



دریچه فناوری

تابستان ۱۴۰۳

گاهنامه شماره



در این شماره می خوانیم:

نسخه نویسی الکترونیکی

بلاک چین چیست؟

معرفی نرم افزار Prezi

و...



مدیر مسئول:

محمد شجاعی

سر دبیر:

امیریم شهبانی

اعضای هیئت تحریریه:

محمد شجاعی

الهام دهستانی

حمیدرضا کاوسی

امیریم شهبانی

طراحی و صفحه آرایی:

شیدانه پورادی حسینی

تأکیدات مهم مقام معظم رهبری
در خصوص فضای مجازی

۱

صراط

(قسمت چهارم)

۲

بلاکچین چیست؟

(قسمت اول)

۳

نسخه نویسی الکترونیکی

(قسمت اول)

۵

آشنایی با قانون جرایم رایانه ای

(قسمت اول)

۷

احراز هویت یکپارچه

یا Single Sign-On

۱۰

معرفی نرم افزار

پری

۸

ابزار هوش مصنوعی

(قسمت اول)

۱۲

فایروال

و سیاست های آن

۱۵

راه های ارتباطی:

پست الکترونیک: daricheh1401fannavari@chmail.ir

@daricheh_fannavari

شماره تماس: ۰۲۶۳۴۱۸۹۶۱۰



سازمان حراست کل کشور
حراست کل استان البرز



تأکیدات مهم مقام معظم رهبری (مدظله العالی)
در خصوص مدیریت فضای مجازی

ادب اسلامی با گسترش فضای مجازی کم رنگ می‌شود. (۱۵)
بهمن ماه سال ۱۳۹۹

«ادب اسلامی را در جامعه بگسترانید. عزیزان من! یکی از چیزهای بسیار مهم، حفظ ادب اسلامی در سخن گفتن است که متأسفانه امروزه با گسترش فضای مجازی به تدریج این ادب اسلامی دارد کم‌رنگ می‌شود. بدزبانی، بدگویی و مانند اینها باید در جامعه جمع شود. امروز بعضی سعی می‌کنند یا بی توجهی می‌کنند و این در جامعه، بخصوص در بعضی از رسانه‌ها چه رسانه‌های صوتی، چه رسانه‌های تصویری و به خصوص در فضای مجازی رو به گسترش است.»

فرصت فضای مجازی برای بصیرت آفرینی (۲۱ اسفند ماه سال ۱۳۹۹)

«امروز فضای مجازی یک فرصتی است برای این کار؛ حالا دشمنان از فضای مجازی جور دیگر استفاده می‌کنند. اما شما جوان‌های عزیز این جوری از آن استفاده کنید: از فضای مجازی استفاده کنید برای امیدآفرینی، برای توصیه به صبر، برای توصیه به حق، برای بصیرت‌آفرینی، برای توصیه به خسته نشدن، تنبلی نکردن، بیکار نماندن و مانند این‌ها. خب این در مورد این کار اول دشمن که قطع زنجیره تواصی و حفاظت از یکدیگر است.»



پیرمرد از پاسخ غیر منتظره و مبهم پیامبر(ص) مات و متحیر شده بود، با خود گفت: «از کدام آب؟ آیا از آب عراق؟»

رسول اعظم(ص) با این تاکتیک اطلاعاتی، ضمن کسب اخبار لازم، از معرفی خود و افشای اسرار نظامی جبهه خودی، خودداری ورزیدند.

همچنین در سربیه عبدالله بن جحش، رسول خدا(ص) فرمانی برای او نوشتند و دستور دادند تا دو روز راه نپیموده است، آن را نخواند. پس از آن در آن بنگرد و به مضمونش عمل کند. عبدالله پس از دو روز راه پیمایی نامه را گشود و در آن خواند: «هرگاه در نامه ام نگرستی، همچنان رهسپار شو تا در نخله میان مکه و طائف فرود آیی. آن جا در کمین قریش باش و اخبارشان را برای ما جست و جو کن.»

از این نقل تاریخی استفاده می شود که سیره آن حضرت در مقام حاکم اسلامی و فرمانده کل نظامی، اتخاذ تدابیری بوده است که اسرار نظامی را حفظ کند و از دسترس دشمن و حتی آحاد مسلمانان به این اسرار جلوگیری کند.

دو- سیره عملی: سیره عملی معصومان(ع) نیز نشان از تاکید بر لزوم حفظ اطلاعات دارد و از آن جا که رفتار آن بزرگواران برای ما حجت است، می توان دلالت آن ها را بر وجوب حفظ اسرار نظامی و حرمت افشای آن، اعم از نظامی و غیر نظامی به دست آورد.

در سیره پیامبر اعظم(ص) می خوانیم در نخستین نبرد بزرگ و سرنوشت ساز مسلمانان با مشرکان، یعنی نبرد بدر، پیامبر اعظم(ص) تصمیم به کسب خبر از موقعیت دشمن گرفتند. آن حضرت پس از مقداری پیشروی، به پیرمردی برخوردند و از وی موقعیت قریش و محمد و یارانشان را پرسیدند. پیرمرد گفت: شما را در جریان نخواهم گذاشت مگر آن که خود را معرفی کنید. حضرت فرمودند: اگر تو ما را مطلع سازی، ما نیز تو را مطلع خواهیم ساخت. پس از آن که پیرمرد اخبار لازم در خصوص موقعیت قریش و زمان حرکت و محل اردوگاه آنان و همچنین درباره لشکر اسلام را بیان کرد، از پیامبر اعظم(ص) خواست خود را معرفی کند. پیامبر اعظم(ص) که از سویی نمی خواستند خلف وعده کنند و از سوی دیگر مصلحت نمی دیدند خود را معرفی کنند، به پیرمرد فرمودند: «ما از آبیم» و بی درنگ دور شدند.



بلاکچین چیست؟

(قسمت اول)

همه چیز درباره فناوری بلاکچین

اگر بخواهیم مفاهیم اولیه و مهم بلاکچین را در یک جدول بیاوریم، به شکل زیر می‌شود:

فارسی	انگلیسی	توضیح
بلاک (بلوک)	Block	به فضاهایی که اطلاعات در آن ذخیره می‌شود بلاک گفته می‌شود
چین (زنجیره)	Chain	اساس قرارگیری بلاک‌ها را به صورت زنجیره یا چین بیان می‌کنند
بلاک چین (زنجیره بلوکی)	Blockchain	به بلاک‌های پشت سرهم زنجیره بلوکی (Blockchain) گفته می‌شود و تشکیل یک دفتر کل توزیع شده را برای ثبت اطلاعات می‌دهند.
دفتر کل توزیع شده	Distributed ledger	دفتر کل توزیع شده یک پایگاه غیرمتمرکز برای ثبت و نگهداری داده است. بلاک چین یکی از انواع دفتر کل توزیع شده است.

در عصر تکنولوژی، دیتا و اطلاعات حرف اول را می‌زنند و روزانه انبوهی از داده‌ها و اطلاعات در دنیای تکنولوژی تولید می‌شود. اما نگهداری، ثبت و استفاده درست از این اطلاعات است که بشر را به سمت پیشرفت و آسایش سوق می‌دهد؛ فناوری نوظهور Blockchain که از آن به عنوان بزرگترین اختراع بشر بعد از اینترنت یاد می‌شود، نقشی بزرگ در این راه ایفا می‌کند. تکنولوژی بلاکچین با ظرفیت‌های خود نشان داده که قصد کمک به هرچه سریع‌تر پیامودن این راه را دارد؛ اما به واقع فناوری بلاکچین چیست؟

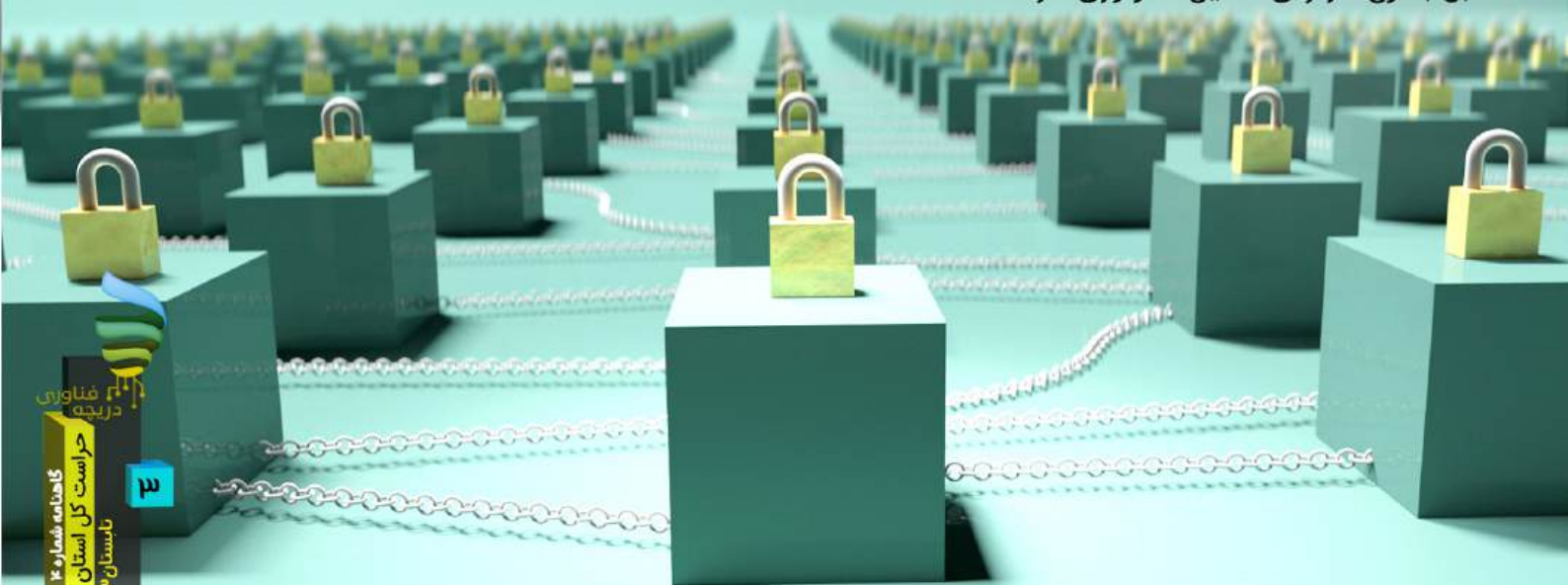
تاریخچه بلاکچین:

شاید یک از دلایلی که اکثراً بیت کوین را با بلاکچین یکی می‌دانند این باشد که تکنولوژی بلاکچین برای اولین بار در سال 2009 در کد برنامه‌نویسی بیت کوین معرفی شد. پس از آن علاوه بر بیت کوین، ارزهای دیگری توانستند از این فناوری استفاده کنند و کوین خود را راه اندازی کنند، بعدها با شناخت بیشتر و بهتر نسبت به این تکنولوژی، متخصصان دریافته‌اند که تنها استفاده و کاربرد بلاکچین ارزهای دیجیتالی نیست؛ بلکه این تکنولوژی کاربردهای فراوانی دارد. در نتیجه می‌توان در زمینه‌های مختلف از آن استفاده کرد. در حال حاضر بلاک چین‌هایی با کاربردهای متفاوت در حال به کارگیری هستند که هر کدام از آن‌ها متناسب با ویژگی‌هایشان، استفاده‌های متفاوتی دارند. اما برگردیم به سوال اساسی بلاکچین چیست؟

مفهوم بلاکچین با داغ‌تر شدن بازار ارزهای دیجیتال بیشتر بر سر زبان‌ها افتاد. اگرچه بلاکچین لزوماً به رمزارزها ارتباطی ندارد، اما بزرگترین رمزارزها (همچون بیت کوین و اتریوم) از تکنولوژی بلاکچین استفاده می‌کنند. بلاکچین را می‌توان به شکلی ساده، راهی برای ثبت و ذخیره اطلاعات به شکل گسترده و توزیع شده دانست. در این مقاله به زبان ساده به پرسش بلاکچین چیست پاسخ می‌دهیم، با ساختار آن آشنا خواهیم شد و در انتها به پرسش‌های رایجی که در زمینه فناوری زنجیره بلوکی مطرح شده، جواب خواهیم داد.

همانطور که در بالا اشاره شد، بلاکچین یک نوع دیتابیس (Database) یا پایگاه داده است. اما دیتابیس چیست؟ دیتابیس مجموعه‌ای از اطلاعات است که به صورت الکترونیکی در یک سیستم کامپیوتری ذخیره شده است؛ اما بلاکچین دیتا و اطلاعات را به روش جدیدی ذخیره می‌کند. در واقع یکی از اصلی‌ترین وجوه تفاوت بلاکچین با سایر دیتابیس‌ها در ساختار ذخیره اطلاعات در آن است. یک زنجیره بلوکی اطلاعات را به صورت گروهي، جمع‌آوری می‌کند که به آن Blocks یا بلوک‌ها گفته می‌شود که مجموعه‌ای از اطلاعات را در خود جای داده است. این بلوک‌ها ظرفیت محدودی دارند و مقدار معینی اطلاعات را می‌توانند ذخیره کنند. هنگامی که ظرفیتیک بلوک تکمیل شد و آن بلوک پر شد، به بلوک پر شده قبلی اضافه می‌شود و به این شکل زنجیره‌ای از بلوک‌های حاوی اطلاعات را ایجاد می‌کند که به آن Blockchain یا زنجیره بلوکی می‌گویند.

بلاکچین به زبان ساده یک دفتر کل توزیع شده یا دیتابیس غیرقابل تغییری است که اطلاعات را ذخیره می‌کند. blockchain از دو کلمه بلاک (Block) و چین (Chain) تشکیل شده است که به معنی زنجیره بلاک یا زنجیره بلوک است؛ اما چرا این نام را برای این تکنولوژی انتخاب کردند؟ اطلاعات در فناوری بلاکچین داخل یک سری بلاک‌هایی قرار می‌گیرند که این بلاک‌ها زنجیره‌وار به یکدیگر متصل هستند از این رو این تکنولوژی بلاکچین نامگذاری شده است، درست مطابق با نوع کارکردی که این تکنولوژی دارد.



بلاکچین چگونه کار می‌کند؟

احتمالا اگر با دنیای کامپیوتر و فناوری اطلاعات آشنا باشید، واژه پایگاه داده به گوشتان خورده است. اگر بخواهیم ساده بگوییم پایگاه داده، فضایی است برای ذخیره اطلاعات که طبیعتا این پایگاه داده توسط یک فرد یا مرکزیت، ایجاد و کنترل می‌شود. فناوری بلاکچین را می‌توان شبکه‌ای در نظر گرفت که کارکردی مانند پایگاه داده دارد اما مرکزیت خاصی ندارد و توسط نهاد یا ارگانی کنترل نمی‌شود، اطلاعاتی که در blockchain ذخیره می‌شوند یک سری تفاوت‌هایی با اطلاعات ذخیره شده در پایگاه داده‌ها دارد.

در بلاکچین تمامی اطلاعات ثبت شده بین تمام اعضای شبکه به اشتراک گذاشته می‌شود و نکته جالب اینجاست که این اطلاعات به هیچ عنوان قابل تغییر یا حذف نیستند. برای متوجه شدن این جمله باید کمی ریزتر شویم و سوال بلاکچین چیست را دقیق تر پاسخ دهیم.

جالب اینجاست حتی اگر بخش بسیار کوچکی از اطلاعات تغییر کند یا حذف شود، هش به طور کلی عوض می‌شود. حتی هش بلاک‌های دیگر هم عوض می‌شود! چرا؟ چون هر بلاک علاوه بر هش خودش، هش بلاک قبلی را نیز ذخیره می‌کند؛ بنابراین از این جهت است که به آن زنجیره بلاک‌ها می‌گویند.

خب حالا که فهمیدیم بلاکچین چیست، این سوال پیش می‌آید که یعنی کسی نمی‌تواند محتویات یک بلاک را تغییر دهد؟ بله، می‌تواند اما این تغییر از چشم اعضای شبکه دور نمی‌ماند و تمام شبکه باید این تغییر را تایید کنند؛ در غیر اینصورت هیچ اعتباری ندارد و تغییرات اعمال نمی‌شود.



پس این دیدگاه که اطلاعات در بلاکچین غیرقابل تغییر است، درست نیست. فرض کنید فردی یک فایل موسیقی را در یک بلاکچین قرار داده و در آن ذخیره کند؛ بنابراین همه اعضای شبکه نسخه‌ای از آن را دارند. حتی اگر خود فرد فایل موسیقی را حذف کند یا تغییر دهد، بقیه اعضای شبکه این اتفاق را نمی‌پذیرند؛ زیرا کپی نسخه اصلی آن فایل موسیقی را دارند. برای حذف این فایل راهی نیست جز اینکه کامپیوترهای اعضای شبکه را گرفته و آن فایل را حذف کند که عملا چنین اتفاقی امکان‌پذیر نیست. اما بعد از توضیح بلاکچین چیست به سراغ ویژگی‌ها و مزایای تکنولوژی blockchain می‌رویم که ببینیم، چرا این فناوری به این سرعت رشد پیدا کرده است.

همان‌طور که پیش‌تر گفته شد، اطلاعات در blockchain داخل یک سری بلاک‌ها ذخیره می‌شوند. این اطلاعات می‌توانند هر چیزی باشند و تنها در تراکنش‌ها خلاصه نمی‌شوند. هر بلاک، علاوه بر اطلاعاتی که درون آن ذخیره می‌شود، دارای «هش» به صورت مجموعه‌ای از کاراکترها است که برای ساخت آن از الگوریتم‌های خاصی استفاده می‌شود. هر بلاک با توجه به اطلاعاتی که درون آن قرار دارد، هش مربوط به خودش را دارد و این هش به نوعی نماد اطلاعات درون آن بلاک هستند.

نسخه نویسی الکترونیکی

(قسمت اول)

ارسال الکترونیکی نسخ پزشکی به داروخانه باعث کوتاه شدن فرآیند گردش کار و افزایش رضایتمندی بیمار می گردد. نسخه نویسی الکترونیک از جنبه های مختلف اهمیت دارد که شاید کمترین بخش آن، کاهش مصرف کاغذ باشد. امکان شناسایی و نشان دار شدن بیمار برای هر اقدام و خدمت مراقبتی و درمانی، شناسائی و امکان حمایت از بیماران نیازمند، جلوگیری از جعل و تخلف و سوء استفاده از نسخ کاغذی، جلوگیری از خطاهای ناشی از ناخوانا بودن نسخ کاغذی، کاهش تداخلات دارویی، کاهش تقاضای القایی و علاوه بر این فراهم سازی بستر تحقق پرونده الکترونیک سلامت، حداقل نتایج استقرار نسخه الکترونیک محسوب می شوند.

همچنین مطالعات نشان داده است استفاده از انواع مختلف فناوریهای اطلاعاتی از جمله نسخه نویسی الکترونیک می تواند با پیشگیری از خطاها و اشتباهات پزشکی، موجب کاهش قابل توجه میزان خطاهای پزشکی و ارتقای کیفیت خدمات ارائه شده به بیماران گردد. نسخه نویسی الکترونیک با غلبه بر مشکلات نسخه نویسی کاغذی باعث کاهش خطاهای پزشکی می گردد.

چالشی که در بحث نسخه نویسی الکترونیک عدم ورود برخی از بیمه های تکمیلی به موضوع نسخه نویسی الکترونیک است.

وقتی مردم خدمت الکترونیک می گیرند، انتظار دارند سایر بخش های خدمتی هم به شکل الکترونیک باشد و مجبور نباشند به کاغذ روی آورند. قانون این الزام را به سازمان های بیمه تکمیلی هم داد و تا حدودی اقدامات لازم از سوی این سازمان ها صورت گرفته است.

عصر حاضر عصر فراصنعتی یا عصر اطلاعات است به گونه ای که کلیه سازمان ها در سرتا سر دنیا، در حال استفاده از موانب فناوری اطلاعات هستند و از آن به عنوان عنصری کلیدی در مراقبت های بهداشتی درمانی استفاده می کنند. در ایران نیز مراکز درمانی و بیمارستانی از این قاعده مستثنا نبوده اند و قابلیت های جدید را برای ارائه خدمات بیشتر و جدیدتر افزایش داده اند. سیستم نسخه نویسی الکترونیک نمونه ای از سیستم های اطلاعات فنی اجتماعی بین رشته ای است که دارای حوزه های گسترده، کاربران مختلف، تخصص های گوناگون، پیچیدگی فراوان، زیر سیستم های مختلف و فرآیندهای پیاده سازی متفاوت می باشد.

در ایران نیز جهت اجرای طرح نسخه نویسی الکترونیک و حذف دفترچه های کاغذی بیمه، علاوه بر مواد ۹۱ و ۹۵ و ۹۱ و ۹۸ برنامه پنجم توسعه و ماده ۷۹ و بند الف ماده ۷۱ برنامه ششم توسعه، در بند چ ماده ۷۰ قانون بودجه و همچنین تبصره دو ماده ۶۷ قانون بودجه سال ۹۸ نیز بر ادامه و اجرای آن تاکید شده است. باتوجه به تعهدات وزارت بهداشت، پیاده سازی نسخه نویسی الکترونیک توسط سازمان بیمه سلامت از سال ۱۳۹۷ به صورت آزمایشی در استان کرمان اجرایی شد. نسخه نویسی الکترونیک از سال ۱۳۹۸ به شکل تدریجی در سایر استان ها شروع و با شتاب بیشتر در سال ۱۳۹۹ پیش رفت.

در نهایت طبق تبصره ۱۷ قانون بودجه که مقرر کرده بود از ابتدای دی ماه ۱۴۰۰ هرگونه تبادل نسخ کاغذی ممنوع است و صرفا در قالب خدمات الکترونیک امکان مبادله مالی بین سازمان های بیمه گر و مراکز ارائه دهنده خدمت امکان پذیر است، بر همین اساس از اول دی ماه ۱۴۰۰ که اجبار قانونی هم داشتیم، نسخه نویسی الکترونیک به شکل جدی آغاز شد. تعاریف متعددی از نسخه نویسی الکترونیک ارائه شده است ولی در کل به فناوری که با استفاده از سیستم کامپیوتری برای ورود، اصلاح و بازبینی و ارسال نسخ دارویی استفاده می شود، نسخه نویسی الکترونیک گفته می شود.

سیستم نسخه نویسی الکترونیک با فراهم نمودن اطلاعاتی کامل از بیمار برای پزشک، ایجاد امکان دسترسی به اطلاعات آنلاین از طریق کامپیوتر، هشدارها و سیستم پشتیبان تصمیم گیری باعث کمک در نسخه نویسی و پیشگیری از اشتباهات مرتبط با نسخه نویسی می گردد. کاربرد این فناوری باعث مشارکت نمودن تمام متخصصان ارائه کننده مراقبت سلامت در زمینه درمان بیمار، از جمله پزشکان، داروساز و پرستار می باشد، در سیستم نسخه نویسی الکترونیک، پزشک به صورت الکترونیک نسخه را به کامپیوتر داروخانه ارسال میکند. این فرآیند باعث کاهش خطاهای دارویی و در نهایت کاهش برگشت دادن نسخه به پزشک جهت تصحیح می گردد.



به نظر می رسد توجه بیشتر به ارائه راهکارهایی که بتواند باعث بالا بردن احتمال موفقیت در پیاده سازی هر یک از حوزه های کاربردی این فناوری در کشورمان گردد، مورد نیاز می باشد.

تحقیقات مختلف، عواملی چون مسائل فرهنگی، اجتماعی، اقتصادی، فنی و تکنولوژیکی، مدیریتی و فرایندی، حقوقی و قانونی، نبودن متولی خاص در این حوزه را به عنوان مهمترین موانع استقرار سلامت الکترونیک در ایران شناسایی و مورد تایید قرار داده اند. به عبارت دیگر در اجرای این طرح ۹۱ درصد بحث فنی و ۷۱ درصد تغییر رفتار است؛ چرا که مقاومت از طرف پزشک یا بیمار وجود خواهد داشت.

امکان مشاهده سوابق و شرح درمان:

نسخه الکترونیک قابلیت دیگری را در اختیار بیمار و پزشک او قرار می دهد که مشاهده سوابق درمان های بیمار است. در واقع دفترچه بیمه الکترونیک وضعیت سلامتی بیمار را به صورت جامع ثبت کرده، دوره های درمان و داروهای تجویزی او را فهرست می کند و در مواقع بیماری های بعدی، پزشک می تواند به صورت دقیق تری اقدام به تجویز دارو و انجام فرآیندهای درمانی کند. همچنین از تداخل های دارویی هم جلوگیری می شود.

سیستم های پشتیبان از تصمیم در نسخه نویسی الکترونیکی:

پرونده الکترونیک سلامت و سیستم پشتیبان تصمیم، دو کاربرد الکترونیکی فناوری اطلاعات هستند که می توانند فعالیت نسخه نویسی پزشکان را حمایت کنند. سیستم های پشتیبان تصمیم (Clinical Decision Support System) یا سیستم های پشتیبان تصمیم دارویی (Medication Decision Support System) در تمام مراحل نسخه نویسی الکترونیکی (نسخه نویسی، انتقال، نسخه پیچی، پایش نسخه) به همراه پرونده الکترونیک سلامت باعث بهبود ایمنی، کیفیت، اثربخشی و هزینه اثر بخشی مراقبت می گردد. سیستم های پشتیبان تصمیم، برنامه های کامپیوتری هستند که برای کمک به ارائه دهندگان مراقبت سلامت طراحی شده اند.

این سیستم ها به عنوان ابزار مبتنی بر دانش می توانند مدیر ارائه کننده مراقبت سلامت را در تجزیه و تحلیل ارزیابی های انجام شده از بیمار، انتخاب راه حل های درمانی موثر در تصمیم گیری های بالینی، بهبود عملکرد پزشکان از طریق مطالعه ارزیابی ها و نتایج آزمایشگاهی، سیستم های تشخیص بیماری ها، سیستم های یادآوری و سیستم های مدیریت بیماری ها کمک می کند. بنابراین سیستم های پشتیبان تصمیم دارای نقش مهمی در کاهش خطاهای پزشکی می باشند. انواع عملکردهای سیستم های پشتیبان از تصمیم گیری در نسخه نویسی الکترونیکی شامل موارد زیر می باشد:

فرهنگ لغات دارویی؛ اطلاعات دوز و فرمول های دارویی؛ دوز های دارویی پیش فرض؛ کنترل نمودن یا بررسی آلرژی های دارویی؛ بررسی نمودن تداخلات دارویی؛ بررسی نمودن دوز دارویی در مقابل عملکرد کلیوی؛ بررسی نمودن دوز دارویی در مقابل سن بیمار؛ بررسی نمودن دوز و انتخاب دارویی ارتباط با نتایج آزمایشگاهی بیمار؛ بررسی انتخاب دارویی در مقابل وضعیت بیمار یا بیماری های زمینه ای وی.

استفاده از سیستم پشتیبان تصمیم در نسخه نویسی الکترونیکی باعث تغییر رفتار ارائه دهنده مراقبت سلامت در صدور نسخه می گردد، زیرا پزشک با دسترسی به منابع اطلاعاتی، کتابخانه های دیجیتال و هشدارهای دارویی می تواند بر فرآیند تصمیم گیری خود تاثیر بگذارد. در کشور ما ایران نیز تحقیقات نشان دهنده فراوانی وقوع خطاهای دارویی، نواقص و مشکلات کمی و کیفی، با پیاده سازی نسخه نویسی الکترونیکی کاهش یافته است.



آشنایی با قانون جرایم رایانه ای

(قسمت اول)

پیشرفت جوامع و به ویژه توسعه ی فناوری ها و فضای مجازی سبب شکل گیری جرایمی شده است که در گذشته نه چندان دور به این شکل وجود نداشتند. جرایمی که با شکل و شیوه خاص ارتکاب خود و در عین حال به دلیل تحقّقشان در ابعاد بسیار متنوع و گسترده؛ سبب شدند که کشورهای مختلف از جمله ایران، به تعریف و تبیین آن ها بپردازند و قوانین خاصی را نیز برای آنان ایجاد کنند.

فضای سایبری علاوه بر امکاناتی که برای رشد و توسعه در اختیار بشر قرار داده، فرصت هایی نیز برای مجرمان ایجاد کرده است. از این روست که امروزه سخن از وجه سیاه اینترنت به میان می آید، از جمله ویژگی های این فضا آن است که مجرمان می توانند راحت تر مرتکب جرم شده و آماج مجرمانه متعددی را هدف بگیرند.

به هرگونه فعالیتی که به منظور انجام تبهکاری در شبکه های رایانه ای به خدمت گرفته شود، جرایم سایبری اطلاق می شود. بر اساس تعریف فوق اقداماتی چون حمله ی الکترونیکی به زیرساخت های حیاتی و ملی کشورها، کلاهبرداری، پولشویی الکترونیکی، استفاده جنایتکارانه از اینترنت، جعل آیدی و حتی استفاده از رایانه و مفاهیم فناوری اطاعات در جریان جنایات غیر سایبری مصداق هایی از جرایم سایبری است.

با توجه به شرایط کنونی گستره ارتباطات جوامع جهانی و نیاز مبرم به استفاده از فناوری های اطلاعاتی و از سوی دیگر این ویژگی های فضای سایبری باعث شده است که مقرراتی در خصوص پاسخ دهی کیفری برای مجرمان چه در حقوق ایران و چه در حقوق بین الملل وضع شود.

روند تدوین قانون جرایم رایانه ای در ایران:

همان طور که از اسم کلاهبرداری رایانه ای پیداست؛ این جرم در محدوده های خاص قابل ارتکاب است و آن هم در فضای مجازی و بین داده های رایانه ای و سامانه های کامپیوتری است. از همین نکته یکی از تفاوت های مهم این جرم با کلاهبرداری معمولی و سنتی مشخص می شود.

در کلاهبرداری سنتی باید جرم در دنیای واقعی رخ دهد اما در جرایم سایبری، کلاهبردار از طریق فضای مجازی و با تغییر دادن داده ها و اطلاعات فرد، این کار را انجام می دهد. مثلاً از طریق فضای مجازی در داده های حساب های بانکی افراد دست می برد و موجودی آن حساب ها را به حساب خود واریز می کند.

با توجه به پیشرفت سریع رایانه و کاربردهای متعدد و متنوع در بخش های مختلف، امکان سوء استفاده از این صنعت و عدم پاسخگویی قوانین مرسوم کیفری به مسائل جرم رایانه ای، در جریان بازنگری بخشی از قانون مجازات اسلامی، (تعزیرات) هیات محترم وزیران مقرر ساخت تا در خصوص جرایم رایانه ای نیز بررسی های لازم صورت گرفته و چنانچه پیشنهادهای مشخصی وجود دارد به متن لایحه ی جدید تعزیرات افزوده شود. دو متن پیشنهاد گردید؛ یکی توسط دبیرخانه شورای عالی انفورماتیک و دیگری به وسیله ی بانک مرکزی. متون پیشنهادی در کمیسیون لوایح دولت بررسی گردید و در نهایت یک لایحه با عنوان «چگونگی برخورد با جرایم رایانه ای» در جلسه هیات وزیران مورخ ۱۳۷۳/۰۶/۰۶ به تصویب رسید که طبق آن فصلی با ۲ ماده به قانون مجازات اسلامی افزوده می شود.

متأسفانه این لایحه در مجلس شورای اسلامی به تصویب نرسید. با وجود تلاش متخصصان و حقوقدانان کشور، فصل یا قانونی با این عنوان به قانون مجازات اسلامی افزوده نشد. تقریباً از اواخر دهه ۷۰ و ابتدای سال ۱۳۸۰ تدابیر گوناگونی در رده های حاکمیتی کشور در خصوص ضرورت مقابله با سوء استفاده های مجرمانه سایبری اتخاذ شده که مهم ترین آن ابلاغیه ۷ ماده ای مقام معظم رهبری درباره ی شبکه های اطلاع رسانی رایانه ای در سال ۱۳۸۰ است که می توان از آن به عنوان منشور سیاست جنایی ملی جرایم رایانه ای یاد کرد. این سیاستنامه، علاوه بر جنبه های کیفری موضوع، حاوی تدابیر پیشگیرانه و ارزشمندی است که توجه و پایبندی به آن می تواند مشکلات این حوزه را تا حد زیادی برطرف کند. در سخنرانی مورخ ۱۳۹۰/۱۲/۱۷ نیز رهبر معظم انقلاب درخصوص فضای مجازی چنین ایراد فرمودند: «گسترش فزاینده فناوری های اطلاعاتی و ارتباطاتی به ویژه شبکه ی جهانی اینترنت و آثار چشمگیر آن در ابعاد زندگی فردی و اجتماعی، و لزوم سرمایه گذاری وسیع و هدفمند در جهت بهره گیری حداکثری از فرصت های ناشی از آن در جهت پیشرفت همه جانبه کشور و ارائه خدمات گسترده و مفید به اقشار گوناگون مردم و همچنین ضرورت برنامه ریزی و هماهنگی مستمر به منظور صیانت از آسیب های ناشی از آن اقتضا می کند که نقطه ی کانونی متمرکزی برای سیاستگذاری، تصمیم گیری و هماهنگی در فضای مجازی کشور به وجود آید».

از سال ۱۳۸۱ فعالیت مجدد حوزه ی جرایم رایانه ای آغاز گردید که به تنظیم پیش نویس جرایم رایانه ای در شورای عالی توسعه ی قضایی قوه ی قضاییه منجر شد و در نهایت لایحه ی جرایم رایانه ای بعد از گذشت ۱۵ سال (از زمان تصویب آن در هیات وزیران آن زمان) توسط شورای عالی توسعه ی قضایی تهیه و پیشنهاد گردید که در خرداد ماه ۱۳۸۱ به تصویب مجلس شورای اسلامی و مورد تایید شورای نگهبان قرار گرفت. قانون جرایم رایانه ای مشتمل بر سه بخش و پنجاه و چهار ماده است و در بخش یکم این قانون به جرایم و مجازات مقرر در قانون می پردازد و در هفت فصل جرایم، به تقسیم بندی و در فصل هشتم موارد تشدید مجازات را مطرح می کند. فصل یکم با عنوان جرایم، علیه محرمانگی داده ها و سامانه های رایانه ای و مخبراتی دسترسی غیر مجاز، شنود غیر مجاز و جاسوسی رایانه ای را از مصادیق این نوع جرم شناخته و حداکثر مجازات این گونه جرایم توسط افراد عادی را بیست میلیون ریال تا شصت میلیون ریال جزای نقدی و از یک تا سه سال حبس در نظر گرفته است.

عنصر مادی اینگونه جرایم، شبیه جرایم علیه امنیت در فضای واقعی است و فقط ابزار جرم تغییر یافته است. در شماره های آتی سایر فصول قانون جرایم رایانه ای بررسی خواهد شد.

نویسنده: الهام همتی

اطلاعات کاربری

نام کاربری:

رمز عبور:

ورود | انصراف

معرفی نرم افزار پریزی (Prezi)

- ایجاد تمایز نسبت به سایر ارائه‌ها
- دسترسی به آرشیو بزرگ پریزی
- قابلیت استفاده از نسخه رایگان

چگونگی کار با پریزی:

پریزی اصطلاحاً ۲/۵ بعدی است، به این معنا که علاوه بر جابجایی عمودی و افقی، حرکت در عمق را نیز فراهم می‌نماید و تفاوت آن با نرم افزارهای ۳ بعدی این است که نمای پرسپکتیو را را به نمایش نمی‌گذارد.

پریزی بر اساس طرح بندی نقشه (Map Layout) است به شکلی یک تخته سفید بزرگ در اختیار شما می‌گذارد و شما همه مطالبی که می‌خواهید ارائه کنید (از تصویر و متن گرفته تا فیلم و انیمیشن و صدا) را داخل این صفحه قرار می‌دهید و پس از تعریف مسیر آیت‌های محتوا، می‌توانید یک انیمیشن ضمنی ایجاد نمایید. شروع ارائه شما با این



امروزه بسیاری از برنامه‌هایی که برای ارائه مقاله در زمینه‌های آموزش، تجارت، کنفرانس‌ها و... استفاده می‌شوند به روش اسلاید به اسلاید هستند. ارائه اسلاید به اسلاید، مانند آنچه در نرم افزار پاورپوینت انجام می‌گیرد بسیار خسته‌کننده می‌باشد چون یک روند خطی ساده را دنبال می‌کند؛ مخصوصاً اگر طراحی اسلایدها بی‌نظم باشند و اندازه، متحرک سازی آیت‌های محتوا و رنگ‌ها به خوبی انتخاب نشود.

یکی از اصلی‌ترین مشکلات روش اسلاید به اسلاید، از دست رفتن کلیت مطلب (زمینه) است، یعنی مخاطب شما به آسانی ممکن است سر رشته مطالب را از دست بدهد و خیلی زود خسته شود.

مشکل از آنجا شروع می‌شود که این شیوه یک مسیر خطی را برای ارائه موضوع طی می‌کند، ولی این در حالی است که مغز انسان بصورت خطی فکر نمی‌کند و این موضوع باعث می‌شود تا مخاطب نتواند در زمان ارائه مطلب تمرکز خوبی داشته باشد و جابجایی سریع بین اسلایدها کلیت مطلب ارائه را از بین می‌برد.

پریزی (prezi) یک نرم افزار مدرن است که کمتر از ۱۰ سال از عمر آن می‌گذرد. این نرم افزار که رقیب سرسخت و جدی نرم افزارهای سنتی اسلاید محور همچون پاورپوینت است، این روزها به شدت مورد استقبال افرادی قرار گرفته است که قصد دارند ارائه‌ای مدرن، حرفه‌ای و متفاوت داشته باشند.

در پریزی قرار نیست که اسلایدهای متعدد داشته باشید، بلکه پریزی شامل یک صفحه سفید نامحدود است. شما قادر هستید اطلاعات را در هر کجای صفحه که تمایل دارید قرار دهید. تنها کافیست برای هر کدام از اطلاعات ارائه خود به ترتیب نمایش، مسیر حرکت و جابجایی تعریف کنید. در واقع نرم افزار پریزی همانند نرم افزار پاورپوینت به قصد کمک رسانی در ارائه‌ها و سخنرانی‌های ما به میدان آمده است و همانطور که از نام آن پیداست هدفی جز ارائه ندارد. اما ویژگی‌های مثبتی در این نرم افزار وجود دارد که حساب آن را از پاورپوینت کاملاً جدا می‌کند.

ویژگی‌های پریزی:

- عدم ایجاد محدودیت‌های اجرایی به نسبت پاورپوینت
- قابلیت زوم روی موضوع دلخواه و حرکت در عمق تصاویر
- حرکات آزادانه
- امکان طراحی صفحه به دلخواه
- امکان ایجاد خلاقیت در ارائه و سخنرانی
- ایجاد رابطه عمیق‌تر با مخاطب و درک بهتر ارتباطات
- یکپارچگی کلام

تصویر بزرگ است که کلیت مطالب شما را به صورت کامل نشان می‌دهد، سپس می‌توانید مشخص کنید که با یک افکت زیبای فلش، این تصویر بزرگ نمایی یا کوچک نمایی شود و با طی یک مسیر دلخواه (مثلاً یک خط راست، یک منحنی، یک چرخش 180 درجه یا هر چیزی که به ذهنتان می‌رسد) به سراغ اولین آیت‌می‌که می‌خواهید درباره آن توضیح دهید بروید.

نگاهی به نظرات و تجربیات افراد متخصص:

در یکی از این مطالب Scott Berkun که نویسنده چندین کتاب پیرامون خلاقیت، رهبری، فلسفه و ارائه مطلب است، در مطلبی با عنوان "چرا از پریزی متنفرم؟" بر اساس تجربیات خود به دلایل مختلفی برای تنفر خود از پریزی اشاره کرده است. اصلی‌ترین دلیل او برای تنفر از پریزی، پررنگ‌تر کردن قابلیت‌هایی است که مانند PowerPoint باعث حواس پرتی مخاطبان از اصل موضوع می‌شود و آن نحوه ارائه پریزی به صورت زوم، چرخش و حرکت است. از نظر Berkun بهترین روش برای یک ارائه مطلب موثر، به کارگیری یک تخته وایت برد و یا در نهایت یک برنامه ترسیم ساده بر روی تابلت برای ترسیم و نوشتن در حین ارائه مطلب است. در مطلبی دیگر Phil Waknell که به صورت حرفه‌ای در زمینه فن بیان و ارائه مطلب فعال است، دو دلیل اصلی را برای استفاده نکردن از پریزی بیان می‌کند:

- اکثر ارائه مطالب با پرزی از قابلیت هایی استفاده می کنند که می توان آن ها را با استفاده از سایر نرم افزارهای ارائه مطلب با صرف زمان کمتری انجام داد.
- یادگیری پرزی بسیار زمان بر است.
- اسلایدهای ساخته شده با پرزی در دسترس عموم قرار می گیرد، مگر آنکه از اکانت های غیر رایگان استفاده کنید.
- اسلایدهای ساخته شده با پرزی براحتی قابل تبدیل به سایر فرمت ها مانند PowerPoint و Keynote نیستند.

جمع بندی و راه حل:

براساس این مطالب می توان ریشه این مشکلات را در چیزی غیر از نرم افزار پرزی یا پاورپوینت و یا هر نرم افزار دیگری پیدا کرد و آن، برخی باورهای غلط و غیر علمی در زمینه ساخت اسلاید و ارائه مطلب است. قوانین و نکات یک ارائه مطلب خوب و طراحی اسلاید حرفه ای چندان پیچیده نیست و در صورتی که یک چارچوب مشخص را دنبال و نکاتی را رعایت کنید می توانید به خوبی از قابلیت های هر نرم افزار براساس نیاز خود به خوبی در ساخت اسلایدهای حرفه ای و در نتیجه آن یک ارائه مطلب بدون نقص، استفاده کنید. باورهایی مثل استفاده از افکت ها و انیمیشن های بسیار، اسلایدهای زیاد و رنگارنگ و متن های خلاصه نشده بعلاوه عدم مهارت کافی در بکارگیری قابلیت های مناسب در ساخت اسلاید و پاورپوینت، موارد عمده ای است که باعث می شود جدا از نوع نرم افزار، نتیجه کار شما غیر حرفه ای باشد.

دلیل بسیاری از افراد در استفاده از پرزی، تنها یک چیز است: «متفاوت و جدیدتر از پاورپوینت قدیمی و کلیشه ای است.» پرزی در مقایسه با پاورپوینت متفاوت است، اما در صورتی که به خوبی از آن استفاده نشود اسلایدهایی به مراتب بدتر از پاورپوینت طراحی خواهید کرد که نتیجه ارائه با هدفی که از انتخاب پرزی داشته اید، کاملاً متفاوت است.

اما راه حل چیست؟ نکته اول اینکه، Prezi، PowerPoint، LibreOffice Impress، Keynote و هر نرم افزار دیگری که برای ساختن اسلاید و ارائه مطلب می شناسید، تنها یک ابزار است، این مهارت و خلاقیت شماست که تعیین کننده نتیجه کار خواهد بود. پاورپوینت به خودی خود فاقد عنصر خلاقیت نیست (نظرات برخی از کاربران در سایت های مختلف)، بلکه شما می بایست با شناخت قابلیت ها و امکانات آن به خوبی از آن ها برحسب نیاز خود استفاده کنید. طراحی یک پاورپوینت پایان نامه و یا درسی، اصول متفاوتی در مقایسه با طراحی یک پاورپوینت تجاری و مالی مدیا دارد.

با مطالعه نظرات مثبت و منفی می توان به این نتیجه رسید که فارغ از آنکه از چه نرم افزاری استفاده می کنید، با رعایت اصول علمی و حرفه ای و در نظر گرفتن تمامی جوانب می توانید اسلایدهای خود را به صورت حرفه ای طراحی کنید و یک ارائه مطلب بی نقص داشته باشید. اگر نحوه ارائه

پرزی علی رغم بسیاری نکات مثبت، مورد انتقاد بسیاری از افراد است، قطعاً راه حل هایی برای کاهش اثر آن و کم رنگ کردن اثرات منفی آن وجود دارد. بخاطر داشته باشید هر نرم افزار نکات مثبت و منفی خاص خود را دارد و شما می بایست براساس معیارهای مختلفی مانند نوع ارائه، نیازها، امکانات، مخاطبان و... تصمیم گیرنده نهایی باشید.

دلیل اول او در زمان آماده کردن ارائه مطلب است، جایی که می بایست ارائه کننده به طور ویژه بر روی مخاطبان، نیازها و توقعات آن ها تمرکز داشته باشد. در حالی که نقطه ضعف بسیاری از نرم افزارهای

ارائه مطلب سادگی آن ها در ساخت اسلایدهای بد است، پرزی در نقطه مقابل نرم افزاری برای ساختن اسلایدهای بسیار جذاب و چشم نواز است که زمان بسیار زیادی نیاز دارد. نتیجه مشخص است: تمرکز بیش از حد ارائه کننده بر روی ساخت اسلاید. در نهایت ممکن است ارائه کننده اسلایدهای بسیار جذاب و خوبی داشته باشد، اما در انتقال موثر مطلب دچار مشکل خواهد شد زیرا پرزی باعث از بین رفتن ارتباط بین ارائه کننده و مخاطب می شود. دلیل دوم به زمان ارائه اشاره دارد. در حین ارائه این نکته بسیار مهم است که مخاطبان تا حد امکان به ارائه کننده توجه داشته باشند تا ارتباطی مناسب جهت انتقال مطلب و پیام مورد نظر ایجاد شود.



حال در صورتی که مخاطب تمام مدت به صفحه خیره شده باشد و کمتر به ارائه دهنده نگاه کند، این ارتباط از بین خواهد رفت که در اینجا نیز نقش پرزی مهم است.

۸ دلیل برای استفاده نکردن از پرزی در

تدریس دانشگاه براون، یکی از قدیمی ترین دانشگاه های آمریکا، در مطلبی کوتاه ۸ دلیل را برای استفاده نکردن از پرزی در تدریس بیان کرده است

- پرزی قابلیت های سازگار با افراد ناتوان و معلول را ندارد.
- با توجه به شیوه ارائه پرزی به صورت زوم یا چرخش و حرکت و تاثیر آن بر بار شناختی، توجه مخاطبان به جای ارائه کننده و مطالب به جلوه های بصری جلب می شود.
- نوع ارائه پرزی می تواند باعث حرکت زدگی و در نتیجه حواس پرتی مخاطبان شود.
- ساخت اسلاید با استفاده از پرزی باعث می شود تا توجه ارائه کننده از موارد مهمی مانند فعالیت های آموزشی و توسعه آن ها به مسایل کم اهمیت تری مانند طراحی اسلایدها معطوف شود.

احراز هویت یکپارچه

یا Single Sign-On

سرویس SSO مورد نظر نیز یک گواهینامه به شکل توکن را که شامل اطلاعات شناسایی کاربر می‌شود، برای ارائه‌دهنده خدمت (نرم‌افزار یا وب سایت) ارسال می‌کند تا از هویت کاربر مطمئن شود.

نحوه عملکرد این سازوکار در عمل نیز اینگونه است که شما برای احراز هویت در یک وب سایت یا یک نرم افزار، کافی است تا تنها یکبار نام کاربری و رمز عبور سرویس SSO را وارد کنید. سامانه Single Sign-On اطلاعات وارد شده از سوی شما را با یک مخزن اطلاعات کاربران، مثلاً با استفاده از پروتکل LDAP یا قرارداد دسترسی سبک‌وزن راهنما، مقایسه کرده و احراز هویت می‌کند و در صورت تأیید، نشست کاربر در سامانه SSO ایجاد می‌گردد. پس از تأیید هویت، این سرویس فرآیند احراز هویت شما را برای تمام وب سایت‌ها و برنامه‌های متصل به این سرویس که شما حق دسترسی به آن‌ها را دارید، به صورت خودکار احراز هویت می‌کند و تا زمانی که شما در سرویس SSO لاگین هستید، نیازی به ورود مجدد رمز عبور و نام کاربری در هیچ‌کدام از سامانه‌های مرتبط نخواهید داشت.

نحوه پیاده‌سازی Single Sign-On چگونه است؟

ساختار پیاده‌سازی SSO از مراحل زیر تشکیل شده است:

- * استفاده از دایرکتوری مرکزی جهت Authentication
- * تصدیق کاربران بر اساس این دایرکتوری
- * تعیین مجوزهای کاربران بر اساس Credential‌های مربوطه

پیاده‌سازی SSO به روش‌های مختلفی صورت می‌پذیرد که ۲ روش آن در زیر آورده شده است:

اسکرپت: در این روش، اسکرپت اطلاعات اکانت کاربر را بصورت رمزگذاری شده به سیستم تشخیص هویت ارسال می‌کند و پس از تأیید هویت، کاربر وارد سیستم می‌شود.

کوکی: در این روش کوکی‌های سیستم کاربر به سروری که کاربر می‌خواهد به آن وارد شود ارسال می‌شود. در واقع سیستم‌های نرم‌افزاری تحت وبی که دامنه (Domain) مشابه دارند، اما بر روی چند سرور قرار گرفته‌اند، جهت تشخیص هویت کاربر از کوکی‌هایی استفاده می‌نمایند که به صورت رمزنگاری شده هستند و بر روی سیستم کاربر قرار گرفته‌اند. به این ترتیب هویت کاربر در تمامی سرورها تأیید می‌شود.

انواع روش‌های احراز هویت با Single Sign-On کدام است؟

شناسایی و احراز هویت دو هسته اصلی اند که در بیشتر سیستم‌های کنترل دسترسی تعبیه شده اند.

استفاده از سامانه‌ها و نرم افزارهای سازمانی، نیازمند داشتن یک حساب کاربری و وارد کردن نام کاربری و رمز عبور آن‌ها است، اما به خاطر سپردن و استفاده از تعداد زیادی اطلاعات کاربری و رمز عبور عملاً روشی ناکارآمد است. شناسایی یگانه SSO (Single sign-on) یکی از زیر مجموعه‌های سازوکارهای مدیریت هویت فدرال در سامانه‌های کامپیوتری است که با ارائه یک سامانه متمرکز تأیید هویت، به کاربران امکان می‌دهد با استفاده از تنها یک مجموعه داده‌های احراز هویت (به عنوان مثال، یک نام کاربری و رمز عبور)، به روشی امن در چند سیستم نرم افزاری و وبسایت مستقل و در عین حال مرتبط وارد شوند.

این سازوکار به کاربران امکان می‌دهد با یک اعتبارنامه ورود، به چندین برنامه و وبسایت دسترسی داشته باشند. پیاده‌سازی SSO می‌تواند توسط شرکت‌ها، سازمان‌های کوچک و متوسط و حتی افراد، برای سهولت مدیریت اطلاعات کاربری‌شان مورد استفاده قرار بگیرد. این فناوری علاوه بر کمک به بهبود امنیت، برای دسترسی به برنامه‌های محلی (Local) و هم دسترسی به برنامه‌های موجود در فضای ابری به کار می‌رود. یک راهکار واقعی شناسایی یگانه، به کاربر این امکان را می‌دهد که یک بار وارد سیستم شود و بدون وارد کردن مجدد اطلاعات مربوط به احراز هویت، بتواند به خدمات مورد نظرشان دسترسی پیدا کند. از نمونه های مشهور چنین سازوکاری می‌توان به نرم‌افزارهای تحت وب گوگل و مایکروسافت اشاره کرد که از یک سامانه متمرکز تأیید هویت استفاده کنند. به طوری که اگر وارد یکی از سرویس‌های گوگل مانند Gmail شوید، امکان دسترسی به سایر سرویس‌های گوگل مانند Google Drive، YouTube، Google Docs و... را نیز خواهید داشت.

Single Sign-on یا شناسایی یگانه (SSO) چطور کار می‌کند؟

پیش از اینکه به مزایا و نکات فنی سازوکارهای Single Sign-on بپردازیم، شاید کنج‌گو باشید که چنین سامانه‌ای دقیقاً چطور کار می‌کند. برای پاسخ به این سوال، ابتدا نحوه احراز هویت بدون SSO را بررسی می‌کنیم. در حالت عادی وقتی می‌خواهید وارد برنامه یا سامانه‌ای شوید، باید نام کاربری و رمز عبور خود را وارد کنید. سامانه یا وبسایت مورد نظر، اطلاعات کاربری که توسط شما وارد شده را با اطلاعات کاربری موجود در پایگاه داده خود مقایسه و صحت آن را بررسی می‌کند و در صورت تأیید هویت به شما اجازه می‌دهد به صفحات مختلف و بسایت یا بخش‌های مختلف سامانه دسترسی پیدا کنید. در مقابل، در روش Single Sign-on یا SSO، احراز هویت به جای نام کاربری و رمز عبور به اعتماد بین دامنه‌ها و نرم افزارها متکی است. یعنی در این روش، رمز عبور توسط کاربر یا حتی یک نرم‌افزار وارد نمی‌شود و احراز هویت کاربر تنها بنا بر اساس اعتبار یک سرویس ارائه‌دهنده هویت صورت می‌گیرد. در این حالت، اپلیکیشن یا وب سایت مورد نظر که ارائه‌دهنده سرویس/خدمت نامیده می‌شود، برای احراز هویت کاربر از یک ارائه‌دهنده هویت مانند گوگل استعلام می‌کند.

چهره، اثر انگشت، DNA، شبکه و مردمک چشم شما از مواردی است که جزء این عامل به حساب می آید و قطعاً تا به حال اثبات شده است که اثر انگشت و DNA شما در کل دنیا منحصر به فرد می باشد.

احراز هویت با عوامل بیومتریک:

عامل بیومتریک، عبارت است از یک ویژگی و خصیصه رفتاری یا فیزیولوژیکی که برای هر فرد یکتا است. بیومتریک یک سیستم خودکار است که انسان ها را از روی ویژگی های فیزیولوژیکی و همچنین رفتارهای فرد شناسایی و احراز هویت می کند. در این گونه سیستم ها یک پایگاه داده از تصاویر مربوط به ویژگی های فیزیولوژیکی افراد وجود دارد که به محض درخواست فرد برای احراز هویت، این تصاویر با تصویر ویژگی های فرد مقایسه شده و در نهایت در صورتیکه تصویر مربوطه در پایگاه داده وجود داشته باشد، شخص احراز هویت می شود.

آنچه که شما انجام می دهید (What You DO):

برخی اوقات می توان فاکتور چهارمی نیز به این موارد اضافه کرد که معمولاً به آن چیزی که شما انجام می دهید نیز گفته می شود. برای مثال، می توان افراد را با استفاده از روش و ریتم استفاده از Keyboard و تایپ کردن توسط آن (KeyStroke Dynamics) شناسایی و احراز هویت کرد؛ که این یک تکنیک احراز هویت بیومتریک یا شیوه رفتاری شما می باشد و جزء دسته بندی Two - Factor Authentication هاست. هر فردی زمان استفاده از کیبورد و تایپ کردن رفتار و روش استفاده خاص خود را دارد که پارامترهایی همچون زمان و نحوه فشردن کلیدها از این دسته رفتارها می باشد.

احراز هویت با KeyStroke Dynamics:

در سازمان ها، به مرور زمان نرم افزارهای مختلفی نصب و راه اندازی شده اند که هرکدام قسمتی از سازمان را مکانیزه می نمایند. بنابراین کاربران سازمان برای ورود به هرکدام از این برنامه های کاربردی، نیاز به کلمه عبور و نام کاربری مجزایی دارند که مشکلات زیر را برای مدیران و کاربران سازمان ایجاد کرده است:

- نیاز مکرر به وارد کردن نام کاربری و کلمه عبور برای ورود به هرکدام از برنامه های کاربردی
- فراموش کردن کلمه عبور و نام کاربری بعضی از این نرم افزارها و درخواست های مکرر برای بازنشانی آن ها
- عدم وجود امکان ردگیری ورود و خروج کاربران به نرم افزارهای مختلف
- عدم توانایی برقراری ارتباطات اتوماتیک بین سیستم های Front-end مانند پرتال ها با سیستم های End-Back مانند اتوماسیون اداری

شناسایی عملی است که کاربر برای معرفی خود به یک سیستم اطلاعاتی، استفاده می کند که معمولاً در قالب یک شناسه ورود یا LoginID وجود دارد. در واقع شناسایی، فرایندی است که طی آن، فرد هویتی را اظهار می کند و از این نقطه، پاسخگویی آغاز می شود. ارائه نام کاربری، شناسه ورود، شماره شناسایی یا کارت هوشمند توسط کاربر، نمایانگر فرایند شناسایی است.

احراز هویت عبارت است از فرایند بررسی اعتبار هویت ادعا شده. احراز هویت نیازمند ارائه اطلاعات دیگری توسط فرد است که باید دقیقاً با هویت مذکور، مرتبط باشد و یکی از مهم ترین مباحث در حوزه امنیت سیستم های کامپیوتری می باشد. احراز هویت، هویت فرد را به وسیله مقایسه یک یا چند عامل با پایگاه داده ای از هویت های معتبر، بررسی می کند. به طور کلی روش های احراز هویت یا Authentication در

حوزه امنیت اطلاعات، به چهار تیپ ساده تقسیم بندی می شود. انواع روش های احراز هویت با Single Sign-On نیز شامل همین موارد است:

چیزی که شما می دانید: (What You Know)

ساده ترین و البته پرکاربردترین روش احراز هویت استفاده از نام کاربری و رمز عبور یا همان Username و Password می باشد.

احراز هویت با رمز عبور:

این روش به عنوان ضعیف ترین شکل حفاظت محسوب می شود. رمزهای عبور ممکن است افشا شوند و به همین دلیل بایستی از آن ها محافظت شود.

چیزی که شما دارید (What You Have):

در واقع داشتن وسیله ای برای احراز هویت است که این وسیله معمولاً به عنوان کارت هوشمند یا Smartcard، در قالب قفل ها یا Token های

USB و یا سایر مواردی از این قبیل می باشد و کاربر برای احراز هویت حتماً باید این وسیله را همراه خود داشته باشد. برای احراز هویت در چنین روشی کاربر می بایست Smartcard یا Token خود را در دستگاهی که ویژه احراز هویت طراحی شده است وارد کند.

احراز هویت با Token:

Token ها ابزارهای فیزیکی هستند که در اندازه هایی مانند کارت های هوشمند و یا حافظه های فلش وجود دارند و دستگاه های مولد رمز عبور هستند که افراد باید آن ها را همراه خود داشته باشند. این ابزارها وظیفه نگهداری یا تولید رمزهای عبور ایستا و یا پویا را برعهده دارند.

چند نوع توکن داریم:

- توکن های رمز عبور ایستا
- توکن های رمزهای عبور پویای همگام
- توکن های رمزهای عبور پویای ناهمگام

چیزی که شما هستید (What You Are):

درواقع احراز هویت با استفاده از ویژگی های خاص بدن شماست.



ابزار هوش مصنوعی

قسمت اول:

افزایش کیفیت تصویر



نحوه بررسی این ابزارها:

برای این که تفاوت عملکرد بین این ابزارها را بهتر درک کنید، یک تست کوچک برای هرکدام انجام داده‌ایم که در ادامه به جزئیات این تست‌ها می‌پردازیم:

- اولین تست ما شامل یک تصویر با کیفیت پایین (۱۲۰ در ۱۲۰ پیکسل) است. در این سناریو، هوش مصنوعی به جای برجسته کردن جزئیات موجود، نیازمند بازتولید آن هاست. بنابراین، انتظار نتایجی با ظاهری مصنوعی داشته باشید. این تست به شما کمک می‌کند ارزیابی کنید که نرم افزار چقدر در افزودن جزئیاتی که به طور یکپارچه با تصویر ادغام می‌شوند، توانایی دارد.

- دومین تست شامل بهبود یک تصویر با کیفیت پایین و پر از نویز است. در حالی که رزولوشن این تصویر (۳۰۰ در ۳۰۰ پیکسل) نسبت به تصویر ورودی در تست اول بهتر است، اما به شما این امکان را می‌دهد که نحوه‌ی بهبود جزئیات تصویر توسط نرم‌افزار را ارزیابی کنید.

- ممکن است همه شما به دنبال بهبود چشمگیر یک تصویر نباشید و گاهی اوقات تنها به ارتقاء ملایمی نیاز داشته باشید. به همین دلیل است که ما تست دوم را نیز گنجانده‌ایم.

- در هر دو تصویر تست، عکس‌های پرسنلی استفاده شده اند؛ این کار ابزار را مجبور می‌کند تا جزئیاتی را اضافه کند که به طور خاص با چهره فرد موردنظر مطابقت داشته باشد، بدون اینکه باعث شود او غیرقابل شناسایی به نظر برسد.

حالا با در نظر گرفتن این موضوع، بررسی این ابزارها را آغاز می‌کنیم:

AnyRec

بسیاری از ابزارهای افزایش رزولوشن تصویری که به صورت آنلاین پیدا کردیم، در نسخه رایگان خود تنها امکان افزایش حداکثر ۴ برابری رزولوشن را ارائه می‌دهند. اما با AnyRec، شما می‌توانید به صورت رایگان رزولوشن تصاویر را تا ۸ برابر افزایش دهید. نتایج تست ما را ببینید که در آن دو تصویر با کیفیت پایین را تا رزولوشن ۸ برابری بزرگ کردیم.

در تست اول، تصویری با کیفیت پایین از مجموعه تصاویر موردنظر را ۸ برابر بزرگ کردیم. به دلیل نبود جزئیات کافی در تصویر اولیه، این ابزار از هوش مصنوعی برای جبران و اضافه کردن جزئیات بیشتر استفاده می‌کند. بنابراین، نتایج ممکن است کمی مصنوعی به نظر برسند. با این حال، این در مقایسه با سایر ابزارهای موجود در این لیست، واقع گرایانه‌ترین نتیجه برای تست اول به شمار می‌رود.

در عصری که تصویر، زبان جهانی ارتباط است، بالا بردن کیفیت عکس با هوش مصنوعی نه تنها یک نیاز بلکه یک ضرورت شده است. این تکنولوژی انقلابی، امکان تبدیل تصاویر معمولی به شاهکارهای دیجیتال را فراهم می‌آورد، بدون نیاز به مهارت‌های پیچیده و با هزینه‌ای نزدیک به صفر. در این مقاله، ما شما را با قدرت و پتانسیل بی‌پایان هوش مصنوعی در بهبود و ارتقای کیفیت تصاویر آشنا می‌کنیم. افزایش کیفیت عکس با هوش مصنوعی؛ راهی به سوی خلق تصاویری خیره‌کننده که پیش از این تنها در خواب و خیال ممکن بود. تکنولوژی هوش مصنوعی، با توانایی خود در تحلیل و پردازش داده‌های پیچیده، انقلابی شگرف در عکاسی دیجیتال به پا کرده است. این فناوری، فراتر از بهبود ساده کیفیت تصاویر، قادر است عمق و جزئیات را در سطحی پیچیده بازنمایی کند و مرزهای میان واقعیت و تصویر را جا به جا نماید. با استفاده از الگوریتم‌های پیشرفته، هوش مصنوعی می‌تواند نویزهای تصویری را کاهش، جزئیات را در نورهای کم و شرایط سخت نورپردازی افزایش دهد و حتی اشیاء یا افراد را از پس زمینه جدا سازد. این تکنولوژی همچنین قابلیت احیای تصاویر قدیمی و آسیب‌دیده را دارد، به طوری که آن‌ها را به شکلی باورنکردنی به زندگی بازمی‌گرداند.

روش بالا بردن کیفیت عکس با هوش مصنوعی چندان پیچیده نیست؛ کافیست هوش مصنوعی مورد علاقه و کاربردتان را انتخاب کرده و عکس‌هایتان را در آن آپلود کنید! ممکن است خیلی از ابزار و سایت‌های هوش مصنوعی نیاز به خرید نسخه پرمیوم داشته باشند اما سایت‌ها ابزارهایی هستند که امکان استفاده رایگان از آنها و افزایش کیفیت عکس به صورت آنلاین و کاملاً رایگان را برایتان فراهم کرده‌اند؛ این سایتها عموماً تجربه کاربری مشابهی دارند. مراحل که باید برای بالا بردن کیفیت عکس توسط هوش مصنوعی انجام دهید، عبارت است از:

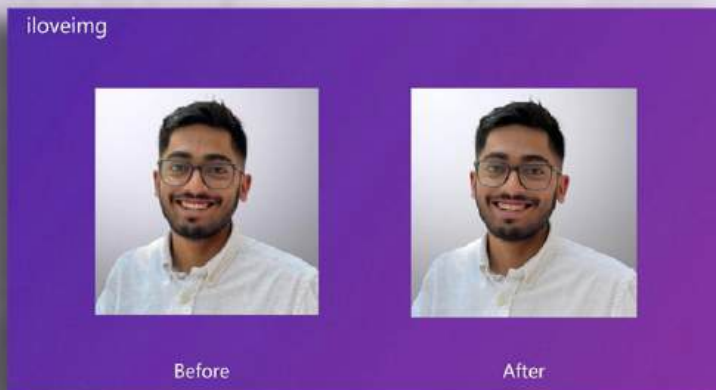


زمانی که به تصویری با کیفیت پایین نگاه می‌کنیم، به احتمال زیاد دلیل آن رزولوشن پایین آن است. این بدین معناست که تصویر از پیکسل‌های کمتری تشکیل شده است؛ بنابراین، اطلاعات کمی برای نمایش آن وجود دارد. افزایش رزولوشن (Upscaling) فرآیندی است که باعث افزایش کیفیت تصویر با بزرگتر کردن اندازه آن می‌شود.

روش‌های سنتی افزایش رزولوشن، رنگ پیکسل جدید در تصویر با رزولوشن بالاتر را با میانگین‌گیری از چهار پیکسل نزدیک آن تعیین می‌کنند. برخی از روش‌ها همچنین از فرمول خاصی برای محاسبه میانگین وزنی ۱۶ پیکسل مجاور استفاده می‌کنند تا رنگ پیکسل‌های جدید را تولید کنند. با این حال، هوش مصنوعی می‌تواند تصاویر را با استفاده از فناوری‌های مبتنی بر Super Resolution Techniques باکیفیت‌تر کند.

ابزارهای هوش مصنوعی حاوی مدل‌هایی هستند که روی مجموعه داده‌های عظیم آموزش داده شده‌اند.

iLoveIMG در تست دوم نیز عملکرد فوق العاده‌ای دارد. نتایج بدست آمده از این ابزار در افزایش کیفیت تصویر تا ۴ برابر، بهتر از هر ابزار دیگری بود که ما استفاده کردیم. همانطور که مشاهده می‌کنید، جزئیات و کیفیت تصویر به طور قابل توجهی بهبود یافته است.



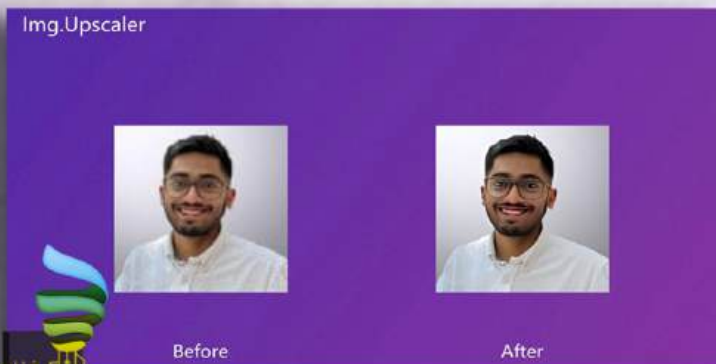
استفاده از iLoveIMG رایگان است، اما برای استفاده از آن باید ثبت نام کنید. با این حال، محدودیتی در تعداد تصاویری که می‌توانید بزرگنمایی کنید وجود دارد. برای دسترسی به قابلیت بزرگنمایی نامحدود تصاویر و حذف تبلیغات، می‌توانید نسخه پولی این ابزار را تهیه کنید. نسخه پرمیوم همچنین حداکثر رزولوشنی را که می‌توانید تصویر را با آن بزرگنمایی کنید افزایش می‌دهد.

قیمت: رایگان / نسخه پولی: 4 دلار به بالا در ماه

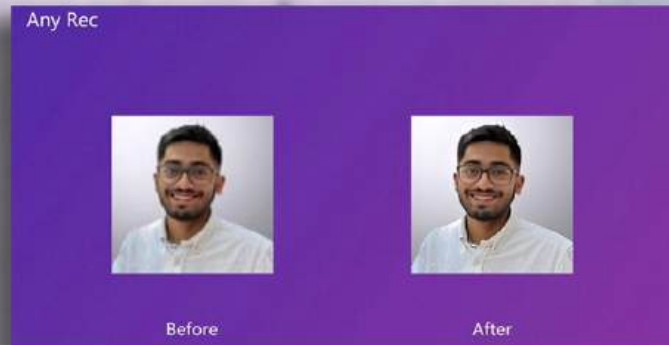
:img.Upscaler

Img.Upscaler یکی دیگر از ابزارهای هوش مصنوعی برای بالا بردن کیفیت عکس‌ها است که به شما امکان می‌دهد رزولوشن تصاویر خود را تا ۴ برابر افزایش دهید. رابط کاربری این ابزار ساده است و می‌توانید تصاویر با فرمت JPG یا PNG را آپلود کنید. در ادامه عملکرد این ابزار را در دو تست مختلف که در آن‌ها تصاویر را تا ۴ برابر رزولوشن اصلی افزایش دادیم، می‌توانید مشاهده کنید.

نتایج تست اول رضایت‌بخش بود. جزئیات تصویر با کمی اعوجاج بازسازی شدند، اما همچنان قابل قبول هستند. بدیهی است که اگر از فاصله دور به تصویر نگاه کنید یا از آن به عنوان Thumbnail استفاده کنید، کیفیت تصویر مناسب به نظر می‌رسد.



در تست دوم تصویر بسیار شارپ بود و ما از نتیجه کلی راضی بودیم. با این حال، اگر با دقت بیشتری به تصویر نگاه کنید و روی چشم‌ها یا عینک موجود در آن زوم کنید، متوجه برخی جزئیات مصنوعی خواهید شد.



عملکرد این ابزار در تست دوم نیز عالی است. تفاوت قابل توجهی در کیفیت تصویر وجود دارد. سایر ابزارهای موجود در این لیست تصویری با وضوح بسیار بالا به ما تحویل دادند، اما AnyRec در حفظ تعادل بسیار خوب عمل می‌کند.

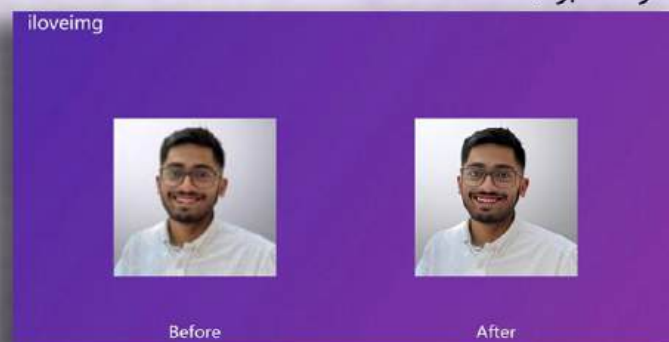


به طور کلی، این بهترین ابزار رایگان بالا بردن کیفیت عکس است که به صورت آنلاین پیدا کرده‌ایم. خوشبختانه طرح رایگان این ابزار محدودیت‌های زیادی ندارد و کاملاً رایگان محسوب می‌شود. البته همواره ابزار هوش مصنوعی ارتقا یافته و امکان تغییر این ارزیابی ممکن است.

قیمت: کاملاً رایگان

:iloveimg

iLoveIMG یک ابزار ساده برای افزایش کیفیت (رزولوشن) تصاویر تا دو یا چهار برابر است. برای استفاده از این ابزار، کافیست تصاویر خود را آپلود کرده و میزان افزایش کیفیت را انتخاب کنید. این برنامه به شما امکان آپلود سه تصویر به صورت همزمان و تنظیم جداگانه میزان افزایش کیفیت برای هر تصویر را می‌دهد. در تست اول، iLoveIMG عملکرد قابل قبولی دارد. همانطور که انتظار می‌رود، دخالت هوش مصنوعی در نتیجه مشهود است، اما کیفیت تصویر به اندازه ای افت نکرده است که غیرقابل استفاده باشد. به خصوص اگر از فاصله دور به تصویر نگاه کنید، اعوجاج‌ها قابل مشاهده نخواهند بود.

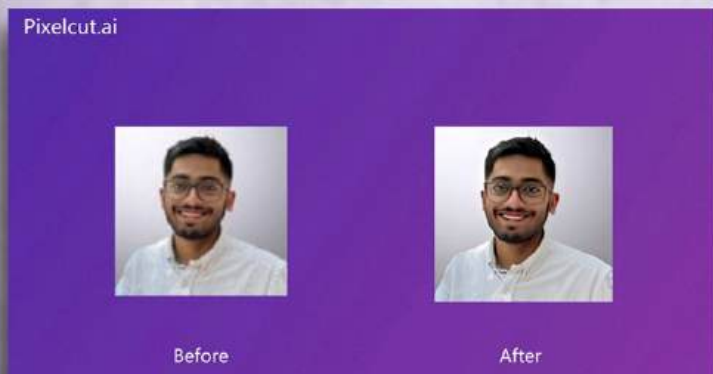


با این حال، ما نمی‌خواهیم تنها بر اساس یک تصویر نمونه در مورد این ابزار قضاوت کنیم؛ چرا که ممکن است روی تصویری با جزئیات کمتر یا تصویری که جزئیات آن به راحتی توسط هوش مصنوعی قابل بازسازی باشد، عملکرد بهتری داشته باشد. در تست دوم، Upscale.Media عملکرد نسبتاً خوبی از خود نشان می‌دهد. اما اگر تصویر را بزرگنمایی کنید، متوجه می‌شوید که برخی از عناصر انگار نقاشی شده‌اند. با این حال، این ابزار همچنان قابل استفاده است و ما از عملکرد آن ناراضی نیستیم.

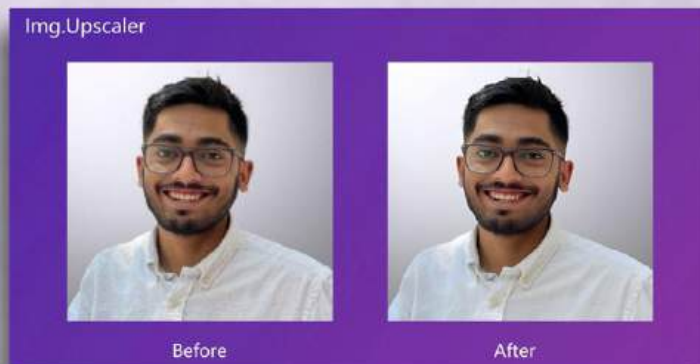


با Upscale.media می‌توانید سه تصویر را به صورت رایگان ارتقا دهید. فراتر از آن، باید اعتبارات اضافی خریداری کنید که به شما امکان ارتقا و دانلود تصاویر و همچنین افزایش رزولوشن خروجی را می‌دهد.

قیمت: رایگان / اعتبار اضافی: 9 دلار برای ۱۰ اعتبار
Pixelcut.ai: بالا بردن کیفیت عکس تا رزولوشن دو برابری از دیگر ابزارهای مناسب برای بالا بردن کیفیت عکس باید به Pixelcut.ai اشاره کنیم. نرم افزار Pixelcut.ai به صورت رایگان تنها امکان افزایش حداکثر دو برابری رزولوشن تصاویر را فراهم می‌کند. با این حال، در صورتی که به ابزارهای دیگری دسترسی ندارید، همچنان گزینه مناسبی به شمار می‌رود. در تست اول، عملکرد این ابزار به طرز شگفت انگیزی خوب است. اگرچه تصویر تا حدی مصنوعی به نظر می‌رسد، اما عملکرد آن نسبت به ابزار قبلی بهتر بوده و در حد سایر ابزارهای برتر لیست قرار می‌گیرد. خروجی تصویر حاوی جزئیات مصنوعی زیادی نیست و چهره همچنان قابل تشخیص است. بنابراین، این نرم افزار می‌تواند برای تصاویر با جزئیات قابل بازتولید، عملکرد بهتری داشته باشد.



این مورد در ابزارهایی که قبلاً بررسی کردیم، مشاهده نشد. با وجود این، Img.Upscaler به طور قابل توجهی کیفیت تصویر ورودی را بهبود می‌بخشد.



با ثبت نام در Img.Upscaler، ماهانه ۲۰ اعتبار رایگان دریافت می‌کنید. این بدان معناست که می‌توانید به صورت رایگان تا ۲۰ تصویر را در هر ماه با این ابزار ارتقا دهید. برای افزایش تعداد اعتبار ماهانه و همچنین رزولوشن نهایی تصاویر خروجی، می‌توانید از پلن‌های پریمیوم این سرویس استفاده کنید تا برای بالا بردن کیفیت عکس محدودیت خاصی نداشته باشید.

قیمت: رایگان / نسخه پولی: 19 دلار به بالا در سال
Upscale.Media: افزایش رزولوشن ۴ برابری عکس به طور رایگان

Upscale.Media یک ابزار جایگزین مناسب برای بالا بردن کیفیت عکس است که به شما امکان می‌دهد تصاویر را تا چهار برابر رزولوشن اصلی آن‌ها بزرگ دهید. این ابزار می‌تواند در صورتی که به سه ابزار برتر ذکر شده در این لیست دسترسی ندارید، مفید باشد. ما دو تصویر آزمایشی را با Upscale.Me-dia تا ۴ برابر رزولوشن اولیه‌شان افزایش دادیم. همچنین از گزینه "بهبود کیفیت" (Enhance Quality) که در دسترس قرار داشت، استفاده کردیم. اما آیا این گزینه تفاوتی ایجاد می‌کند؟ بیایید باهم بررسی کنیم.

پاسخ کوتاه این است که خیر، تفاوتی ایجاد نمی‌کند. در تست اول، نتایج متوسط بودند. بیشتر جزئیات تصویر به خوبی بازتولید نشده‌اند و تصویر کاملاً غیرطبیعی به نظر می‌رسد.



فایروال

وسایست های آن

چکیده مدیریتی:

فایروال دستگاه یا برنامه ای برای کنترل جریان ترافیک شبکه، بین دو شبکه یا میزبان با وضعیت امنیتی متفاوت می باشد. در گذشته فایروال ها اکثراً در لبه شبکه به کارگیری می شد. این کار بخشی از امنیت میزبان های داخلی را تامین می کند اما در مقابل تمام انواع و شکل های حمله موثر نیست؛ زیرا حملات از یک میزبان داخلی به دیگری و بدون عبور از فایروال های شبکه ارسال می شود. به همین دلیل و برخی دلایل دیگر، طراحان شبکه اغلب فایروال را در مکانی قرار می دهند که علاوه بر لبه شبکه، سایر تجهیزات و حتی دستگاه های قابل حمل را در یک لایه امنیتی قابل قبول، پوشش دهد. تهدیدات به تدریج دامنه عملکردشان را از لایه های پایین شبکه به لایه های بالاتر (لایه نرم افزار) منتقل می کنند که این امر موجب کاهش اثربخشی نظارت و تاثیر فایروال ها بر متوقف کردن تهدیدات در ارتباطات شبکه می شود. به هر حال فایروال ها هنوز هم لازم است اثرات این تهدیدات را در لایه های پایین شبکه متوقف کنند. همچنین فایروال ها می توانند بر لایه های نرم افزاری و در کنار سایر تجهیزات و تکنولوژی های امنیتی، نظارت هایی را داشته باشند.

فایروال ها توانمندی های متفاوتی در آنالیز ترافیک شبکه، مجوز دادن و جلوگیری کردن از موارد خاص را دارند. درک قابلیت انواع فایروال ها، طراحی سیاست های آن و اطلاع از تکنولوژی هایی که بتواند نیازمندی های سازمان را برطرف کند؛ برای حفاظت از ترافیک شبکه ضروری است. هدف از این مقاله آگاهی بخشی در خصوص تکنولوژی فایروال ها، قابلیت های امنیتی، مزایا و معایب آن می باشد. همچنین مثال هایی از محل نصب فایروال ها در شبکه، اثرات نصب فایروال در نقاط مختلف شبکه و توصیه هایی برای سازماندهی فایروال ها در زمان انتخاب، پیکربندی، راه اندازی و مدیریت آن را بررسی خواهیم کرد.

* برای افزایش اثربخشی و امنیت فایروال ها، عمل به توصیه های زیر لازم و ضروری می باشد:

سیاستی ایجاد کنید که مشخص کند فایروال ها با ترافیک های ورودی و خروجی چگونه باید رفتار کند. سیاست فایروال تعیین می کند چگونه فایروال در یک سازمان با ترافیک ورودی و خروجی، یک IP خاص یا دامنه خاصی از IP ها، پروتکل ها، برنامه ها، نوع محتوا و... بر اساس نیازها و سیاست های امنیت اطلاعات آن سازمان باشد.

همان طور که انتظار می رفت، این ابزار در تست دوم نیز عملکرد خوبی دارد. تصاویر خروجی از وضوح مناسبی برخوردار هستند و بافت آنها هنگام زوم کردن مصنوعی به نظر نمی رسد.

Pixelcut.ai



Before



After

Pixelcut.ai به شما امکان ارتقا رزولوشن تعداد محدودی از تصاویر را به صورت رایگان می دهد. با خرید نسخه پولی این نرم افزار، می توانید محدودیت تعداد تصاویر را برداشته و رزولوشن آنها را تا چهار برابر افزایش دهید.

قیمت: رایگان / نسخه پولی: 9.99 به بالا در ماه

سخن پایانی:

در این مطلب به ۴ ابزار هوش مصنوعی پرداختیم که برای بالا بردن کیفیت عکس حرف زیادی برای گفتن دارند. همانطور که توضیح دادیم، یکی از این ابزارها کاملاً رایگان است ولی باقی موارد با وجود اینکه بخشی از قابلیت های خود را رایگان ارائه می دهند، ولی برای بهره گیری از امکانات بیشتری باید از نسخه پولی آن ها استفاده کنید. همچنین با جستجو در اینترنت می توانید به ابزار دیگری نیز دسترسی پیدا کنید که در این مقاله گنجانده نشده است.

جزئیات ایجاد سیاست، به انواع مختلف فایروال بستگی دارد. البته بعضی از فایروال ها نیاز به بررسی عملکرد دارند و برای داشتن قوانین بهینه لازم است به قابلیت های آن ها توجه شود. به عنوان مثال برخی فایروال ها ترافیک شبکه را بر اساس مجموعه قوانین و به ترتیب از بالا به پایین مدیریت می کند. بنابراین لازم است قوانینی که بیشترین احتمال مطابقت با ترافیک شبکه مد نظر را داشته باشد، در بالاترین مکان قرار گیرد.

* معماری، سیاست ها، نرم افزار و سایر اجزای فایروال را در طول دوره زمانی استفاده از فایروال مدیریت کنید.

مدیریت فایروال جنبه های زیادی دارد، به عنوان مثال انتخاب نوع یا انواع فایروال برای قرار دادن در شبکه و تعیین محل قرارگیری آن در شبکه، به طور قابل توجهی بر سیاست های امنیتی فایروال تاثیرگذار است.



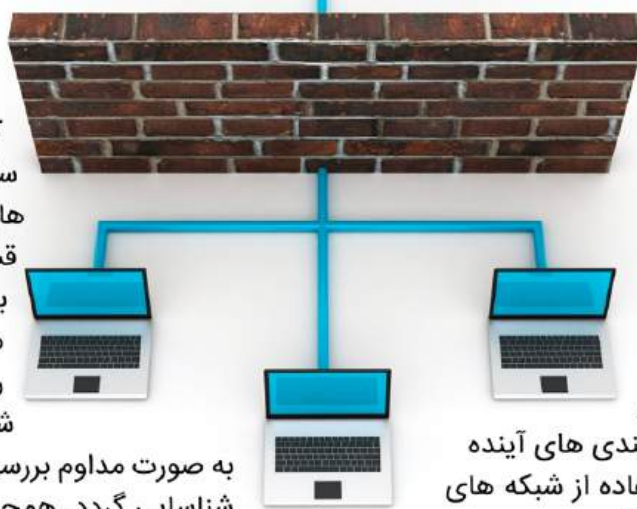
سازمان ها باید به سمت تهیه آنالیز ریسک هدایت شوند تا بتوانند لیست نوع ترافیک شبکه مورد نیاز و نحوه ایمن سازی آن را تهیه کنند. به عبارت دقیق تری می توان گفت IP های مجاز و پروتکل های لازم، مشخص کردن IP های منبع و مقصد مورد استفاده، انواع پروتکل های مورد استفاده (TCP، ICMP، VIP و...) مشخص شوند. به طور کلی می توان گفت تمام ترافیک های ورودی و خروجی (مگر مواردی که مورد نیاز سازمان باشند)، باید متوقف شوند. این موارد می توانند ریسک حملات را کاهش داده و حجم ترافیک ناخواسته شبکه سازمان را کاهش دهد.

* تمام نیازمندی ها را در نظر بگیرید، وقتی در حال تصمیم گیری برای انتخاب فایروال هستید ملاحظات زیادی برای انتخاب و برنامه ریزی فرآیندها در انتخاب فایروال مناسب یک سازمان وجود دارد.



قوانین و سیاست های فایروال باید همراه با تغییر الزامات، قوانین و تجهیزات سازمان به روز رسانی شود. به عنوان مثال به کارگیری یک نرم افزار جدید در سازمان نیازمند بروز رسانی سیاست های فایروال می باشد. عملکرد قسمت های مختلف فایروال نیز باید بررسی شوند تا مشکلات بالقوه منابع را شناسایی نموده و از آسیب رسانی به تجهیزات جلوگیری می شود. لاگ ها و هشدار سیستم باید

به صورت مداوم بررسی شوند تا تهدیدات موفق و ناموفق شناسایی گردد. همچنین مجموعه قوانین فایروال ها نیز باید به وسیله یک سیستم مدیریت تغییر کنترل شود؛ چراکه ایجاد خلل در امنیت و فعالیت های اقتصادی به صورت مستقیم وجود دارد. لازم است فایروال های نرم افزاری مطابق بانک آسیب پذیری های سازنده، به صورت مستمر به روز رسانی شوند.



سازمان ها باید تعیین کنند کدام ناحیه از شبکه باید محافظت شود و کدام نوع از تکنولوژی فایروال در حفاظت از نوع داده آن ناحیه موثرتر عمل می کند. همچنین ملاحظات در خصوص عملکرد فایروال و نگرانی هایی برای ادغام آن در شبکه و زیرساخت های امنیتی وجود دارد.

علاوه بر موارد مطرح شده، طراحی فایروال شامل ملزومات فیزیکی سازمان، کارکنان و در نظر گرفتن نیازمندی های آینده مانند بهره گیری از IPv6 با استفاده از شبکه های خصوصی مجازی (VPN) می باشد.

* قوانینی را به کار گیرید که از سیاست های سازمان پیروی کرده و در عین حال از قابلیت های فایروال پشتیبانی کند. مجموعه قوانین فایروال باید تا حد امکان نسبت به ترافیک شبکه ای که کنترل می کند، مشخص باشد. یکی از مواردی که باید در تعیین قوانین فایروال مورد توجه قرار بگیرد، پروتکل های مدیریتی خود فایروال است.

به مناسبت چهلمین سال تاسیس وزارت اطلاعات، دانشگاه اطلاعات و امنیت ملی برگزار می‌کند:

سومین همایش دوسالانه اطلاعات

سطح است آینده ما را نوظهور و فناوری‌ها

محورهای همایش

تاثیر فناوری‌های نوظهور بر:

کارکردهای اطلاعات

تحول مفاهیم در اطلاعات

حکمرانی اطلاعاتی

تعامل اطلاعات با سیاست و مردم

مهلت ارسال مقالات: ۳۰ مهر ۱۴۰۳

اعلام نتایج: ۳۰ آبان ۱۴۰۳

برگزاری همایش: آذر ۱۴۰۳

سایت همایش: conf.uins.ac.ir



وزارت اطلاعات
جمهوری اسلامی ایران



دانشگاه اطلاعات و امنیت ملی
U.I.N.S

ISC
Source World Science Citation Center



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

دانش با یادگیری زیاد بدست نمی آید،
چرا که همانا علم نور است که خدا در
قلب هر کس که هدایتش را بخواهد قرار
می دهد. رسول اکرم (ص)



سازمان حراست کل کشور
حراست کل استان البرز



فناوری
دریچه