نور، حرارت و فشار می‌شود.
برای آشنایی تعدادی از قطعاتی که از نیمه هادی ها ساخته شده‌اند آورده شده است:

- انواع مختلف دیود
- انواع مختلف ترانزیستور
- سلول های نوری
- سلول های خورشیدی
- تریستورها
- چیپست ها
- ریزپردازنده ها
- پردازنده های گرافیکی
- چیپست های حافظه

سخن پایانی

در عصر حاضر، نیمه‌هادی‌ها نقشی کلیدی در صنعت الکترونیک ایفا می‌کنند. از تلفن‌های هوشمند و کامپیوترهای شخصی گرفته تا تجهیزات پزشکی، خودروهای مدرن، ماهواره‌ها و تلویزیون‌های هوشمند، حضور این فناوری گسترده است. همچنین نیمه‌هادی‌ها محرک اصلی برخی از بزرگ‌ترین نوآوری‌ها مانند اینترنت اشیاء (IoT)، انرژی هوشمند، و رباتیک محسوب می‌شوند و تاثیرات قابل توجهی در بسیاری از صنایع دارند. با پیشرفت مداوم در طراحی و ساخت نیمه‌هادی‌ها، چشم‌انداز آینده این فناوری بسیار روشن است. انتظار می‌رود که توسعه بیشتر در این زمینه منجر به ارائه دستگاه‌ها و سامانه‌هایی شود که دارای هوشمندی بیشتر و کارایی بالاتر هستند و بهبودهای چشمگیری را در حوزه‌های مختلف از جمله انرژی و کاربردهای پیشرفته الکترونیکی به ارمغان آورند.

منابع

1. James M. Fiore. Semiconductor Devices: Theory and Application. April 2021
2. Peter Y.Yu Semiconductor Physics and Devices.1995
3. Corey Richard. Understanding Semiconductors: A Technical Guide for Non-Technical People.2022

کابل‌های نوری:

نگاهی عمیق به فیبر نوری و انواع آن

صابر درس‌خوان
کارشناس ارشد شبکه
کارشناس مسئول زیرساخت

مقدمه و پیشینه

تکامل انتقال داده‌ها، تلاشی بی‌وقفه برای سرعت، ظرفیت و قابلیت اطمینان بوده است. در این تلاش مداوم، کابل‌های فیبر نوری به عنوان آخرین نسل بی‌چون و چرا ظهور کرده‌اند و انقلابی در نحوه انتقال اطلاعات در فواصل وسیع و در شبکه‌های پیچیده ایجاد کرده‌اند. برخلاف کابل‌های مسی سنتی که داده‌ها را به عنوان سیگنال‌های الکتریکی منتقل می‌کنند، کابل‌های فیبر نوری از پالس‌های نوری استفاده می‌کنند که آنها را قادر می‌سازد تا داده‌های بیشتری را با سرعت‌های بسیار بالاتر و در فواصل بسیار بیشتر با حداقل تخریب سیگنال حمل کنند. این جهش تکنولوژیکی در توسعه مخابرات مدرن، اینترنت و شبکه‌های داده پرسرعت نقش مهمی داشته و تصویری پر جنب و جوش از دنیای به طور فزاینده به هم پیوسته ما ترسیم می‌کند.

طیف فناوری فیبر نوری

در هسته خود، یک کابل فیبر نوری از یک رشته نازک شیشه یا پلاستیک تشکیل شده است که توسط یک روکش محافظ، یک پوشش بافر، اعضای مقاوم و یک ژاکت بیرونی احاطه شده است. جادو در اصل بازتاب داخلی کلی نهفته است، که به موجب آن پالس‌های نوری در امتداد هسته فیبر هدایت می‌شوند و بدون امکان خروج از مرز روکش، بازتاب می‌شوند. این مکانیسم هوشمندانه امکان انتقال فوق‌العاده کارآمد داده‌ها را فراهم می‌کند.
کابل‌های فیبر نوری به طور کلی به دو نوع اصلی طبقه‌بندی می‌شوند که با نحوه عبور نور از هسته آنها متمایز می‌شوند:

- فیبر چند حالته (**MMF**): این نوع فیبر قطر هسته بزرگتری دارد، معمولاً ۵۰ یا ۶۲.۵ میکرومتر. این هسته بزرگتر اجازه می‌دهد تا چندین حالت یا مسیر نور به طور همزمان از طریق کابل عبور کنند. در حالی که این امر اتصال **MMF** را آسان‌تر و ساخت آن را ارزان‌تر می‌کند، مسیرهای نوری متعدد می‌توانند منجر به پراکندگی مودال شوند - جایی که پالس‌های نوری مختلف در زمان‌های کمی متفاوت می‌رسند. این پراکندگی پهنای باند و فاصله انتقال موثر را محدود می‌کند و آن را برای کاربردهای برد کوتاه‌تر مانند داخل ساختمان‌ها، مراکز داده یا شبکه‌های محلی (**LAN**) ایده‌آل می‌کند.

۱. فیبر چند حالته با ضریب درجه‌بندی شده (**GIMF**): زیرگروهی از **MMF** که در آن ضریب شکست هسته به تدریج از مرکز به سمت روکش کاهش می‌یابد. این طراحی به یکسان‌سازی زمان‌های سیر حالت‌های مختلف نور کمک می‌کند، پراکندگی مودال را کاهش می‌دهد و در مقایسه با فیبر نوری چندحالته با ضریب شکست پله‌ای، برد مؤثر را افزایش می‌دهد.

- فیبر تک‌حالته (**SMF**): در تضاد کامل با فیبر نوری چندحالته، قطر هسته بسیار کوچکتری دارد، معمولاً حدود ۹ میکرومتر. این هسته باریک فقط به یک حالت یا مسیر نور اجازه می‌دهد تا از طریق کابل منتشر شود. عدم وجود پراکندگی مودال به این معنی است که پالس‌های نور با دقت بسیار بیشتری حرکت می‌کنند و پهنای باند بسیار بالاتر و فواصل انتقال بسیار طولانی‌تری را ممکن می‌سازند که اغلب ده‌ها یا حتی صدها کیلومتر را بدون نیاز به تقویت سیگنال پوشش می‌دهد. این امر فیبر نوری تک‌حالته را به ستون فقرات ارتباطات از راه دور، کابل‌های زیر دریا و زیرساخت‌های اینترنت پرسرعت تبدیل می‌کند.

۱. فیبر نوری تک‌حالته استاندارد (G.۶۵۲): رایج‌ترین نوع فیبر نوری تک‌حالته، که برای طیف وسیعی از کاربردها

بهینه شده است.

۲. فیبر با پراکندگی تغییر یافته G.۶۵۳ (**DSF**): برای تغییر طول موج با پراکندگی صفر به ناحیه‌ای که تضعیف کمتر است طراحی شده است، اما این می‌تواند در سیستم‌های مالتی‌پلکسینگ تقسیم طول موج متراکم (**DWDM**) مشکلاتی ایجاد کند.

۳. فیبر با پراکندگی تغییر یافته غیر صفر (**NZDSF** G.۶۵۵): نوع پیشرفته‌تری است که طول موج با پراکندگی صفر را به خارج از پنجره عملیاتی معمول تغییر می‌دهد و اثرات غیرخطی که می‌تواند در سیستم‌های **DWDM** رخ دهد را کاهش می‌دهد و آن را برای شبکه‌های با ظرفیت بالا و مسافت طولانی بسیار مناسب می‌کند.

فراتر از این طبقه‌بندی‌های اولیه، انواع مختلف فیبر تخصصی وجود دارد که برای شرایط یا کاربردهای خاص محیطی مهندسی شده‌اند، مانند فیبرهای غیر حساس به خمش که برای مقاومت در برابر خمش‌های محکم‌تر بدون افت سیگنال طراحی شده‌اند، یا فیبرهای نوری پلاستیکی (**POF**) برای کاربردهای برد بسیار کوتاه و پهنای باند کم.

نتیجه‌گیری

کابل‌های فیبر نوری دستاوردی عظیم در فناوری انتقال داده هستند و رشته‌های درخشان آنها تار و پود عصر دیجیتال ما را می‌بافند. از شبکه‌های گسترده‌ای که قاره‌ها را به هم متصل می‌کنند تا کانال‌های پرسرعت درون مراکز داده ما، تمایز بین فیبر چندحالته و تک‌حالته، کاربرد و عملکرد آنها را تعیین می‌کند. با ادامه پیشروی بی‌وقفه فناوری، توسعه راه‌حل‌های فیبر نوری پیشرفته‌تر، نویدبخش گسترش بیشتر افق‌های ممکن در ارتباطات است و تضمین می‌کند که جریان اطلاعات به سرعت و بی‌حد و مرز خود نور باقی بماند.

دل نوشت

برای خوانندگان پالسی نو

سید محمدحسن الهی

در حوزه‌های مدیریتی متفاوت سازمان‌های مدرن و بزرگ بویژه دانشگاه ما، به طور فزاینده‌ای مشاهده می‌شود که به متخصصان فناوری اطلاعات مسئولیت‌هایی واگذار می‌شود که بسیار فراتر از مرزهای منابع و امکانات موجود سازمان است. کارشناسان فناوری اطلاعات، در حالی که متعهد به پیشرفت هستند، نگرانی عمیقی را در مورد عدم تعادل بین درخواست‌ها و واقعیت‌های موجود ابراز می‌نمایند. این گلایه به معنای ردِ توسعه نیست، بلکه یادآوری این است که ظرفیت‌های فنی باید بر پایه پشتیبانی متعادل از آن متمرکز باشد. هیچ سیستمی را نمی‌توان بدون ابزار لازم برای آن گسترش و توسعه داد، ایمن کرد یا مدرن نمود و از هیچ متخصصی نمی‌توان انتظار داشت که برای آنچه ابزار آن وجود ندارد، راه‌حل ارائه دهد.

در چارچوب سیاست‌های رشد و توسعه، این موضوع هم فوری و هم مهم تلقی می‌شود. همسویی رشد با منابع دیگر اختیاری نیست، بلکه ضرورتی است اجتناب‌ناپذیر. درخواست‌ها باید بر برنامه‌ریزی منطقی، سرمایه‌گذاری متعادل و شناخت این که توسعه بر انتظارات واقع‌بینانه استوار است، متمرکز گردد. تنها از این طریق است که رشد و توسعه می‌تواند بدون فرسایش پرسنلی که ستون‌های آن است ادامه یابد.

... و این طریق، مسیری است که می‌توان آن را **پالسی نو** نامید.

روش‌های رایج مهندسی اجتماعی برای سوءاستفاده از شبکه‌های کامپیوتری

جواد فرهادی
کارشناس ارشد نرم افزار

مقدمه و پیشینه

مرزهای دیجیتال، قلمرویی از کدهای پیچیده و سیستم‌های به‌هم‌پیوسته، دائماً در محاصره مهاجمان است. در حالی که بدافزارهای پیچیده و سوءاستفاده‌های پیچیده‌تر از آن اغلب تیتر خبرها را به خود اختصاص می‌دهند، یک تهدید موذیانه‌تر و قدیمی‌تر، حتی قوی‌ترین خطوط دفاعی شبکه‌ها را نیز به‌طور مداوم تضعیف می‌کند: مهندسی اجتماعی.
مهندسی اجتماعی هنر دستکاری روانشناختی است نه استفاده از آسیب‌پذیری‌های فنی، بلکه از عنصر ذاتی انسان در هر سیستم فناوری سوءاستفاده می‌کند. برای دهه‌ها، مهاجمان به‌طور استادانه‌ای از تاکتیک‌های مهندسی اجتماعی برای عبور از فایروال‌ها، نفوذ به محیط‌های امن و استخراج اطلاعات حساس استفاده کرده‌اند که اغلب عواقب مخربی برای سازمان‌ها داشته است.
جذابیت مهندسی اجتماعی در سادگی ظریف و اثربخشی عمیق آن نهفته است. مهاجمان به جای صرف منابع برای کشف نقص‌های نرم‌افزاری مبهم، در دسترس‌ترین و اغلب ضعیف‌ترین حلقه - یعنی کاربر انسانی - را هدف قرار می‌دهند. مهندسان اجتماعی با درک و سوءاستفاده از روانشناسی، اعتماد، کنجکاوی و حتی ترس انسان، می‌توانند به‌طور مؤثر افراد را فریب دهند تا داده‌های محرمانه را فاش کنند یا اقداماتی را انجام دهند که امنیت شبکه را کاملا به خطر می‌اندازد.

مهندسی اجتماعی به عنوان پایگاه فریب

فریب‌ها در مهندس اجتماعی متنوع است، هر نوع آن با دقت برای سوءاستفاده از تمایلات خاص انسانی ساخته شده است. از جمله فراگیرترین آنها، فیشینگ است، نوعی فریب دیجیتالی که در آن مهاجمان از طریق ایمیل، پیامک یا رسانه‌های اجتماعی، خود را به عنوان نهادهای قانونی مانند بانک‌ها، شرکت‌های فناوری یا حتی بخش‌های داخلی فناوری اطلاعات جا می‌زنند. این ارتباطات اغلب حس و حال فوریت را به هدف القا می‌کنند یا جوایز وسوسه‌انگیزی را ارائه می‌دهد و گیرندگان را مجبور به کلیک روی لینک‌های مخرب یا دانلود پیوست‌های آلوده می‌کنند. این لینک‌ها معمولاً به وب‌سایت‌های جعلی منتهی می‌شوند که برای جمع‌آوری اطلاعات ورود به سیستم یا اطلاعات شخصی طراحی شده‌اند و به امید به دام انداختن یک قربانی ناآگاه، شبکه گسترده‌ای را ایجاد می‌کنند.

فیشینگ نیزه‌ای، نوعی هدفمندتر و پیچیده‌تر، ارتباط نزدیکی با فیشینگ دارد. در اینجا، مهاجمان برای جمع‌آوری اطلاعات خاص در مورد قربانیان مورد نظر خود - نقش‌های شغلی، همکاران، فعالیت‌های اخیر یا

حتی علایق شخصی آنها - شناسایی انجام می‌دهند. این رویکرد سفارشی به آنها اجازه می‌دهد تا پیام‌های بسیار شخصی‌سازی شده و متقاعدکننده‌ای ایجاد کنند که احتمال موفقیت را به طرز چشمگیری افزایش می‌دهد. مثلا ایمیلی ظاهراً از طرف مدیرعامل به کارمند بخش مالی ارسال می شود که درخواست انتقال وجه فوری به یک فروشنده ظاهراً قانونی را دارد.

یکی دیگر از تاکتیک‌های قدرتمند، «پیش‌داوری» است، جایی که مهاجم یک سناریو یا «بهانه» ساختگی برای جلب اعتماد قربانی و استخراج اطلاعات ایجاد می‌کند. این روش ممکن است شامل جا زدن خود به عنوان یک تکنسین پشتیبانی فناوری اطلاعات باشد که نیاز به تأیید جزئیات حساب برای حل یک مشکل فرضی دارد، یا یک نماینده خدمات مشتری که نیاز به تأیید اطلاعات شخصی برای «به‌روزرسانی حساب» دارد. نکته کلیدی، ایجاد یک روایت باورپذیر است که درخواست داده‌های حساس را توجیه می‌کند.

«طعمه‌گذاری» شامل فریب دادن قربانیان با وعده چیزی مطلوب، مانند نرم‌افزار رایگان، موسیقی یا محتوای اختصاصی است. مهاجمان رسانه‌های آلوده، مانند درایوهای **USB** با برچسب عناوین جذاب، را در مکان‌های عمومی رها می‌کنند یا دانلودهای وسوسه‌انگیز را در وب‌سایت‌های مشکوک ارائه می‌دهند. کنجکاوی اغلب بر احتیاط غلبه می‌کند و افراد را به وصل کردن درایو آلوده یا دانلود فایل مخرب سوق می‌دهد و در نتیجه سیستم‌ها یا شبکه‌های آنها را آلوده می‌کند.

در نهایت، **Tailgating** (یا **Piggybacking**) یک تکنیک مهندسی اجتماعی فیزیکی است که در آن یک فرد غیرمجاز، یک فرد مجاز را تا یک منطقه محدود دنبال می‌کند. مهاجم با وانمود کردن به اینکه متعلق به آن منطقه است، مثلاً حمل جعبه یا دستپاچه به نظر رسیدن، می‌تواند از ادب یا بی‌توجهی دیگران سوءاستفاده کند تا به مناطق یا سیستم‌های حساس دسترسی فیزیکی پیدا کند.

نتیجه‌گیری: تقویت فایروال انسانی

تهدید مداوم مهندسی اجتماعی یک واقعیت حیاتی را برجسته می‌کند:

دفاع‌های تکنولوژیکی به تنهایی کافی نیستند. موثرترین استراتژی در برابر این حملات موذیانه شامل تقویت «**فایروال انسانی**» از طریق آموزش جامع و مداوم آگاهی امنیتی است. آموزش کارمندان در مورد تاکتیک‌های رایج مورد استفاده مهندسان اجتماعی، پرورش فرهنگ شک و تردید نسبت به درخواست‌های ناخواسته و ایجاد پروتکل‌های روشن برای مدیریت اطلاعات حساس از اهمیت بالایی برخوردار است. سازمان‌ها . نهادهای نظارتی مسئول باید پرسنل خود را برای تشخیص علائم فریب توانمند سازند و به آنها اعتماد به نفس لازم برای پرسش، تأیید و گزارش فعالیت‌های مشکوک بدون ترس از مجازات را بدهند. با در نظر گرفتن عنصر انسانی نه به عنوان یک آسیب‌پذیری، بلکه به عنوان یک مدافع هوشیار، شبکه‌ها می‌توانند در برابر مهاجمان نامرئی دیجیتال، مقاومت بیشتری نشان دهند.

ویکی واژه

WIKIWORD

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.

سید محمدحسن الهی

SSL/TLS

(Secure Socket Layer / Transport Layer Security)

این پروتکل در ایمن‌سازی ارتباطات از طریق اینترنت اساسی است. این پروتکل اتصال بین کلاینت و سرور را رمزگذاری می‌کند و تضمین می‌کند که اطلاعات حساس مانند اطلاعات ورود به سیستم و داده‌های مالی قابل رهگیری نیستند. **TLS**، جانشین مدرن **SSL**، احراز هویت، محرمانگی و یکپارچگی داده‌ها را فراهم می‌کند و آن را برای مرور امن و تراکنش‌های آنلاین ضروری می‌سازد.

HTTPS

(Hypertext Transfer protocol Secure)

HTTPS پسوند امن **HTTP** است که به طور گسترده برای ارتباطات وب استفاده می‌شود. با استفاده از **SSL/TLS**، تضمین می‌کند که داده‌های رد و بدل شده بین مرورگر و سرور وب رمزگذاری و محافظت شده باقی می‌مانند. این پروتکل اکنون برای هر وب‌سایت قابل اعتمادی استاندارد است و از استراق سمع و دستکاری غیرمجاز داده‌های منتقل شده جلوگیری می‌کند.

IPSec

(Internet Protocol Security)

IPSEC مجموعه‌ای از پروتکل‌ها است که برای ایمن‌سازی ارتباطات پروتکل اینترنت طراحی شده است. این پروتکل که در لایه شبکه عمل می‌کند، رمزگذاری، احراز هویت و مکانیسم‌های تبادل کلید را فراهم می‌کند. این پروتکل معمولاً در شبکه‌های خصوصی مجازی (**VPN**) استفاده می‌شود، جایی که از داده‌های عبوری در شبکه‌های غیر قابل اعتماد محافظت می‌کند و محرمانگی و یکپارچگی را تضمین می‌کند.

PGP

(Pretty Good Privacy)

PGP پروتکلی است که به ایمن‌سازی ایمیل و فایل‌ها اختصاص داده شده است. این پروتکل هشینگ، فشرده‌سازی داده‌ها، رمزنگاری کلید متقارن و رمزنگاری کلید عمومی را برای ارائه محرمانگی و احراز هویت ترکیب می‌کند. مدل اعتماد غیرمتمرکز **PGP**، آن را در بین افراد و سازمان‌هایی که به دنبال رمزگذاری قوی بدون تکیه صرف بر مقامات متمرکز هستند، محبوب کرده است.

WPA3

(Wi-Fi Protected Access 3)

WPA3 جدیدترین استاندارد برای ایمن‌سازی شبکه‌های بی‌سیم است. این پروتکل روش‌های رمزگذاری را تقویت می‌کند، در برابر حملات جستجوی فراگیر مقاومت می‌کند و ویژگی‌هایی مانند رمزگذاری داده‌های شخصی‌سازی شده را برای شبکه‌های WI-FI باز معرفی می‌کند. **WPA3** نشان دهنده تکامل مداوم امنیت بی‌سیم در پاسخ به تهدیدات سایبری رو به رشد است.

SSH

(Secure SHell)

SSH برای دسترسی امن از راه دور به سیستم‌ها و سرورها استفاده می‌شود. این پروتکل با ارائه ارتباطات رمزگذاری شده، احراز هویت و بررسی‌های یکپارچگی، جایگزین پروتکل‌های ناامن قدیمی‌تر مانند **TELNET** می‌شود. مدیران و مهندسان برای مدیریت سیستم‌ها از راه دور بدون افشای اعتبارنامه‌ها یا دستورات حساس در معرض رهگیری، به **SSH** متکی هستند.

S/MIME

(Secure/ Multipurpose Internet Mail Extensions)

S/MIME استانداردی برای ایمن‌سازی ارتباطات ایمیلی ارائه می‌دهد. این پروتکل اصالت فرستنده را تضمین می‌کند، از محرمانه بودن پیام‌ها از طریق رمزگذاری محافظت می‌کند و با امضاهای دیجیتال، یکپارچگی را حفظ می‌کند. این پروتکل در حفاظت از تبادلات ایمیل‌های شرکتی و دولتی نقش مهمی داشته و دارد.

زیرســاخت و حکمرانــی داده؛ اســاس کارآمــدی ســلامت دیجیتــال

الهام منقش
دانشـجوی دکتـری تخصصـی مدیریت اطلاعـات سـلامت اطلاعات

سلامت دیجیتال به‌عنوان یکی از محورهای تحول‌آفرین در نظام‌های بهداشت و درمان، فرصت‌های بی‌سابقه‌ای برای بهبود کیفیت خدمات، افزایش بهره‌وری و گسترش عدالت در دسترسی ایجاد کرده است. از پرونده الکترونیک سلامت گرفته تا سامانه‌های پایش از راه دور بیماران، همه و همه بر بستری از داده‌های ساخت‌یافته و زیرساخت امن بنا شده‌اند. با این حال، تجربه جهانی و ملی نشان داده است که هرگونه ضعف در معماری زیرساخت یا حکمرانی داده، می‌تواند پروژه‌های سلامت دیجیتال را با شکست یا کاهش اثرگذاری مواجه کند. ازاین‌رو، کیفیت زیرساخت‌ها و اثربخشی حکمرانی داده به‌عنوان دو رکن اساسی در توسعه سلامت دیجیتال، نقشی تعیین‌کننده در پایداری و پیشرفت نظام سلامت ایران دارند. این مقاله به بررسی ضرورت‌ها، چالش‌ها و راهکارهای توسعه این دو رکن و تحلیل جایگاه آن‌ها در ارتقای کارآمدی نظام سلامت کشور می‌پردازد.

زیرساخت؛ ستون فقرات سلامت دیجیتال

زیرساخت سلامت دیجیتال مجموعه‌ای از اجزای فنی، ارتباطی و سازمانی است که امکان جمع‌آوری، ذخیره‌سازی، پردازش و تبادل داده‌های سلامت را فراهم می‌آورد. این زیرساخت باید دارای ویژگی‌های زیر باشد:

- یکپارچگی: ارتباط میان سامانه‌های بیمارستانی، مراکز بهداشت، آزمایشگاه‌ها و بیمه‌ها، تنها در صورتی ممکن است که استانداردهای تبادل داده (مانند **HL7** و **FHIR**) رعایت شود.
- مقیاس‌پذیری: توانایی پاسخ به حجم روبه‌افزایش داده‌ها، خصوصاً با ورود تصاویر پزشکی، داده‌های ژنومی و داده‌های اینترنت اشیا پزشکی(**IoMT**).
- پایداری و تاب‌آوری: حفظ عملکرد سیستم در برابر اختلالات فنی، حوادث طبیعی و تهدیدات سایبری.

بدون این زیرساخت پایدار، حتی بهترین الگوریتم‌های تحلیلی و هوش مصنوعی نیز کارکردی نخواهند داشت.

حکمرانی داده؛ از جمع‌آوری تا تصمیم‌سازی

حکمرانی داده در سلامت دیجیتال، مجموعه‌ای از سیاست‌ها، فرآیندها و ساختارهای مدیریتی است که بر کیفیت، امنیت و استفاده بهینه از داده‌ها نظارت دارد. این حکمرانی باید پاسخگوی سه نیاز اصلی باشد:

- اعتماد عمومی: مردم تنها زمانی داده‌های حساس خود را در اختیار نظام سلامت قرار می‌دهند که مطمئن باشند این داده‌ها به‌طور ایمن و اخلاقی مدیریت می‌شوند.
- کیفیت داده: داده‌های ناقص، تکراری یا فاقد استاندارد، پایه تصمیم‌گیری‌های نادرست خواهند بود.
- دسترس‌پذیری هدفمند: داده‌ها باید برای پژوهش، سیاست‌گذاری و ارائه خدمات در دسترس باشند، اما این دسترسی باید با اصل حداقل‌گرایی و حفظ حریم خصوصی همراه باشد.

چالش‌های موجود در ایران

در کشور ما، چند مانع ساختاری و اجرایی، توسعه زیرساخت و حکمرانی داده را کند کرده است:

- پراکندگی سامانه‌ها: هر دانشگاه علوم پزشکی یا سازمان مرتبط، اغلب سامانه‌های مختص خود را دارد که با سایر سامانه‌ها همخوانی کامل ندارند.
- ضعف در استانداردسازی: فقدان الزام جدی به استفاده از استانداردهای بین‌المللی تبادل داده، موجب کاهش قابلیت همکاری سیستم‌ها شده است
- محدودیت‌های بودجه و منابع انسانی متخصص: توسعه مراکز داده، شبکه‌های امن و تیم‌های تخصصی نیازمند سرمایه‌گذاری پایدار است.
- چالش‌های حقوقی و حریم خصوصی: نبود یک قانون جامع و به‌روز در حوزه حفاظت از داده‌های سلامت، باعث ابهام در مسئولیت‌ها و حقوق ذی‌نفعان شده است.

الزامات توسعه زیرساخت و حکمرانی داده

برای عبور از چالش‌ها، مجموعه‌ای از اقدامات راهبردی ضروری است:

- ایجاد معماری ملی داده سلامت: یک نقشه‌راه جامع که تعامل میان تمامی اجزای نظام سلامت را تعریف و استاندارد کند.
- توسعه مراکز داده ملی و منطقه‌ای: با قابلیت پشتیبان‌گیری، بازیابی پس از فاجعه و انطباق با الزامات امنیت سایبری.
- نهاد مستقل حکمرانی داده: سازمانی با اختیارات قانونی برای نظارت بر کیفیت، امنیت و به‌کارگیری داده‌ها در سراسر کشور.
- سرمایه‌گذاری در نیروی انسانی: تربیت متخصصان داده‌کاوی، امنیت اطلاعات و معماری سیستم‌های سلامت.
- به‌روزرسانی چارچوب‌های قانونی: تصویب قوانین مشخص درباره مالکیت داده، رضایت آگاهانه و حق فراموشی.

تجربه‌های جهانی و درس‌آموخته‌ها

کشورهایی مانند استونی و دانمارک نشان داده‌اند که با یکپارچه‌سازی کامل داده‌های سلامت و ایجاد زیرساخت‌های ابری امن، می‌توان دسترسی آنی پزشکان و بیماران به اطلاعات را فراهم کرد و تصمیم‌گیری‌های بالینی را بهبود بخشید. نقطه مشترک موفقیت این کشورها، وجود یک مرکز ملی حکمرانی داده و تعهد به استانداردسازی سراسری است.

نتیجه‌گیری

زیرساخت و حکمرانی داده، نه صرفاً یک پشتیبان فنی، بلکه قلب تپنده سلامت دیجیتال هستند. اگر این دو حوزه به‌درستی طراحی و پیاده‌سازی شوند، می‌توان انتظار داشت که سلامت دیجیتال در ایران از سطح پروژه‌های پراکنده فراتر رفته و به یک نظام پایدار و کارآمد تبدیل شود. این مسیر مستلزم سرمایه‌گذاری، همکاری بین‌بخشی و مهم‌تر از همه، اعتمادسازی میان مردم و حاکمیت است. بدون این پیش‌نیازها، سلامت دیجیتال نه به‌عنوان افق نوین، بلکه به‌عنوان فرصتی از دست‌رفته در حافظه تاریخ باقی خواهد.

هوش مصنوعی و حریم خصوصی شهروندان؛ فرصت‌ها و چالش‌ها در مسیر ارتقای اعتماد عمومی

بابک زارع‌آبادی
کارشناسی پژوهشگری علوم اجتماعی
کارشناس فناوری اطلاعات مرکز تحقیقات مدیریت خدمات بهداشتی درمانی تبریز

مقدمه

هوش مصنوعی در سال‌های اخیر به یکی از مهم‌ترین فناوری‌های تحول‌آفرین در جهان تبدیل شده است. این فناوری در حوزه‌های مختلف از جمله سلامت، آموزش، بانکداری و شهرهای هوشمند در حال گسترش است و فرصت‌های متعددی برای بهبود کیفیت زندگی شهروندان فراهم کرده است با این حال، بهره‌برداری گسترده از داده‌های شخصی، پرسش‌هایی جدی درباره حریم خصوصی و نحوه اعتماد مردم به سامانه‌های هوشمند مطرح می‌سازد. در واقع، حفظ حریم خصوصی شهروندان و ایجاد شفافیت در استفاده از داده‌ها، یکی از مهم‌ترین چالش‌های اخلاقی و مدیریتی عصر هوش مصنوعی به شمار می‌رود.

کاربردهای هوش مصنوعی در خدمات عمومی

سلامت دیجیتال: پرونده الکترونیک سلامت و سیستم‌های تشخیص بیماری مبتنی بر **AI** می‌توانند کیفیت مراقبت‌های پزشکی را ارتقا دهند.
شهرهای هوشمند: مدیریت حمل‌ونقل، انرژی و خدمات شهری با تحلیل داده‌ها، موجب صرفه‌جویی در منابع و افزایش رفاه شهروندان می‌شود.
آموزش هوشمند: استفاده از پلتفرم‌های آموزشی مبتنی بر یادگیری ماشین می‌تواند عدالت آموزشی را افزایش دهد.
این کاربردها زمانی موفق خواهند بود که مردم نسبت به امنیت داده‌های خود اطمینان داشته باشند.

فرصت‌ها

بهبود کیفیت خدمات عمومی و سلامت
تسریع در تصمیم‌گیری‌های مدیریتی
افزایش بهره‌وری در سیستم‌های شهری و ملی

چالش‌ها و دغدغه‌های اخلاقی

نقض حریم خصوصی: جمع‌آوری و تحلیل داده‌های فردی بدون شفافیت می‌تواند اعتماد عمومی را کاهش دهد.
نگرانی از امنیت داده‌ها: نبود قوانین مشخص در حفاظت از اطلاعات ممکن است زمینه‌ساز سوء استفاده یا نشت داده‌ها شود.
ضرورت پاسخگویی: شهروندان باید بدانند داده‌های آن‌ها چگونه و برای چه اهدافی مورد استفاده قرار می‌گیرد.

تجربه‌های بین‌المللی

اتحادیه اروپا با تصویب مقررات **GDPR**، چارچوبی شفاف برای حفاظت از داده‌ها و اعتمادسازی ایجاد کرده است.
کشورهای آسیایی در شهرهای هوشمند از **AI** بهره می‌گیرند، ولی همزمان در تلاشند استانداردهای بومی برای حفظ داده‌های شهروندان تدوین کنند.

جایگاه ایران

در ایران توسعه خدمات دیجیتال در بخش‌های مختلف از جمله سلامت و آموزش سرعت گرفته است. اما نبود یک چارچوب جامع در زمینه حفاظت از داده‌های شخصی، می‌تواند چالش‌هایی در اعتمادسازی ایجاد کند. تدوین قوانین شفاف و آموزش عمومی درباره حقوق شهروندان در فضای دیجیتال، می‌تواند زمینه‌ساز افزایش پذیرش و موفقیت پروژه‌های هوش

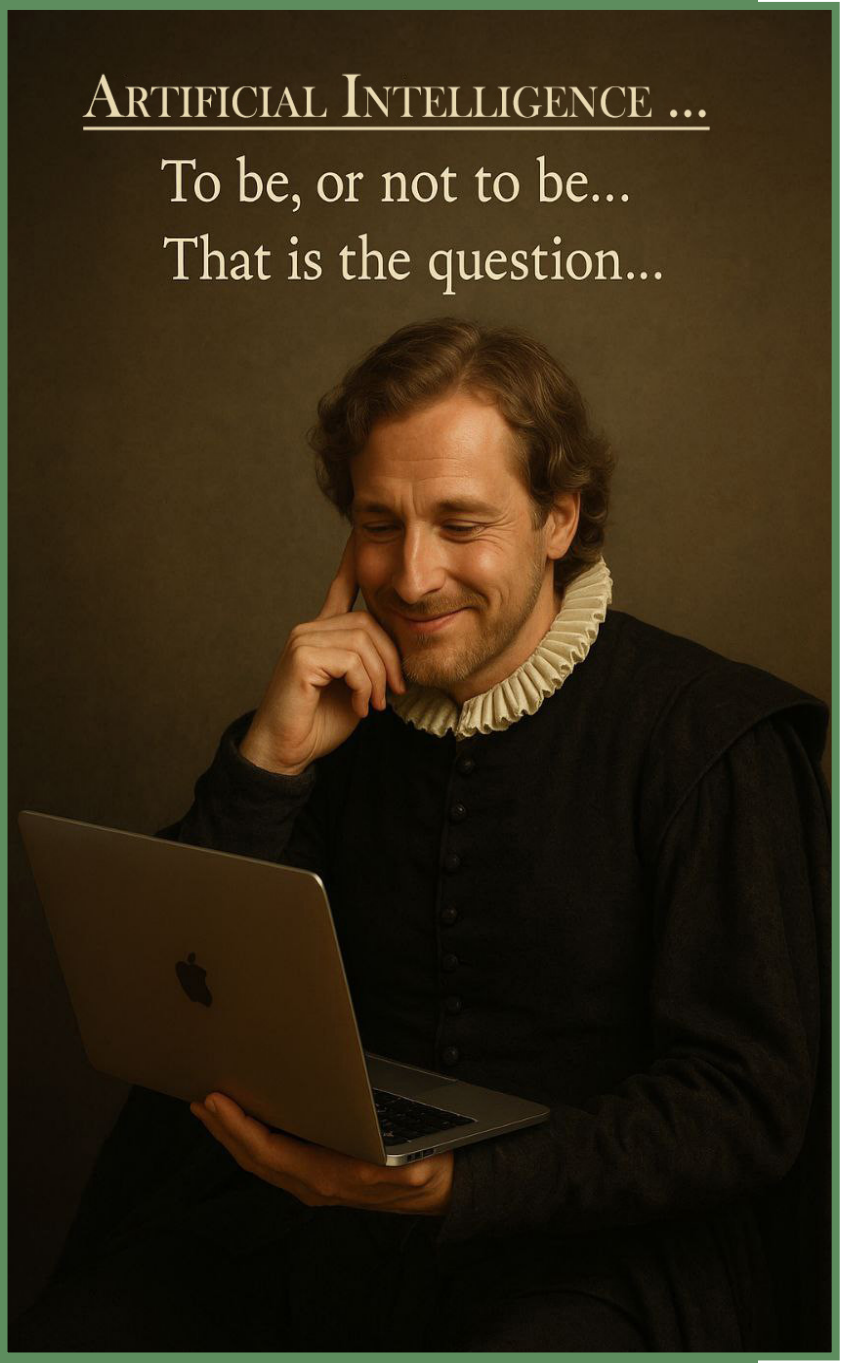
مصنوعی باشد.

جمع‌بندی و پیشنهادها

هوش مصنوعی می‌تواند ابزار ارزشمندی برای ارتقای کیفیت خدمات عمومی در ایران باشد. با این حال، موفقیت آن به میزان اعتماد شهروندان بستگی دارد. برای تقویت این اعتماد:

۱. باید قوانین مشخص در حوزه حفاظت از داده‌ها تدوین شود.
۲. استفاده از داده‌های شهروندان باید با شفافیت و اطلاع‌رسانی کافی همراه باشد.
۳. آموزش عمومی درباره حقوق دیجیتال، می‌تواند مشارکت فعال‌تری از سوی مردم ایجاد کند.

در نهایت، حفظ حریم خصوصی نه تنها یک ارزش اخلاقی، بلکه پیش‌شرط موفقیت راهبردهای هوش مصنوعی در کشور است.



منابع:

1. **European Parliament**. (2018). **General Data Protection Regulation (GDPR)**.
2. **Zuboff, S**. (2019). **The Age of Surveillance Capitalism**. **PublicAffairs**.
3. **O'Neil, C**. (2016). **Weapons of Math Destruction**. **Crown**.
4. **China State Council**. (2017). **New Generation Artificial Intelligence Development Plan**.
5. **Rahimi, F., & Shafiei, A**. (2022). **Ethical challenges of AI in healthcare in Iran**. **Iranian Journal of Medical Ethics**, 15(2), 45-52.

آمادگی الکترونیکی (بخش اول)

رقیه قاسمپور
دانشجوی دکتری تخصصی جامعه شناسی گرایش بررسی مسائل ایران
مسئول واحد بررسی اسناد و مدارک دانشگاه

آمادگی الکترونیکی

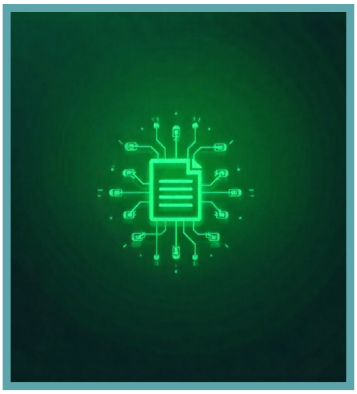
آمادگی الکترونیک از ظرفیت‌هایی صحبت می کند که جهان دوم را به موازات جهان اول آماده سازی می‌کند. در نگاه کلی آمادگی الکترونیک به معنای استفاده از فناوری‌های ارتباطی و اطلاعاتی برای توسعه اقتصادی و رفاهی درون یک کشور است، این آمادگی تعیین کننده میزانی است که یک کشور، دولت یا بنگاه اقتصادی برای حصول منافع برآمده از فناوری‌های اطلاعاتی و ارتباطی قابلیت دارد.

آمادگی الکترونیکی در حوزه اسناد

منظور از آمادگی الکترونیکی در حوزه اسناد، اصولاً فرآیندی است که طی آن اسناد و مدارکی که دیگر مورد استفاده قرار نمی‌گیرند، با هدف امکان دسترسی به آنها در آینده ذخیره و طبقه‌بندی می‌شوند. این فرآیند اگر به صورت الکترونیکی و دیجیتالی انجام شود، بایگانی الکترونیکی نامیده می‌شود. در روش سنتی و دستی، بایگانی اسناد در سازمان‌ها توسط واحد بایگانی یا دبیرخانه انجام می‌شد، اما با پیاده‌سازی سیستم بایگانی الکترونیکی، بیشتر مراحل آن به صورت خودکار و توسط نرم افزار انجام می‌شود.

ذخیره‌سازی و طبقه‌بندی اسناد برای هر سازمانی ضروری است. اما بایگانی دستی انبوه عظیم اسنادی که روزانه در سازمان‌ها رد و بدل می‌شوند، سرعت و زمان زیادی را خواهد گرفت. برای حل این مشکل کافیست تا از نرم افزارهای سازمانی برای الکترونیکی کردن بایگانی استفاده گردد. به این ترتیب می‌توان ضمن مدیریت اسناد از مزایای دیجیتالی کردن آنها نیز بهره برد.
بایگانی الکترونیکی به این معنا می‌باشد، که تمامی اطلاعاتی که در روش سنتی بر روی کاغذ ثبت شده بودند، به اطلاعات الکترونیکی تبدیل شده و بر روی یک سیستم کامپیوتری ذخیره می‌شوند. تبدیل اسناد کاغذی به داده های الکترونیکی به این صورت است، که اسناد کاغذی با استفاده از یک اسکنر، اسکن شده و به صورت الکترونیکی در سیستم ذخیره می‌گردد.
در بایگانی الکترونیکی، اسناد برای طولانی مدت به صورت دیجیتالی ذخیره و طبقه‌بندی می‌شوند. از

سوی دیگر، کلمه آرشیو نیز به مجموعه اسناد بایگانی شده گفته می‌شود. آرشیو دیجیتال نیز مجموعه اسنادی است که از طریق عکسبرداری یا اسکن به اسناد دیجیتال تبدیل شده و یا از ابتدا به صورت دیجیتال بوده و در سیستم ذخیره‌سازی شده‌اند.



بایگانی الکترونیکی مزایای متعددی دارد، اما آنچه باعث اهمیت آن می‌شود، ضرورت استفاده از آن در عصر دیجیتال است. با توجه به افزایش نقش کامپیوتر و دیجیتالی شدن بسیاری از کارها، استفاده از بایگانی به روش سنتی نه تنها دیگر کارآمد نیست، بلکه در فرآیند دیجیتالی انجام کارها اختلال و گسست ایجاد می‌کند. همچنین، بسیاری از محتواها و اسنادی که در سازمان‌های امروزی تولید می‌شوند، اساساً از ابتدا دیجیتال هستند و بایگانی آنها به صورت کاغذی نیازمند چاپ مجدد آنهاست. این مساله در مورد برخی از اسناد مانند پایگاه‌های داده، فیلم‌ها، فایل‌های صوتی و تصاویر عملاً غیرممکن است. به عبارتی، دیجیتالی شدن زندگی و فعالیت‌های کاری بشر موجب ایجاد سیستم جدیدی شده است که استفاده از سیستم‌های سنتی را به مراتب مشکل‌تر از گذشته کرده است. بنابراین سازمان‌هایی که بر استفاده از بایگانی کاغذی اصرار بورزند، باید هزینه گزافی برای آن پرداخت کنند و بیش از پیش از رقبای خود عقب خواهند ماند. علاوه بر اینها، بایگانی دیجیتال محدودیت عمر بایگانی‌های کاغذی را نخواهند داشت و آنچه امروزه ذخیره می‌شود در آینده‌های دور نیز در دسترس خواهند بود. بایگانی الکترونیکی همچنین، ضعف‌های بایگانی کاغذی را در برابر بلایای طبیعی ندارد و به دلیل پوسیدگی یا عدم مراقبت دائمی از بین نخواهند رفت.

البته آرشیوهای الکترونیکی نیز نیاز به مراقبت های اولیه دارند، اما آنچه ماندگاری آنها را بیشتر می‌کند، پشتیبان‌گیری راحت از آنهاست. می‌توان به راحتی از آرشیو دیجیتالی، چندین نسخه پشتیبان تهیه کرد ولی تهیه نسخه پشتیان از بایگانی کاغذی هزینه بسیار گزافی خواهد داشت. آرشیوهای الکترونیکی امنیت مورد نیاز سازمان ها را نیز فراهم می‌کند و امکان کنترل بهتری را بر روی اسناد و دسترسی افراد به آنها فراهم می‌کنند.

بایگانی الکترونیکی علاوه بر ذخیره‌سازی و طبقه‌بندی اسناد، فواید دیگری نیز دارد که در سیستم‌های بایگانی سنتی مشاهده نمی‌گردد. در ادامه تعدادی از این مزایا آورده شده است:

۱. افزایش ایمنی داده‌ها: اسناد و مدارک فیزیکی همیشه در معرض خطر و آسیب قرار دارند. آتش‌سوزی، سیل یا هر اتفاق ناگوار مشابه همیشه می‌تواند یک تهدید برای بایگانی سازمان باشد. اما با الکترونیکی کردن بایگانی اسناد و سوابق، می‌توان چنین مشکلی را برطرف کرد. اطلاعات دیجیتالی می‌تواند با خیال راحت در مکان‌ها متعددی ذخیره شود و نگران هزینه‌های هنگفت بازیابی اطلاعات از دست رفته نبود.
۲. کارایی و سرعت بیشتر: پیدا کردن یک سند در میان انبوه اسناد کاغذی ساده‌ترین راه برای اتلاف وقت و انرژی است! بخش قابل توجهی از ساعات کاری در واحدهای دبیرخانه سنتی، فقط برای یافتن اسناد صرف می‌شود. هرچند گاهی به دلایل قانونی، سازمان ممکن است نیاز به نگهداری نسخه کاغذی و اصلی اسناد داشته باشد، اما برای فرآیندهای داخلی سازمان نیازی به اسناد کاغذی نخواهد بود. بنابراین با دیجیتالی کردن بایگانی سازمان، می‌توان اسناد مورد نیاز را در عرض چند ثانیه پیدا کرده و بازیابی نمود. بنابراین هم سرعت و هم کارایی افزایش پیدا می‌کند.
۳. نیاز به فضای کمتر: قیمت املاک و اجاره آنها هر روز بیشتر می‌شود. اگر قرار به استفاده از اسناد کاغذی باشد، میزان محیطی که برای ذخیره فیزیکی آنها نیاز است، روز به روز افزایش پیدا می‌کند. این موضوع باعث می‌شود هزینه‌های زیادی به سازمان تحمیل شود. با الکترونیکی کردن بایگانی اسناد، تنها با استفاده از یک هارد دیسک کوچک می‌توان تعداد بسیاری زیادی از اسناد را با ایمنی بالا ذخیره نمود.

۴. بازیابی راحت‌تر اسناد و مدارک: الکترونیکی کردن بایگانی، بازیابی اسناد و مدارک را نیز آسان می‌کند. یکی از ساده‌ترین علت‌های آن امکان دسترسی به اطلاعات از هر زمان و مکان است. برای این کار کافیست تا یک درگاه جستجوی آنلاین برای آرشیو دیجیتالی وجود داشته باشد. به این‌ترتیب از هر مکان و زمانی می‌توان با یک جستجوی ساده، اسناد و مدارک مورد نیاز را بازیابی کرد.
۵. صرفه‌جوئی در هزینه‌ها: شرکت‌ها و سازمان‌ها زیادی به الکترونیکی کردن سیستم بایگانی روی آورده‌اند. علت اصلی این موضوع نیز صرفه‌جویی در هزینه‌هاست. روش سنتی بایگانی نیازمند تعداد زیادی نیروی انسانی و حجم زیادی کاغذ است. بنابراین با الکترونیکی کردن بایگانی نه تنها به محیط زیست کمک می‌گردد، بلکه تا مقدار زیادی در هزینه‌های سازمان صرفه‌جویی خواهد شد.

همچنین دیجیتالی کردن فرآیند بایگانی مستلزم توجه به نکاتی است که در ادامه به برخی از مهم‌ترین موارد آنها اشاره می‌شود.

۱. صرفه اقتصادی: ابتدایی‌ترین نکته‌ای که باید به آن توجه کرد این است که آیا الکترونیکی کردن بایگانی توسط خود سازمان به‌صرفه خواهد بود یا خیر. اگر تعداد اسنادی که نیاز به بایگانی آنها وجود دارد کمتر از هزار سند باشد، می‌توان بایگانی دیجیتالی آنها را برون‌سپاری کرد. اما اگر سندهای زیادی وجود دارد و هر روز بر تعداد آنها افزوده می‌شود، بهتر است به دنبال یک سیستم حرفه‌ای برای بایگانی دیجیتال در سازمان بود.
۲. انتخاب سخت افزار مناسب: برای دیجیتالی کردن بایگانی، نیاز به سخت افزارهای مناسب کامپیوتری است. در این مرحله باید تصمیم گرفته شود که آیا این سخت افزارها تهیه خواهد شد یا اینکه از سیستم‌های ابری استفاده خواهد گردید. در هر حال هنگام انتخاب سخت افزار باید به ویژگی‌های آن توجه گرددد و اطمینان حاصل شود که تمام نیازهای نرم افزار بایگانی دیجیتال را برای ذخیره‌سازی و حفظ اسناد برآورده می‌کند.
۳. قابلیت یکپارچه سازی با اتوماسیون اداری: نرم افزار اتوماسیون اداری برای مدیریت روزانه اسناد و مکاتبات سازمان‌ها به کار می‌روند و در بسیاری موارد به ذخیره‌سازی و بایگانی اطلاعات کمک می‌کنند. با این حال، ابزارهای سیستم‌های اتوماسیون برای بایگانی و مدیریت اسناد محدود است و پیچیدگی‌های سیستم‌های مدیریت اسناد (**DMS**) را ندارند. بنابراین بهتر است نرم‌افزاری انتخاب شود که بتواند با اتصال به سامانه اتوماسیون، اسناد روزانه را دریافت و بایگانی کند. یا در صورت لزوم بتواند مستقیما از داخل اتوماسیون، اسنادی را که به آنها نیاز است بازیابی کند.
۴. تحت وب بودن: یکی از ویژگی‌هایی که برای بیشتر نرم افزارهای اداری ضروری است، تحت وب بودن است. اگر نرم افزار بایگانی تحت وب باشد، می‌توان به راحتی از هر مکان و زمانی به آن دسترسی پیدا کرد. به علاوه برای استفاده از آن محدودیت سخت افزار یا سیستم‌عامل خاصی وجود ندارد و کافیست تا با یک مرورگر به آدرس اینترنتی آن متصل شد. در این صورت، برای ایجاد تغییرات در سیستم‌های کامپیوتری و نرم افزاری سازمان محدودیت‌های کمتری وجود خواهد داشت.
۵. ذخیره‌سازی و قابلیت جستجو: یک نرم افزار بایگانی باید بتواند اسناد را به اشکال و ترتیب‌های مختلفی سازماندهی کند. به علاوه باید قابلیت‌های مناسبی برای جستجو در میان اسناد در اختیار قرار بدهد.
۶. ساده‌تر کردنِ پیروی از قوانین: اسناد و مدارک نقش مهمی در ایفای وظایف حقوقی سازمان‌ها مثلاً برای ارائه گزارش‌های مالیاتی دارند. هر چند قوانین مربوط به اسناد در

کشورهای مختلف متفاوت هستند، اما در میان تمامی آنها ۲ ویژگی مشترک وجود دارد: اسناد باید به موقع ارائه شوند و قابلیت دستکاری نداشته باشند. به علاوه در برخی کشورها ممکن است استانداردهای خاصی برای امنیت اسناد و طرز کار نرم افزارهای بایگانی وجود داشته باشد که باید به آنها توجه گردد.

۷. ساختار ایمنی قوی: ابتدایی‌ترین کار برای حفاظت از اسناد و مدارک سازمانی در یک سیستم بایگانی دیجیتال، تهیه نسخه پشتیبان از آنهاست. با این حال اتفاقات غیرمترقبه بسیاری می‌توانند آرشیو اسناد بایگانی شده را به خطر بیندازند. این اتفاقات می‌تواند شامل نقص و خرابی سخت‌افزارها، آتش‌سوزی، سوانح طبیعی و حتی هک شدن سیستم‌ها باشد. بنابراین هنگام استفاده از نرم افزار بایگانی باید روش مطمئنی برای پشتیبانی منظم و چندلایه از داده‌ها و اسناد سازمانی دنبال گردد.

اصول بایگانی الکترونیکی شامل موارد زیر می‌باشد:

- اصل قابلیت انعطاف: بر طبق این اصل، سیستم بایگانی باید این قابلیت را داشته باشد که با تغییر و تحولات مختلف سازگار باشد.
- اصل آسان بودن: سیستم بایگانی باید ساده و آسان باشد، و افراد مختلف بتوانند نحوه تنظیم مدارک و بایگانی اسناد را به آسانی و با سرعت زمان اندک درک کنند.
- اصل قابلیت اجرا: اصل قابلیت اجرا به این معنی می‌باشد که، سیستم آرشیو باید با توجه به نوع کار و امکاناتی که موجود است، بتوان آن را پیاده‌سازی نمود.
- اصل سرعت و دقت: سیستم آرشیو باید به گونه ای باشد که ضمن اینکه اسناد و مدارک با دقت ذخیره می‌شوند، با سرعت قابل دستیابی باشند.
- اصل افراد با صلاحیت: افرادی که کار بایگانی را انجام می‌دهند، باید مهارت و صلاحیت کافی برای انجام این کار را داشته باشند.
- اصل نظم اصولی و منطقی: در انجام امور بایگانی اسناد باید نظم و اصول خاصی همچون وجود ارتباط منطقی بین عنوان پرونده‌ها، نظم در شماره و تاریخ اسناد، حذف کپی‌های اضافی از اسناد رعایت شود.

تکنولوژی OCR چیست؟

تکنولوژی **OCR** ابزاری قدرتمند برای تبدیل تصاویر حاوی متن به فایل‌های قابل ویرایش است. با استفاده از این فناوری، نیازی به تایپ مجدد اسناد و متون نیست **OCR** با شناسایی حروف و اعداد در تصاویر اسکن شده یا عکس‌ها، آن‌ها را به متن قابل جستجو تبدیل می‌کند. این تکنولوژی در حوزه‌های مختلفی مانند اسناد اداری، کتابخانه‌ها، خودروهای خودران و بسیاری از صنایع دیگر کاربرد دارد.
در واقع این تکنولوژی به شما در تشخیص و شناسایی حروف و اعداد، در تصاویر اسکن شده و یا حتی نسخه فیزیکی چاپی کمک می‌کند.
فناوری او سی آر در فارسی به نام‌های نسخه‌خوانی نوری و فناوری تشخیص متن ترجمه و شناخته می‌شود، با دانلود نرم افزار **OCR** و استفاده از آن می‌توان در کوتاه‌ترین زمان، تصاویر را به متون قابل جست‌وجو تبدیل کرد و در آخر فایل دیجیتالی که حاوی متن مورد نظر کاربر می‌باشد را دریافت نمود.

OCR مخفف چیست؟

OCR مخفف و کوچک شده (**Optical Character Reader**) به معنای کاراکترخوان نوری می‌باشد، این فناوری با نام تکنولوژی (**Recognition text**) نیز شناخته می‌شود.

اهمیت نویسه خوانی نوری

اهمیت نویسه خوانی نوری یا تکنولوژی **OCR** در این است که یک فایل تصویری، حجم زیادی دارد و جستجوی متنی در آن ممکن نمی‌باشد، در حالی که فایل خروجی سامانه نویسه خوان نوری بسیار کم حجم و قابل جستجو است، بحث صرفه جویی در زمان نیز در او سی آر بسیار اهمیت دارد، علاوه بر آن **OCR** دارای مزایا و فوایدی است که بر اهمیت استفاده از این فناوری اضافه می‌کند.

شیوه عملکرد تکنولوژی OCR چگونه است؟

تکنولوژی **OCR** و نرم‌افزارهایی که مجهز به آن هستند، از نحوه کار مشخصی برخوردارند. نحوه کار تکنولوژی **OCR** بسیار آسان و راحت می‌باشد و هر کاربری می‌تواند از قابلیت‌ها استفاده کند، همانطور که دانستیم، هدف این سیستم تجزیه و تحلیل محتوای یک سند فیزیکی و تبدیل عناصر آن به متون قابل استفاده برای پردازش داده می‌باشد.
بنابراین ابتدا تصاویری که دارای متن و نوشته خاصی هستند توسط دستگاه اسکنر و یا دوربین، اسکن شده و وارد رایانه می‌شوند، به این ترتیب تصاویر مربوطه به عنوان یک فایل گرافیکی قابل استفاده هستند.
در مرحله بعد کار اصلی نرم افزار **OCR** شروع می‌شود و فایل تصویری مورد نظر را تبدیل به فایل متنی کرده و آن را در یکی از قالب‌های متنی در کامپیوتر ذخیره می‌کند. در ادامه به صورت مجزا این مراحل را توضیح می‌دهیم.

- تبدیل شکل فیزیکی سند به یک تصویر: در اولین مرحله از فرآیند که به عبارتی پیش پردازش تصویر می‌باشد، او سی آر شکل فیزیکی سند را به یک تصویر تبدیل می‌کند، در مرحله اول باید دقت دستگاه بالا باشد و هر نوع انحراف یا خطای ناخواسته را حذف کند. در مرحله بعدی، تصویر به یک عکس سیاه و سفید تبدیل می‌شود و کاراکترها از طریق مناطق روشن و تاریک شناسایی و ارزیابی می‌شوند؛ بعد از آن تصویر با استفاده از یک سیستم **OCR** به بخش‌های جداگانه، مثل صفحات گسترده، متن یا گرافیک تقسیم می‌شود.
- تشخیص کاراکترها و اعداد از طریق هوش مصنوعی: با کمک هوش مصنوعی بخش‌های تاریک تصویر تجزیه و تحلیل می‌شود تا بتوان کاراکترها و اعداد را تشخیص داد.
- اصلاح ایرادهای فایل نهایی: در آخر هوش مصنوعی نقص‌ها و ایرادات فایل نهایی را هنگام پردازش مجدد اصلاح می‌کند، یکی از روش‌های مؤثر برای دقیق‌تر بودن خروجی این مرحله، آموزش لغت‌نامه و اصطلاحات مرتبط به متن به هوش مصنوعی می‌باشد.

در نهایت هم باید خروجی هوش منصوعی به کلمات یا فرمت‌های مدنظر محدود شود تا تغییرات و تشخیص‌های هوش مصنوعی از واژه‌ها، فراتر از کلمات مورد نظر کاربر نباشد.

خطاب به مخاطبان «پالسی نو»

اکنون که سومین شماره «**پالسی نو**» در اختیار شماست، بیش از پیش به همراهی و همفکری شما دلگرمیم. رسالت این نشریه فراتر از انتشار چند مقاله و یادداشت است؛ ما باور داریم که «**پالسی نو**» تنها در پرتو تعامل سازنده با شما معنا پیدا می‌کند.

از شما مخاطبان گرامی دعوت می‌کنیم با نقدهای سازنده، پیشنهادهای ارزشمند و مطالب ارزنده خود، در مسیر پویاتر شدن این رسانه شریک باشید. ما صمیمانه مشتاقیم تا دیدگاه‌ها و دغدغه‌های شما را بشنویم و آنها را در شماره‌های آینده بازتاب دهیم.

بیایید با هم نشریه‌ای بسازیم که نه تنها بازتاب‌دهنده اندیشه‌ها و تجربیات امروز باشد، بلکه چراغی برای فردای روشن‌تر در حوزه نوآوری، فناوری و سیاست‌گذاری نیز گردد.

«**پالسی نو**» خانه‌ای است برای گفت‌وگوی شما

آدرس وب سایت نشریه:

anp.tbzmed.ac.ir

آدرس ایمیل برای ارسال مطالب:

anp@tbzmed.ac.ir

صفحه اینستاگرام:

anew_pulse

کاربرد فناوری‌های نوین در آموزش بهداشت و ارتقای سطح سلامت جامعه

دکتر زینب جوادی والا
دکتری تخصصی آموزش و ارتقا سلامت
رئیس مرکز آموزش هوشمند
استادیار گروه آموزش بهداشت و ارتقای سلامت

چکیده

در دهه اخیر، تغییرات فناورانه گسترده‌ای در شیوه‌های آموزش سلامت رخ داده است. ابزارهایی همچون هوش مصنوعی، واقعیت مجازی، اپلیکیشن‌های موبایلی، و سامانه‌های یادگیری الکترونیکی، شکل سنتی آموزش بهداشت را دگرگون کرده‌اند. این فناوری‌ها از یک‌سو امکان ارائه آموزش‌های تعاملی و شخصی‌سازی‌شده را فراهم می‌کنند و از سوی دیگر، بستر داده‌محور و پایدار برای پایش اثر بخشی مداخلات آموزشی در سطح جامعه ارائه می‌دهند.
این مقاله با مروری بر کاربرد این فناوری‌ها، نشان می‌دهد چگونه می‌توان از ظرفیت‌های نوین برای افزایش سواد سلامت، تغییر رفتار و ارتقای عدالت در دسترسی به خدمات آموزشی بهره برد.

مقدمه

در جهانی که روزبه‌روز شاهد رشد بیماری‌های غیرواگیر، بحران‌های بهداشت روان، آلودگی‌های زیست‌محیطی، و تهدیدات همه‌گیر هستیم، توانمندسازی مردم برای درک و مدیریت سلامت خود از اهمیت فزاینده‌ای برخوردار است.
آموزش بهداشت به عنوان رکن کلیدی ارتقاء سلامت، باید از شیوه‌های سنتی مانند کلاس‌های حضوری یا بروشورهای چاپی فراتر برود و با نیازهای روز و سبک زندگی دیجیتال تطبیق یابد.
آموزش بهداشت اساس ارتقای سلامت جامعه و پیشگیری از بیماری‌ها است. با وجود این، روش‌های سنتی آموزش، اغلب محدود به کلاس‌های حضوری یا رسانه‌های عمومی بوده و در ایجاد تغییر پایدار در رفتارهای فردی و اجتماعی چندان کارآمد نبوده‌اند. فناوری‌های نوین می‌توانند این محدودیت‌ها را برطرف کرده و تجربه‌های آموزشی جذاب، فراگیر و اثرگذار ایجاد کنند.

برخی از انواع فناوری‌های نوین و کاربرد آنها

فناوری‌های نوین این ظرفیت را دارند که آموزش بهداشت را از یک فعالیت منفعل، به فرآیندی مستمر، پویا، جذاب و متناسب با شرایط فردی و فرهنگی هر گروه هدف تبدیل کنند. در این بخش برخی از متداولترین انواع فناوریها در آموزش بهداشت آورده شده است.

۱. اپلیکیشن‌ها و پلتفرم‌های دیجیتال
- برنامه‌های **mHealth** برای پایش شاخص‌های سلامت و آموزش سبک زندگی سالم.
- پلتفرم‌های آموزش آنلاین با محتوای چندرسانه‌ای و تعاملی برای گروه‌های مختلف سنی.
- شبکه‌های اجتماعی برای اجرای کمپین‌های سلامت و آموزش همگانی.

۲. واقعیت مجازی (**VR**) و واقعیت افزوده (**AR**)
- شبیه‌سازی محیط‌های آموزشی برای دانشجویان و کارکنان حوزه سلامت.
- آموزش کودکان و نوجوانان با استفاده از بازی‌ها و انیمیشن‌های مبتنی بر **AR**.

۳. هوش مصنوعی و یادگیری ماشین
- طراحی آموزش‌های شخصی‌سازی‌شده بر اساس نیازهای بهداشتی فرد.
- چت‌بات‌ها و دستیارهای مجازی برای پاسخ به پرسش‌های عمومی مردم.
- تحلیل داده‌های رفتاری برای شناسایی گروه‌های پرخطر و مداخله آموزشی هدفمند.

۴. اینترنت اشیا (**IoT**) و ابزارهای پوشیدنی
- ساعت‌های هوشمند و مچ‌بندهای سلامت که با نمایش اطلاعات در لحظه، رفتار فرد را اصلاح می‌کنند.
- دستگاه‌های **IoT** خانگی (مثل ترازوهای هوشمند و دستگاه‌های پایش فشار خون) که به کاربران و پزشکان امکان

تحلیل و آموزش رفتارهای سالم را می‌دهند.

- پایش از راه دور بیماران مزمن و آموزش همزمان برای خودمراقبتی.

۵. گیمیفیکیشن (**Gamification**) در آموزش بهداشت

- استفاده از مکانیزم‌های بازی مانند امتیاز، مدال و رقابت برای تشویق افراد به رعایت اصول بهداشتی.
- نمونه‌ها: اپلیکیشن‌هایی که کودکان را به مسواک‌زدن منظم، یا بزرگسالان را به افزایش فعالیت بدنی ترغیب می‌کنند.
- مزیت اصلی: افزایش انگیزه درونی و پایدارسازی رفتارهای سالم از طریق لذت و تعامل.

اثرات کلان فناوری‌های نوین بر ارتقای سلامت جامعه

یکی از مهم‌ترین نقش‌هایی که فناوری می‌تواند در بهبود کیفیت زندگی داشته باشد، ارائه خدمات بهداشتی جدید است. فناوریهای نوین پزشکی کمک می‌کنند بیماری‌ها به شکل دقیق‌تر و موثرتری تشخیص داده شده و درمان شوند. همچنین فناوری، شیوه های آموزش را نیز متحول کرده است و کیفیت زندگی افراد را با ایجاد امکان دسترسی به منابع و فرصت‌های آموزشی بهبود بخشیده است. جدول ۱ چالشها و راهکارهای کاربرد این فناوری ها را نشان می دهد. به طور خلاصه برخی از تاثیرات فناوریهای نوین در ارتقای سلامت جامعه به شرح زیر می باشد:

- افزایش سواد سلامت در میان اقشار مختلف.
- اصلاح رفتارهای ناسالم (مثل کاهش مصرف دخانیات یا بهبود الگوی تغذیه).
- عدالت در سلامت از طریق دسترسی همه‌جانبه به آموزش حتی در مناطق محروم.
- کاهش هزینه‌های نظام سلامت با تمرکز بر پیشگیری به جای درمان.

چالش	راهکار پیشنهادی
شکاف دسترسی به اینترنت	توسعه زیرساخت ارتباطی در مناطق روستایی و کم‌برخوردار
فقدان سواد دیجیتال	آموزش سواد رسانه‌ای و دیجیتال در نظام آموزش عمومی
محتوای غیربومی یا بی‌کیفیت	تولید محتوای چندرسانه‌ای با مشارکت دانشگاه‌ها، متخصصان پزشکی، و طراحان تجربه کاربری
نگرانی‌های امنیت اطلاعات	تدوین چارچوب حقوقی حفاظت از داده‌های سلامت در اپلیکیشن‌ها و سامانه‌ها
ارزیابی ضعیف مداخلات	طراحی مکانیزم‌های پایش، تحلیل داده و بازخورد مستمر در هر ابزار فناورانه

نتیجه‌گیری

فناوری‌های نوین در آموزش بهداشت، چشم‌انداز جدیدی برای ارتقای سلامت جامعه گشوده‌اند. ادغام گیمیفیکیشن، اینترنت اشیا، اپلیکیشن‌های سلامت، واقعیت مجازی و هوش مصنوعی می‌تواند آموزش‌های بهداشتی را اثربخش‌تر، جذاب‌تر و ماندگارتر سازد. آینده آموزش بهداشت به سمت ترکیب این فناوری‌ها و طراحی راهکارهای یکپارچه خواهد بود؛ مسیری که می‌تواند همزمان سطح آگاهی عمومی، کیفیت زندگی و عدالت در سلامت را ارتقا دهد.

منابع

1. World Health Organization. (2021). Global strategy on digital health 2020–2025. WHO.
2. Free, C., et al. (2013). The effectiveness of mobile-health technology-based health behaviour change or disease management interventions: a systematic review. PLoS Medicine.
3. Gentry, S. V., et al. (2019). Virtual reality and augmented reality in medical education: A systematic review. BMJ Open.
4. Sardi, L., Idri, A., & Fernández-Alemán, J. L. (2017). A systematic review of gamification in e-Health. Journal of Biomedical Informatics.
5. Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of Things for health care: A comprehensive survey. IEEE Access.
6. نقش تکنولوژی در بهبود کیفیت زندگی – ایریسا. https://www.irisaco.com/role-of-technology-in-life-quality

آموزش فناوری اطلاعات:
مبانی هک اخلاقی
بخش سوم

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

در آموزش قبلی به مراحل و فازهای هک اخلاقی پرداخته شد که شامل **Footprinting**، **Enumeration** ، **Scanning** و **System Hacking** بودند. در این بخش از آموزش به شکلی عمیق تر به فاز **Footprinting** با هدف گردآوری داده خواهیم پرداخت.

Footprinting اولین و بنیادی‌ترین مرحله در هر آزمون نفوذ یا عملیات هک اخلاقی است. در این فاز، شما به عنوان هکراخلاقی سعی می‌کنید حداکثر اطلاعات ممکن را درباره هدف خود، به صورت غیرمخرب و غیرفعال (بدون ارسال حتی یک بسته داده به سمت هدف) جمع‌آوری کنید. به زبان ساده این فاز مانند نقشه‌برداری و شناسایی منطقه قبل از حمله به یک قلعه است. هرچه اطلاعات شما دقیق‌تر باشد، مراحل بعدی موثرتر خواهند بود.

هدف اصلی، درک گستره (**Scope**) حمله و ایجاد یک نمایه کامل از سازمان هدف است. شما به دنبال پاسخ این سوالات خواهید بود:

سازمان هدف چه چیزهایی را در اینترنت نمایان کرده است؟

- دامنه‌های آن چیست؟
- آدرس‌های **IP** آن چیست؟
- شبکه‌های آن چگونه است؟
- چه افرادی در آن کار می‌کنند؟ (برای مهندسی اجتماعی)
- از چه تکنولوژی‌هایی استفاده می‌کند؟ (مثلاً نوع وب سرور، سیستم عامل)

انواع Footprinting:

- غیرفعال (**Passive**): در این روش، هیچ ترافیک و داده ای مستقیماً به سمت سیستم‌های هدف ارسال نمی‌شود و اطلاعات صرفاً از منابع عمومی و در دسترس جمع‌آوری می‌شود. لذا شناسایی و ردیابی آن برای هدف بسیار دشوار است. برای مثال جستجو در گوگل و بررسی پست‌های شبکه‌های اجتماعی از سازمان هدف نمونه هایی رایج از گردآوری اطلاعات به شکل غیرفعالانه می باشد.
- فعال (**Active**): در این روش، ترافیک به سمت هدف ارسال می‌شود تا پاسخ هایی از سامانه های سازمان دریافت شده و اطلاعات بیشتری به دست آید. در این روش خطر شناسایی شدن وجود دارد، زیرا فعالیت شما ممکن است در لاگ‌ها و سامانه های امنیتی

و نظارتی سیستم هدف ثبت شود و توسط سامانه ها بلوکه شود. برای مثال: پینگ کردن یک سرور، انجام یک **query** در **DNS** از ساده ترین فعالیت ها در این زمینه می باشند.

در ادامه، مهم‌ترین تکنیک‌ها به همراه مثال و ابزارهای مربوطه آورده شده است:

۱ - جمع‌آوری اطلاعات از موتورهای جستجو (**Google Hacking / Dorking**)

موتورهای جستجو مانند **Google**، انبوهی از اطلاعات حساس را **index** کرده‌اند که ممکن است به صورت عمومی در دسترس باشند. برای مثال ممکن است صفحات و فایل‌های حاوی پسورد، اطلاعات لاگ، صفحات مدیریت، دوربین‌های تحت وب، اطلاعات خطاها و نام های کاربری و اطلاعات تماس افراد کلیدی در آن فهرست شده باشند. برای مثال جهت **Dork-ing** در یک سامانه یا سازمان خاص دستورات زیر در جستجوی پیشرفته آن استفاده می شوند و می توان پارامترها را با عملگرهای **AND** و **OR** نیز تلفیق نمود.

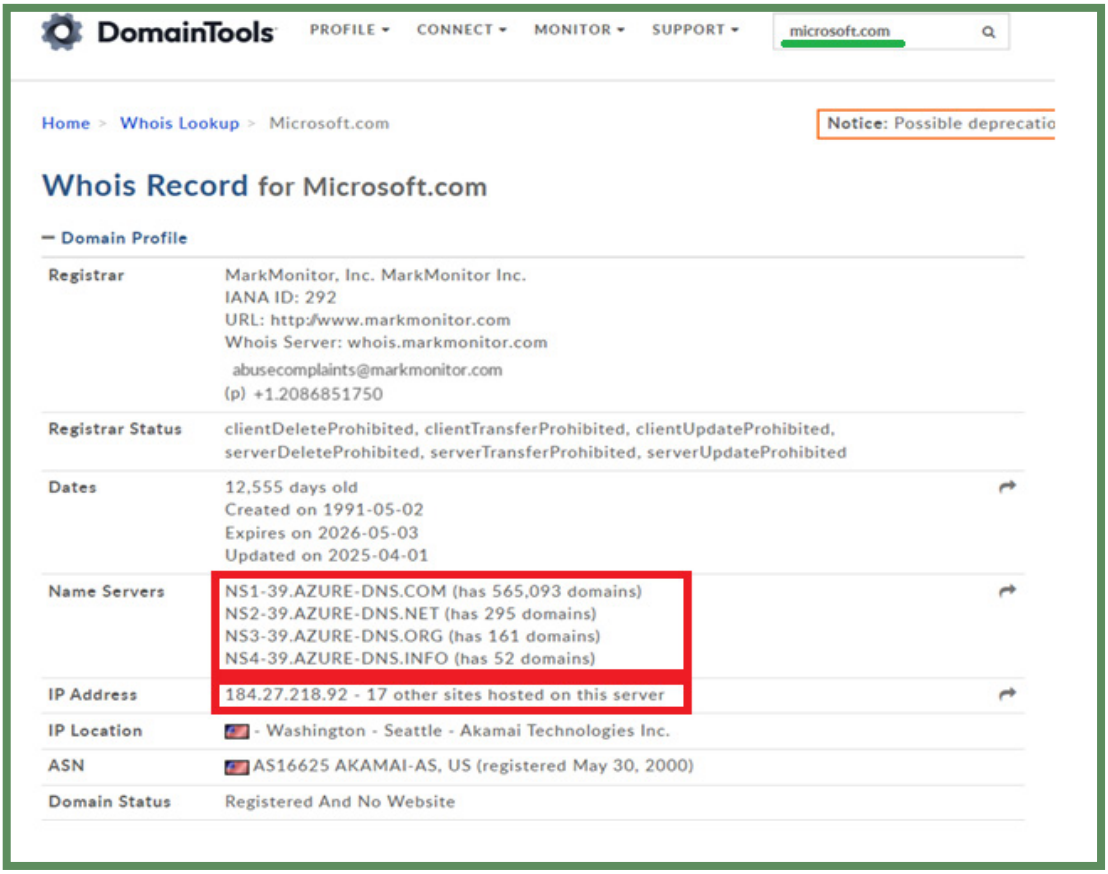
site: target.com	جستجو فقط در دامنه هدف
intitle: password	یافتن فهرست‌هایی که کلمه password در عنوان دارند
filetype: pdf	یافتن تمام فایل‌های PDF در یک سایت که ممکن است حاوی اطلاعات مهم کاربری یا لاگ ها باشند
inurl: admin / login.php	یافتن صفحات لاگین admin

برای مثال در سایت دانشگاه با جستجوی تصویر زیر نتایجی از صفحات **Login.aspx** که صفحات طراحی شده با تکنولوژی **ASP.Net** می باشد واکشی می شود و این صفحات می تواند اولین نقطه آسیب پذیری برای هکرهای کلاه سیاه با هدف آسیب به سازمان باشد.

در این زمینه هکر اخلاقی دارای خلاقیت و هوش به همراه تکنیک های حدس‌زنی ناشی از تجربه می تواند در یافتن اطلاعات حساس و کلیدی و پیشنهاد حذف یا عدم ایندکس آن در **Google** برای پیشگیری از آسیب های جدی به سازمان کمک کند.

۲ - جمع‌آوری اطلاعات با ابزارهای **WHOIS**

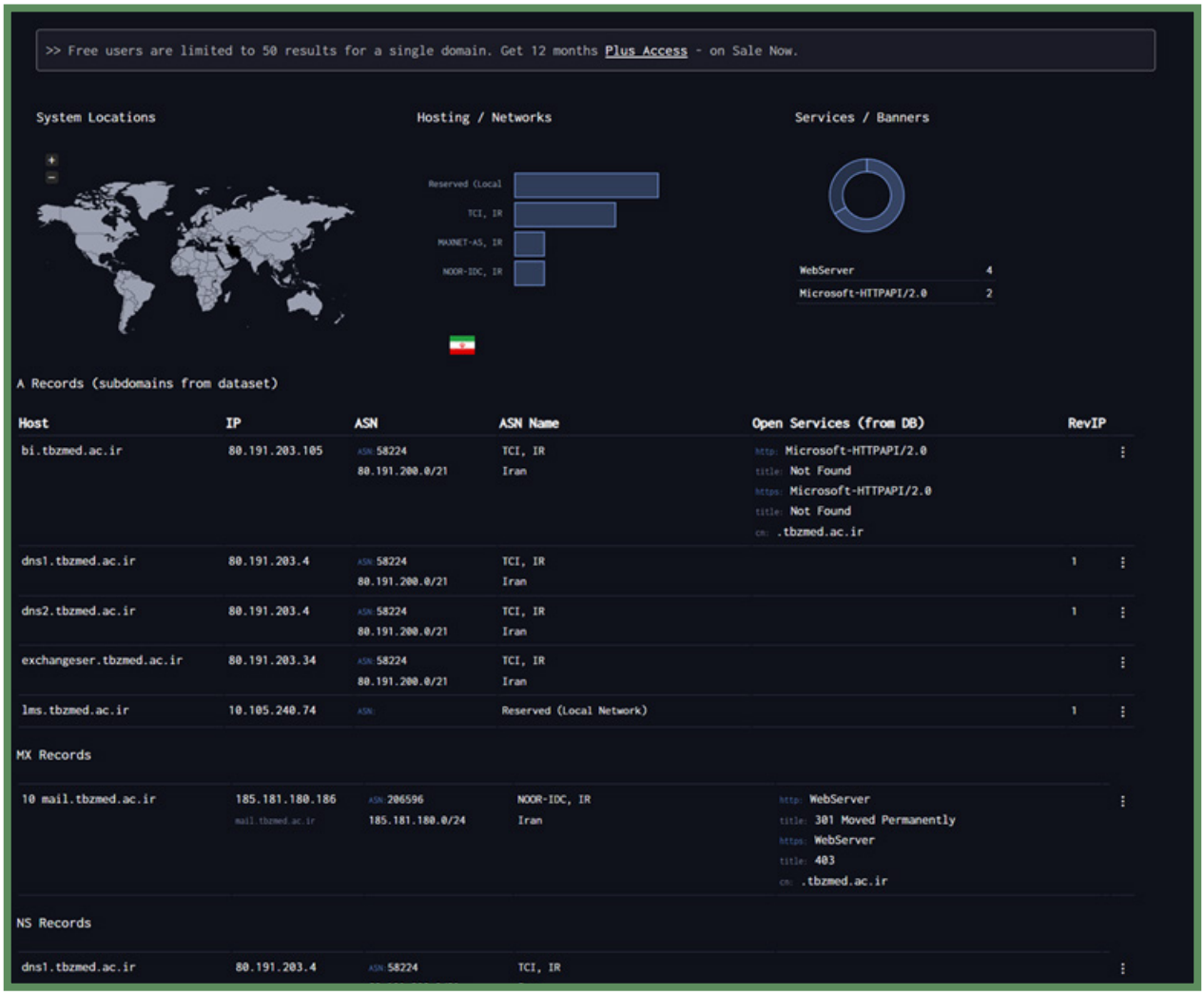
WHOIS یک پروتکل پایگاه داده است که اطلاعات ثبت‌کننده یک دامنه را نگهداری می‌کند. با فرآیند **WHOIS** می توان نام و اطلاعات تماس صاحب دامنه، تاریخ ثبت و انقضا، **Name Server** های دامنه را یافت. لذا می توان سرورهای مربوط به سامانه و اطلاعاتی از قبیل ایمیل و حتی تلفن تماسی از سازمان ثبت کننده را در اختیار گرفت و گام های بعدی را اجرا نمود. لذا رعایت پروتکل های امنیتی در این باب نیز می بایست از طرف هکر اخلاقی گوشزد شود.
ابزارهای متنوعی برای اجرای این فرآیند چه در دامنه های بین المللی از قبیل **net**. و **com**. و چه در دامنه های داخلی **ir**. وجود دارد. وب‌سایت‌های **whois** مانند **whois.icann.org** و **whois.domaintools.com** برای دامنه های بین المللی و **whois.irdomain.com** برای دامنه های ایرانی مورد استفاده قرار می گیرند. ضمن آنکه در لینوکس(به ویژه لینوکس کالی) و ویندوز ابزارهای قابل نصبی نیز وجود دارند که این کار را انجام می دهند. در تصویر زیر دامنه **Microsoft.com** مورد **WHOIS** قرار گرفته و اطلاعاتی در مورد آن واکشی شده است.



همانطور که مشاهده می شود اطلاعات ثبت کننده دامنه، تاریخ های ثبت و انقضا، **Nameserv-er** ها که محل قرار گیری داده ها را نشان می دهد و **IP** یا آدرس پروتکل اینترنتی وب سایت مایکروسافت که درآمریکا مستقر است قابل واکشی می باشد. اطلاعات محدود به این موارد نبوده و ایمیل، شماره تماس و شهر ثبت کننده را نیز شامل می شود.

۳ - بررسی **DNS** و نگاه کردن به **Record**های آن

DNS مانند دفترچه تلفن اینترنت است. استخراج **Record**های **DNS** اطلاعات حیاتی درباره زیرساخت شبکه به ما می‌دهد. انواع رکوردها در این زمینه قابل واکشی می باشد که **A** نشان دهنده **IP** سامانه، **MX** سرورهای ایمیل سازمان، **NS** سرورهای مسئول دامنه و **TXT** اطلاعات متنی از جمله تایید مالکیت یا تنظیمات امنیتی را شامل می شود. برای این منظور نیز ابزارهایی همچون دستور **nslookup** در ویندوز، **dig** در لینوکس و ابزارهای آنلاینی چون **dnsdumpster.com** بصورت رایگان در دسترس می باشند. لینوکس های امنیتی گفته شده در مطلب قبلی نیز ابزارهای اختصاصی دارند. برای مثال در بررسی سایت دانشگاه اطلاعات زیر مشاهده می شود که شامل رکوردهای مختلف و آدرس ها و نکات ریز قابل استفاده برای هکرها می باشد.



در این بخش بصورت خلاصه به سه روش گردآوری اطلاعات سازمان ها بصورت خلاصه پرداختیم. در نسخه بعدی به روشهای دیگر از جمله مهندسی اجتماعی اشاره خواهد شد و بصورت کاربردی تری از دستورات و واکشی اطلاعات بهره برداری خواهد شد.

ادامه دارد...

پیام مخاطب

محمدرضا عمرانی‌فر
کارشناسی ارشد مهندسی سازه
رئیس گروه کارشناسان ساختمان دانشگاه

سردبیر محترم پالسی نو،

با سلام و احترام،

انتشار مطالب اخیر نشریه در خصوص فناوری‌های نوظهور، به‌ویژه هوش مصنوعی، امنیت سایبری، دیجیتال توئین و چت‌بات‌های پزشکی، شایسته قدردانی است. پرداختن جامع به این موضوعات و بهره‌گیری از منابع معتبر علمی و بین‌المللی، نشان‌دهنده نگاه آینده‌نگرانه و رویکرد علمی **پالسی نو** است. همچنین تأکید بر نقش این فناوری‌ها در ارتقای کیفیت خدمات و بهبود مدیریت منابع، ارزش علمی و عملی مجله را برجسته‌تر ساخته است.

با وجود این نقاط قوت، به نظر می‌رسد تقویت برخی ابعاد می‌تواند بر غنای **پالسی نو** بیفزاید:

۱. افزودن داده‌ها و مطالعات موردی داخلی: استفاده از نمونه‌ها و آمار بومی دانشگاه، قابلیت اجرایی و انطباق گزارشات منتشر شده با شرایط کشور را افزایش خواهد داد.
۲. اولویت‌بندی چالش‌ها و راهکارها: مشخص ساختن حوزه‌های فوری و حیاتی، روند تصمیم‌گیری را تسهیل می‌کند.
۳. تحلیل ریسک و پیامدها: بررسی ابعاد فنی، قانونی و مالی همراه با ارائه راهکارهای کاهش ریسک، به سیاست‌گذاری مطمئن‌تر منجر می‌شود.
۴. بومی‌سازی محتوا: انطباق توصیه‌ها با زیرساخت‌ها، قوانین و منابع انسانی ایران، بر کارآمدی مطالب می‌افزاید.
۵. تدوین نقشه راه اجرایی: تفکیک اقدامات به کوتاه‌مدت، میان‌مدت و بلندمدت و تعریف شاخص‌های کلیدی عملکرد (**KPIs**) مسیر عملیاتی مشخصی فراهم می‌آورد.
۶. پایش و ارزیابی مستمر: اختصاص بخشی به ارزیابی دوره‌ای می‌تواند ضامن پایداری و ارتقای مستمر اقدامات باشد.

در پایان، شماره اخیر را باید گامی ارزشمند در مسیر توسعه مباحث فناورانه در حوزه سلامت دانست. امید است پیشنهادهای مطرح‌شده بتواند در ارتقای کیفیت و اثرگذاری شماره های آتی **پالسی نو**، سودمند واقع شود.

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

جواد فرهادی

کارشناس ارشد نرم افزار

وحید عباس‌زاده

دانشجوی PHD الکترونیک
کارشناس شبکه

الهام منقش

دانشجوی دکتری تخصصی مدیریت اطلاعات سلامت اطلاعات سلامت

صابر درس‌خوان

کارشناس ارشد شبکه
کارشناس مسئول زیرساخت

بابک زارع آبادی

کارشناسی پژوهشگری علوم اجتماعی
کارشناس فناوری اطلاعات مرکز تحقیقات مدیریت

دکتر زینب جوادی والا

دکترای تخصصی آموزش و ارتقا سلامت
رئیس مرکز آموزش هوشمند
استادیار گروه آموزش بهداشت و ارتقای سلامت

رقیه قاسمپور

دانشجوی دکتری تخصصی جامعه شناسی گرایش بررسی مسائل ایران
مسئول واحد بررسی اسناد و مدارک دانشگاه

سیدمحمدحسن الهی

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

A New Pulse

anew_pulse