انجمن علمی کامپیوتر
دانشگاه آزاد اسلامی واحد لاهیجان

گیلانو

- دستور پخت موفقیت در سئو
- اسکریپت X-UI (V2ray / Xray)
- خلق تصویر با هوش مصنوعی مولد
- و...

ماهنامه علمی دانشجویی - سال سوم - شماره چهل و سوم - ۳۰ اسفند ۱۴۰۳

فصـــــلِ دل‌شـــادِ بهـــاران می‌رسـد
ســـالِ نو، هنگـــامِ ســور و تازگی است
نغـــمه‌ی مـــاهور و شـــور و چـــارگـــاه
پـــاک شـــد ز ابر آســـمان، بیـــدار شد
صورتِ گـــل‌ها پر از رنـگ و خوشی است
چـــارمیـــن نـوروزِ گیـــــلانو شـــده
ای عزیـــزان، ســـــالِ نـو پیـــروز باد

نغـــزیِ ســرما به پـایـــان می‌رسـد
شـورِ رویـش، مثلِ توفـان می‌رسـد
از سرایِ مرغِ خوش‌خـوان می‌رسـد
مِـهر، تابـان، حال‌پُرســان می‌رسـد
چرخشِ گَردان، به درمـان می‌رسـد
علم بَس، چون اشکِ باران می‌رسـد
کارها امســال، سامـــان می‌رسـد

فرهاد فخری
ویراستار نشریه گیلانو

گیلانو

همیشه به خود اعتماد داشته باشید. اگر یک بار کاری را با موفقیت انجام داده باشید، باز هم می‌توانید.
آنتونی رابینز

- ماهنامه علمی دانشجویی - سال سوم - شماره چهل و سوم - ۳۰ اسفند ۱۴۰۳
- صاحب امتیاز: انجمن علمی مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد لاهیجان
- مدیر مسئول: سورنا کریمی سلیمی
- سردبیر: ریحانه محمدپور
- ویراستار: فرهاد فخری
- طراحی جلد و صفحه‌آرایی: معصومه چنانهن
- هیأت تحریریه:

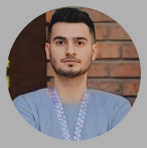
مائده عاشوری، فرشته قدیمی، ریحانه محمدپور، فرها فخری، سورنا کریمی سلیمی، مطهره عاشوری، امیرحسین شبرنگ، حجت آزادروش

فهرست

سخن سردبیر

ریحانه محمدپور
دانشجوی کارشناسی مهندسی کامپیوتر

سلام و درود خدمت تمامی همراهان نشریه‌ی گیلانو!
آغاز سال جدید و و فصل بهار که پر از تازگی و شادابی است را خدمتتان تبریک عرض می‌کنم و امیدوارم این فصل جدید، خوشحالی و موفقیت و سلامتی را برای همگان به ارمغان بیاورد. خوشحالم که در کنار هم در این مسیر پیشرفت کردیم و هر لحظه‌ای که با هم گذراندیم، ارزشمند بوده‌است.
سال نو فرصتی است تا با نگاهی تازه به زندگی و هدف‌هایمان توجه کنیم و برای پیشرفت هر چه بیشتر تلاش کنیم. این فصل، دعوتی است برای رشد و شکوفایی. بیایید باهم و در کنار هم، این فصل را به‌عنوان فرصتی برای اهدافمان و تلاش برای تحقق آن‌ها در نظر بگیریم.
از صمیم قلب از همه‌ی شما عزیزانی که تا به امروز در کنار ما بوده‌اید تشکر می‌کنم. مقالات و تلاش‌های شما باعث پیشرفت و ارتقای کیفیت نشریه شده و ما را در مسیر موفقیت یاری کرده و افتخارات و تجربیات زیادی کسب کردیم. این همکاری‌ها موجب شده‌است تا گیلانو به یکی از منابع معتبر علمی تبدیل شود.
این روحیه‌ی همیاری و کمک به یکدیگر، نه‌تنها فضای نشریه را گرم‌تر و صمیمی‌تر می‌کند، بلکه باعث می‌شود همه‌ی ما در کنار هم، به سطح بالاتری از دانش و مهارت برسیم و در سال جدید، با تقویت این دوستی‌ها و همکاری‌های بیشتر، به یکدیگر کمک کنیم تا هر یک از ما بهترین نسخه‌ی خود را ارائه دهد.
هر یک از شما با زحمات و ایده‌های خلاقانه‌تان، نقش مهمی در پیشرفت و ارتقای کیفیت نشریه ایفا کرده‌اید. امیدوارم که بتوانید در این سال جدید، زندگی‌ای سرشار از خوش‌بختی و موفقیت را تجربه کنید.
با آرزوی سالی پربار و موفق برای همه‌ی شما عزیزان.



سخن مدیر مسئول

سورنا کریمی سلیمی
دانشجوی کارشناسی مهندسی کامپیوتر

به نامِ خالقِ دانش که بِنْماید مسیر نو
سپاس از یاورِ دانش که نام آوَرْد گیلانو
«فرهاد فخری»

یک سال دیگر را پشت سر گذاشتیم؛ سالی پر از تجربه‌های ارزشمند، چالش‌های گوناگون و دستاوردهایی که همگی حاصل تلاش، همدلی و پشتکار اعضای پرتلاش جامعه‌ی علمی و دانشجویی بود. نوروز، نه‌تنها نشانه‌ی آغاز بهاری دیگر، بلکه فرصتی است برای تأمل بر مسیر طی‌شده و ترسیم افق‌های روشن‌تر برای آینده‌ای که در پیش داریم.

به‌عنوان مدیر مسئول نشریه‌ی گیلانو و دبیر انجمن علمی مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد لاهیجان، بر خود واجب می‌دانم که از تک‌تک افرادی که در این مسیر همراه ما بودند، از صمیم قلب قدردانی کنم. از تمامی اعضای نشریه، نویسندگان، طراحان، ویراستاران و تمامی عزیزانی که در تولید و انتشار مطالب علمی، فرهنگی و تخصصی سهیم بودند، بی‌نهایت سپاسگزارم. همچنین از اعضای انجمن علمی مهندسی کامپیوتر، اساتید گران‌قدر، دانشجویان علاقه‌مند، عوامل پرتلاش تیم اجرایی و تولید محتوای انجمن و تمامی افرادی که در شکل‌گیری و پیشرفت این انجمن نقش ایفا کردند، نهایت تشکر و قدردانی را دارم.

خانواده‌ی انجمن علمی مهندسی کامپیوتر، چیزی فراتر از یک تیم علمی است؛ این انجمن خانه‌ای برای خلاقیت، یادگیری، رشد و همدلی است. هر عضو این خانواده، نه‌تنها با دانش و مهارت خود، بلکه با انرژی، انگیزه و روحیه‌ی همکاری، این فضا را به بستری زنده و پویا برای رشد فردی و جمعی تبدیل کرده‌است. در کنار هـــم، ایده ایده‌هایی را به واقعیت بدل کردیم، پروژه‌هایی را به ثمر رساندیم و در مسیری که دشواری‌های خود را داشت، به جلو حرکت کردیم. این انجمن، جایی است که موفقیت‌های فردی، دستاوردهای جمعی را رقم می‌زند و هر گامی که در آن برداشته می‌شود، راهی تازه برای آینده‌ای روشن‌تر می‌گشاید.

در طول این سال، باهم رویدادهای بزرگی را رقم زدیم. برگزاری دوره‌های برنامه‌نویسی و کارگاه‌های آموزشی که بستری برای یادگیری و رشد مهارت‌های فنی و علمی بود، تجربه‌ای ارزشمند برای اعضای انجمن محسوب می‌شود. کسب رتبه‌ی سوم در مسابقه‌ی برنامه‌نویسی آنلاین AZAD CODE و همچنین، شرکت در مسابقات ICPC2023، ICPC2024 و برنامه‌ریزی و تشکیل تیم برای ICPC2025، نقطه‌ی عطفی در فعالیت‌های رقابتی ما بود. بازدید از نمایشگاه الکامپ فرصتی کم‌نظیر برای آشنایی با فناوری‌های نوین و تعامل با فعالان صنعت فناوری اطلاعات فراهم کرد. در این میان، تیم بارگذاری مدارک که در فرایند ثبت‌نام ورودی‌های مهر و بهمن سال ۱۴۰۳ دانشگاه آزاد اسلامی واحد لاهیجان نقشی کلیدی ایفا کرد، نشان از همدلی و تعهد اعضای انجمن دارد. همچنین مراسم معارفه‌ی نودانشجویان مهندسی کامپیوتر ورودی نیم‌سال مهر ۱۴۰۳ به‌عنوان نقطه‌ی آغازین مسیر دانشجویان جدید، نقش مهمی در آشنایی و ارتباط بهتر آن‌ها با فضای علمی و اجرایی انجمن داشت. اما بی‌تردید، یکی از مهم‌ترین رویدادهای امسال، همکاری انجمن علمی مهندسی کامپیوتر در برگزاری هفتمین کنفرانس بین‌المللی بازشناسی الگو و تحلیل تصویر (IPRIA2025) بود که فرصتی بی‌نظیر برای تعامل با پژوهشگران برتر و مشارکت در یک رویداد علمی معتبر فراهم کرد.

همه‌ی این رویدادها، تجربه‌های تازه‌ای بودند که ما را به یکدیگر نزدیک‌تر کرده و زمینه‌ی رشد فردی و گروهی را فراهم ساختند. هر لحظه‌ی این مسیر، درس‌های ارزشمندی برای ما داشت که در ادامه‌ی مسیر انجمن تأثیرگذار خواهند بود.

در این میان، تشکر ویژه‌ای دارم از هیأت مدیره‌ی انجمن علمی مهندسی کامپیوتر که همواره در تمام این مسیر، با همه‌ی فراز و نشیب‌ها و چالش‌های خاص خود، کنارم بودند و باهم توانستیم بر همه‌ی این موانع غلبه کنیم. همراهی، تعهد و تلاش بی‌وقفه‌ی این عزیزان، نیروی محرکه‌ی این انجمن بوده و هست و بدون آن‌ها، بسیاری از دستاوردها محقق نمی‌شد.
بدون شک، هیچ مسیری خالی از چالش و کاستی نیست. اگر در این مسیر کمبودی وجود داشت، تلاش خواهیم کرد که در سال جدید با همفکری و همراهی شما عزیزان، بهبود یابد و انجمن را به سطحی بالاتر برسانیم.
بدون تردید، موفقیت‌هایی که در طول این سال به دست آمد، نتیجه‌ی همکاری و تلاش جمعی تمامی شما عزیزان بوده‌است. هر ایده، هر پیشنهاد، هر مقاله، هر تلاش کوچک و بزرگ، سنگ بنایی برای ساختن آینده‌ای پربارتر و محیطی پویاتر برای یادگیری و پیشرفت بوده‌است.

اکنون که به استقبال سال ۱۴۰۴ می‌رویم، آرزو می‌کنم که این سال، سرشار از دستاوردهای علمی درخشان، رشد فردی و جمعی، و فرصت‌هایی بی‌نظیر برای پیشرفت و نوآوری باشد. امیدوارم در کنار یکدیگر، مسیرهای تازه‌ای را کشف کنیم، موانع را پشت سر بگذاریم و به قله‌های بالاتری از موفقیت دست یابیم.

مائده عاشوری
دانشجوی کارشناسی مهندسی کامپیوتر

شبکه‌های کامپیوتری از اجزاء و دستگاه‌های گوناگونی تشکیل شده‌اند که هر کدام وظیفه‌ی مشخصی دارند. شبکه‌های کامپیوتری از دو بخش نرم‌افزاری «اکتیو» و بخش سخت‌افزاری «پسیو» تشکیل شده‌اند. یکی از مهمترین دستگاه‌های اکتیو، دستگاهی به نام روتر است.

روتر چیست؟

روترها وظیفه دارند تا داده‌ها را بین شبکه‌های مختلف مسیریابی و منتقل کنند. اگر ما فقط یک شبکه داشته باشیم که در یک محدوده و رنج IP فعالیت می‌کند، و اگر فعالیت کاربران در درون شبکه باشد و با خارج از شبکه ارتباطی صورت نگیرد، نیازی به استفاده از روتر نیست.

روتر دستگاهی سخت‌افزاری است؛ اما می‌توان با بعضی از نرم‌افزارها، کارکرد روتر فیزیکی را شبیه‌سازی کرد. تفاوت روترهای سخت‌افزاری و نرم‌افزاری این است که روترهای نرم‌افزاری، توان و پایداری روترهای سخت‌افزاری را ندارند.

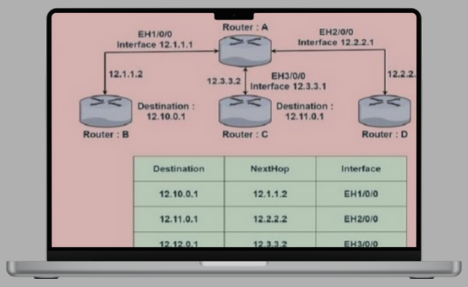
روتر در کدام لایه‌ی شبکه کار می‌کند؟

مسیریاب یا روتر همان‌طور که از نامش پیداست وظیفه‌ی مسیردهی به بسته‌های دیتا را از مبدأ به مقصد به عهده دارد. روترها در مدل OSI در لایه‌ی سوم شبکه یا همان Network کار می‌کنند. لایه‌ی نتورک «لایه‌ی شبکه» قلب یک شبکه است. روترها گاهی دو شبکه‌ی محلی را به هم وصل می‌کنند (LAN 2 LAN) و گاهی بین یک شبکه‌ی گسترده و شبکه‌ی محلی (LAN 2 WAN) قرار داده می‌شوند.

روتر چگونه کار می‌کند؟

در قدم اول یک روتر بایستی خود را به مودم و از مودم به سایر دستگاه‌های خانه یا دفترمان مانند کامپیوترهای شخصی و پرینتر متصل کند. بدین طریق دستگاه‌های موجود در شبکه قادرند با یکدیگر ارتباط داشته باشند. در گام بعدی به‌محض رسیدن یک بسته حاوی داده، روتر با نگاه کردن به آدرس IP آن که از پیش تعیین شده، تصمیم به هدایت بسته از طریق بستر اینترنت می‌گیرد. سپس با استفاده از جدول هدایت تعبیه‌شده در روتر و سایت‌های مربوطه، بهترین و کوتاه‌ترین مسیر انتقال بسته‌ی مشخص‌شده و بسته ارسال می‌گردد. نحوه‌ی کارکرد روتر بر اساس مدل OSI در لایه‌ی سوم (Network) قرار دارد. روترها در داخل خود یک جدول مسیریابی یا Routing Table دارند که بر اساس این جدول می‌توانند بسته‌ها را بین شبکه‌ها رد و بدل کنند. تصویری که مشاهده می‌کنید یک جدول مسیریابی است که در آن اطلاعاتی مانند آدرس شبکه‌های موجود، اولویت مسیرها (Metric) و روتر بعدی (Next Hop) بیان شده‌است.

جدول مسیریابی نوعی نقشه است که به بسته‌ی اطلاعات بهترین مسیر را برای رسیدن به مقصد خود نمایش می‌دهد.



روتر بر اساس این جدول مسیریابی، از مسیرهای موجود برای رسیدن به شبکه‌ی مورد نظر استفاده می‌کند. انواع روترها برای شبکه‌های بی‌سیم یا وایرلس و هم برای شبکه‌های کابلی مورد استفاده قرار می‌گیرند. روترهای بی‌سیم و روترهای کابلی، کارکرد یکسانی دارند تفاوت آن‌ها فقط در این است که از شبکه‌هایی با تکنولوژی‌های گوناگون پشتیبانی می‌کنند.

تفاوت روتر و سوییچ

سوییچ مسئول تحویل دادن بسته‌ها به تجهیزات مختلفی مثل روترها و سرور در داخل یک شبکه است. از سوییچ به‌عنوان پل دارای چند پورت نیز یاد می‌شود؛ چرا که از چندین پورت مختلف، داده‌ها را می‌گیرد و از آن‌جا به‌سمت مقصد نهایی ارسال می‌کند.

طرز کار سوییچ

در گام نخست، زمانی که یک کامپیوتر مبدأ، بسته‌ای را روانه‌ی کامپیوتر دیگری می‌کند، سوییچ این بسته را همراه آدرس MAC مبدأ و مقصد در قالب فریم می‌پیچد و از آن‌جا به مقصد می‌فرستد. در سمت گیرنده سوییچ این بسته را تجزیه کرده و با نگاه کردن به آدرس IP آن، فقط به کامپیوتری که آدرس MAC آن با محتوای موجود در بسته مطابقت داشته باشد می‌فرستد.

دو دستگاه پرکاربرد در بخش اکتیو شبکه، سوییچ و روتر است. همان‌طور که پیش‌تر ذکر شد، سوییچ‌ها در شبکه وظیفه دارند تا بسته‌ها را درون یک شبکه جابه‌جا کنند که به این فرایند سوییچینگ گفته می‌شود اما سوییچ‌ها توانایی این را ندارند که بسته‌ها را بین شبکه‌های دیگر تبادل کنند. آن‌ها می‌توانند درون یک Broadcast Domain داده‌ها را انتقال دهند؛ البته سوییچ‌های لایه‌ی سه می‌توانند کار مسیریابی را انجام دهند.

تفاوت روتر با مودم چیست؟ آیا روتر همان مودم است؟

معمولاً روتر و مودم به اشتباه با یکدیگر یکسان فرض می‌شوند، در صورتی که این دو کارکرد کاملاً متفاوتی دارند. مودم در شبکه وظیفه دارد تا داده‌ها را به‌سمت سرویس‌دهنده‌ی اینترنت (ISP) بفرستد و همچنین داده‌هایی را از سوی ISP دریافت کند. مودم (Modem) مخفف کلـمه‌های Modulator/Demodulator است و برای اینکه بتواند سیگنال‌های دیجیتالی را که از کامپیوتر دریافت می‌کند روی خط تلفن ارسال کند، آن‌ها را به سیگنال‌های آنالوگ تبدیل می‌کند و دقیقاً برعکس همین فرایند در مراکز ارائه‌دهنده‌ی اینترنت صورت می‌گیرد؛ یعنی سیگنال دیجیتال به سیگنال آنالوگ تبدیل می‌شود.

روتر دستگاهی است که داده‌ها را بین شبکه‌های مختلف مسیریابی می‌کند. به این کار روتینگ می‌گویند. برای مثال شما یک شبکه‌ی LAN دارید و همکار شما نیز یک شبکه‌ی LAN در طبقه‌ای دیگر دارد و هر دو شبکه رنج IP یا Broadcast Domain کاملاً متفاوتی با هم دارند. اگر شما بخواهید داده‌ای را برای همکارتان در شبکه‌ی دیگر ارسال کنید، باید حتماً از یک روتر استفاده کنید تا بتوانید داده‌ها را بین شبکه‌ها مسیریابی کنید. در غیر این صورت هیچ بسته‌ای نمی‌تواند خارج از محدوده‌ی شبکه ردوبدل شود.

Static Routing یا مسیریابی استاتیک

در روش مسیریابی استاتیک، مدیر شبکه به‌صورت دستی مسیرهایی برای روتر تعریف می‌کند؛ یعنی مدیر شبکه به‌صورت دستی روترها را پیکربندی و مسیرها را برای ارسال بسته‌های دیتا تنظیم می‌کند. جدول مسیریابی در این روش به‌صورت دستی ایجاد می‌شود و واضح است که این روش تنظیمات روتر در مورد شبکه‌های با روترهای کم و پیچیدگی کم مناسب است به این دلیل که اگر بخواهیم در روتری که در حال انجام مسیریابی استاتیک است تغییراتی بدهیم، باید تنظیمات تمام روترها را بر این اساس دوباره انجام دهیم و جدول مسیریابی آن‌ها را آپدیت کنیم. بر اساس روش مسیریابی استاتیک روتر بسته‌ها را فقط در این مسیرها انتقـال می‌دهد و اطلاعـات در مورد شبکه‌هایی کـــه به

اینترفیس روتر متصل شده‌است به‌صورت دستی در روتر ایجاد می‌شود. ما آن‌ها را به‌عنوان Connected Route می‌شناسیم.

Dynamic Routing یا مسیریابی دینامیک

در روش مسیریابی دینامیک، روتر بر اساس پروتکل‌های مسیریابی که توسط مدیر شبکه تنظیم شده‌است، بهترین مسیر را انتخاب می‌کند. مسیریابی دینامیک به روترها اجازه می‌دهد به‌وسیله‌ی پروتکل‌های روتینگ همدیگر را شناسایی کنند و مسیرهای شبکه را ایجاد و تنظیم کنند. پروتکل‌های مسیریابی به روتر کمک می‌کنند تا بهترین مسیر را برای انتقال بسته‌ها انتخاب کنند. برخی از پروتکل‌های مسیریابی عبارت‌اند از EIGRP، OSPF و IS-IS.

انواع روترها

۱- روتر بی‌سیم (Wireless Router): این نوع روترها با استفاده از اتصال کابل اترنت با مودم ارتباط برقرار می‌کند. مودم با تبدیل سیگنال‌ها و در اختیار قرار دادن بسته‌ها بر عهده‌ی روتر، وظیفه‌ی خود را انجام می‌دهد. حال روتر بی‌سیم یا Wireless Router با توزیع داده‌ها با استفاده از یک آنتن ارسال بسته‌ها را ممکن می‌سازد. نکته‌ای که وجود دارد، این است که روترهای Wireless، شبکه‌ی محلی یا LAN درست نمی‌کنند؛ اما درعوض تشکیل‌دهنده‌ی WLAN «شبکه محلی بی‌سیم» هستند.

۲- روتر سیمی (Wired Router): همانند مورد قبلی از اتصال کابل اترنت با مودم استفاده می‌کند اما با این تفاوت که به‌جای ارسال سیگنال داده‌ها با استفاده از آنتن، از سیم استفاده می‌کند. باید گفت که یک روتر سیمی، شبکه‌ی محلی (LAN) درست خواهد کرد.

۳- روتر هسته (Core Router): از این مدل از مسیریاب‌ها در شبکه‌های تخصصی یک سازمان یا شرکت استفاده می‌شود. روترهای معمولی که در خانه‌ها یا مکان‌های عمومی مانند رستوران‌ها استفاده می‌شود، با روترهای Core یا هسته تفاوت دارند. تفاوت این دو مدل در میزان حجم بسته‌های انتقالی و ارتباط آن‌ها با شبکه‌های دیگر است. یعنی ممکن است بسته‌ای که توسط روتر هسته ارسال می‌شود حجم کمتر یا بیشتری داشته باشد و همچنین امکان دارد که روتر با هیچ شبکه‌ی خارجی نیز در ارتباط نباشد.

۴- روتر مرزی (Edge Router): برخلاف روترهای هسته، روترهای مرزی با شبکه‌های خارجی و به‌خصوص اینترنت در ارتباط هستند. این نوع مسیریاب‌ها همگی در یک شبکه زندگی می‌کنند؛ یعنی به‌صورت مستقیم یا غیرمستقیم با یکدیگر ارتباط دارند. لازم به ذکر است که روتر مرزی از پروتکل دروازه‌ی مرزی (Border Gateway Protocol) یا به اختصار (BGP) برای برقراری ارتباط با شبکه‌های LAN و WLAN به‌منظور دریافت و ارسال بسته‌ها (Packets) استفاده می‌کند.

۵- روتر مجازی (Virtual Router): روتر مجازی یک روتر نرم‌افزاری و مبتنی بر ابر است که با استقرار روی سرورهای سخت‌افزاری x86، مسیریابی، سوییچینگ، امنیت، دسترسی VPN و سایر عملکردها را ارائه می‌کند. به‌کمک این روتر می‌توان اتصالات VPN را با دستگاه‌هایی که مستقیماً قادر به نصب نرم‌افزار VPN نیستند، مثل کنسول‌های بازی، بعضی از تلویزیون‌های هوشمند و برخی دستگاه‌های قدیمی‌تر به اشتراک گذاشت.

با این کار VPN روی رایانه‌ی شخصی شما فعال می‌شود و دستگاه دیگر به‌جای آنکه به روتر معمولی متصل شود، به شبکه‌ی رایانه‌ی شما وصل خواهد شد. درحقیقت رایانه‌ی شخصی به‌عنوان یک لایه‌ی محافظ میانی بین دستگاه‌ها عمل می‌کند.
این نوع مسیریاب عملکردی مشابه با یک روتر استاندارد فیزیکی را انجام می‌دهد با این تفاوت که به‌صورت مجازی و نرم‌افزاری اجرا می‌شوند. در حالت‌های مختلف ممکن است از VRRP (Virtual Router Redundancy Protocol) برای ایجاد روترهای مجازی اولیه استفاده شود. بزرگ‌ترین امتیاز روتر مجازی این است که با تنظیم رایانه‌ی خود به‌عنوان یک روتر مجازی، می‌توانید اتصالات VPN را با دستگاه‌هایی که نمی‌توانند مستقیماً نرم‌افزار VPN را نصب کنند به اشتراک بگذارید.

با عرض درود و خسته نباشید خدمت عزیزانی که در سال گذشته و هم سال‌های قبل تلاش کردند و باعث سربلندی و افتخار هیأت تحریریه و انجمن علمی مهندسی کامپیوتر شدند. ان‌شاءالله در سال جدید بتوانیم در کنار هم و با تلاش یکدیگر موفقیت بیشتری برای انجمن علمی به ارمغان بیاوریم. از خدای منان سعادت، سخاوت، سربلندی، سروری، سلامتی و سروری برای همه‌ی عزیزان خواستارم. عید نوروز بر شما دانشجویان آینده‌ساز مبارک!

فرشته قدیمی
دانشجوی کارشناسی روان‌شناسی

بازیدرمانی (Play Therapy) روشی است که در آن به کودکان کمک می‌شود تا احساسات و تجربیات و تفکرات خود را بیان کنند. بازی‌های رایانه‌ای به‌عنوان یکی از فعالیت‌های محبوب در دنیای امروز شناخته می‌شود که به‌عنوان یک روش درمانی جدید برای اصلاح ناهنجاری‌های موجود در نوار مغزی میتواند باعث کمک به بهبودی تمرکز در کودکان و نوجوانان مبتلا به اختلال نقص توجه / بیش‌فعالی می‌شود.

معرفی اختلال نقص توجه / بیش‌فعالی (ADHD)

اختلال نقص توجه / بیش‌فعالی (Attention Deficit / Hyperactive Disorder) یکی از شایع‌ترین اختلالات رفتاری دوران کودکی محسوب می‌شود. میزان شیوع این اختلال ۳ تا ۷ درصد گزارش شده‌است. هنوز علت این اختلال شناخته نشده‌است اما پژوهش‌های فراوانی از مبنای نورولوژیکی در این اختلال خبر می‌دهند که در این خصوص لوب پیشانی نقش فراوانی دارد. لوب پیشانی دارای ماهیت اجرایی است و در تمرکز و سازمان‌دهی دخالت دارد و همچنین رفتارهای بازدارنده مانند کنترل کردن رفتار حرکتی و بازداری از توجه متمرکز به محرک‌های نامربوط را به عهده دارد.

این اختلال نه‌تنها باعث کاهش تمرکز و توجه می‌شود، بلکه موجب مشـکل در روابط اجتماعـــی، نوع تعامل و نحوه‌ی واکنش‌دهی به دیگران می‌شود. متأسفانه این کودکان در پیدا کردن دوست و یا نگه داشتن آن دچار مشکل هستند و به‌سختی در گروه همسالان خود پذیرفته می‌شوند.

انواع روش‌های درمان

به‌طورکلی درمانهای اختلال نقص توجه / بیش‌فعالی به سه دسته‌ی کلی تقسیم می‌شود. دسته‌ی اول دارودرمانی است که بسیار رایج می‌باشد. دسته‌ی دوم رفتاردرمانی و دسته‌ی سوم درمان‌شناختی است.

دارودرمانی و رفتاردرمانی تا حدودی پاسخ‌گو هستند ولی نمیتواند به‌صورت مستقیم مشکلات را بهبود ببخشد. همچنین همهی کودکان نمی‌توانند پاسخ یکسانی دریافت کنند.

در درمان‌شناختی رویکرد اصلی، رویکرد بازتوانی است. در این رویکرد از تکالیف و تمرینهای شناختی جهت بهبود عملکرد استفاده می‌شود. یکی از این رویکردهای نوین برای کمک به تقویت و بازپروری اجزای شناختی، بازی‌های رایانه‌ای است.

بازی‌های رایانه‌ای از اصول زیربنایی درمان‌های شناختی به‌صورت توانایی تمرکز و سازمان‌دهی از طریق فراهم کردن فرصت‌هایی برای تمرین کردن جنبه‌های مختلف توجه و سازمان‌دهی استفاده می‌کند؛ خصوصاً بازی‌هایی که به‌طورخاص برای اهداف درمانی طراحی شده‌اند.

این بازی‌ها شامل تمرین‌های مکرر یک سری از تکالیف است که نیازمند سطوح متفاوت توجه است. فرض بر این است که فعال کردن مداوم توجه باعث تغییر در ظرفیت شناختی می‌شود. در کنار بازی‌های رایانه‌ای، بازی‌های حرکتی تأثیر به‌سزایی دارد. بازی‌های حرکتی به کنترل تکانه کمک می‌کند. زمانی که کودک کنترل بر بدن خود را یاد بگیرد، مغز بین سطح حرکتی و شناختی ارتباط برقرار می‌کند.

سودآوری از بازی‌های رایانه‌ای در درمان

مجموعاً بازی‌های رایانه‌ای و حرکتی فواید ذهنی، جسمی و روان‌شناختی برای کودکان دارای نقص توجه / بیش‌فعالی دارد. فواید ذهنی شامل مفاهیم اندازه، شکل، رنگ، وزن، فضا، فاصله، نماد دیداری و... است. فواید جسمی شامل پرورش یک بدن با کارآمدی بالا است که به زمان و مکان و اینکه چگونه در شرایط مختلف حرکت کند و عملکرد نشان دهد بستگی دارد. بدنی که اندام‌های حسی آن با بازدهی و دقت تمام در حال کار هستند، می‌توانند اطلاعات دقیق و مرتبطی را به مغز بدهند. فواید روان‌شناختی شامل کسب اعتماد به نفس به‌عنوان یک فرد مستقل، خودآگاه و دارای آزادی عمل است.

در این بازی‌ها پس از حل هزاران مشکل عینی (تمام بازی‌ها تا حدودی معمایی ساخته می‌شوند)، کودک توانایی زیادی در حل مسئله، سازمان دادن، تصویرسازی و ایجاد ارتباط به دست می‌آورد.

انواع بازی‌های رایانه‌ای برای درمان

۱- بازی‌های تمرکزی و استراتژیک: این نوع بازی‌ها نیاز به تفکر منطقی، برنامه‌ریزی و تصمیم‌گیری دارند.

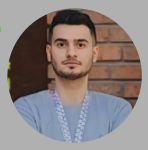
۲- بازی‌های پازل: بازی‌های پازلی می‌توانند به تقویت حل مسئله و تمرکز کمک کنند.

۳- بازی ورزشی: سبب افزایش هماهنگی و تمرکز می‌شوند.

۴- بازی‌های واقعیت مجازی (VR): این نوع بازی‌ها می‌توانند تجربه‌ای نوظهورکننده ارائه دهند که موجب کمک به تقویت توجه و تمرکز شوند.

کودکان مبتلا به اختلال نقص توجه / بیش‌فعالی در معرض خطر بیشتری از نظر ابتلا به اختلالات سلوک، خلقی، اضطرابی و یادگیری می‌باشند. باتوجه‌به این موضوع بهبود این اختلال یکی از مهم‌ترین اهداف درمانی می‌باشد که بسیار مشکل است. روش بازی‌های رایانه‌ای که روش جالـبی برای کودکان و نوجـوانان است، می‌تواند به‌عنوان یک روش مؤثر در افزایش توجه و تمرکز و سازمان‌دهی آن‌ها شود. البته باید توجه داشت که این بازی‌ها تحت نظر یک روان‌درمانگر باید انجام شود؛ زیرا استفاده‌ی نامناسب و بیش از حد، نه‌تنها تأثیر درمانی ندارد بلکه موجب گسترش اختلال می‌شود.

نوروز به‌عنوان یک جشن جهانی، یادآور این است که هر روز می‌تواند فرصتی جدید برای تحول و پیشرفت باشد. پس بیایید از این فرصت استفاده کنیم و با پذیرش تغییرات مثبت در زندگی‌مان، به سوی آینده‌ای روشن‌تر و شادتر حرکت کنیم. سال نو مبارک و امیدوار به موفقیت‌ها و شادی‌های بی‌پایان در سال جدید!



سورنا کریمی سلیمی
دانشجوی کارشناسی مهندسی کامپیوتر

در سال‌های اخیر، هوش مصنوعی مولد (Generative AI) به یکی از هیجان‌انگیزترین حوزه‌های یادگیری ماشین تبدیل شده‌است. این فناوری قادر است با تحلیل و یادگیری از مجموعه‌ای عظیم از داده‌ها، تصاویری خلق کند که از نظر کیفیت و جزئیات گاهی فراتر از توانایی‌های انسان به نظر می‌رسند. در این مقاله، به بررسی چگونگی عملکرد این سیستم‌ها، مدل‌های مطرح، کاربردها، ریاضیات و الگوریتم‌های مورد استفاده و چالش‌های پیش رو خواهیم پرداخت.

مبانی هوش مصنوعی مولد در خلق تصاویر

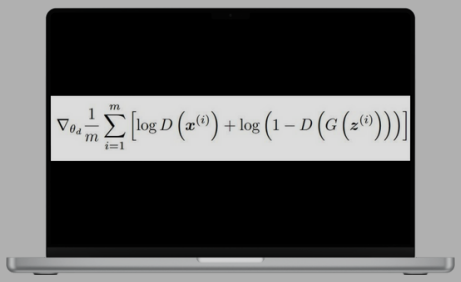
هوش مصنوعی مولد در زمینه‌ی تولید تصویر عمدتاً بر پایه‌ی دو معماری مهم عمل می‌کند: شبکه‌های مولد تخاصمی (GANs) و مدل‌های انتشار (Diffusion Models). این روش‌ها به مدل‌های پیچیده‌ی آماری و احتمالاتی متکی هستند که امکان تولید داده‌های جدید و واقع‌گرایانه را فراهم می‌کنند.

شبکه‌های مولد تخاصمی (GANs)

شبکه‌های مولد تخاصمی که توسط یان گودفلو و همکارانش در سال ۲۰۱۴ معرفی شدند، از دو شبکه‌ی عصبی تشکیل شده‌اند: یک شبکه‌ی مولد (Generator) که داده‌های مصنوعی تولید می‌کند و یک شبکه‌ی متمایزکننده (Discriminator) که سعی دارد واقعی بودن داده‌ها را تشخیص دهد. تعامل و رقابت بین این دو شبکه منجر به تولید تصاویری با کیفیت بالا می‌شود.

ریاضیات پشت GANs

GAN ها در چارچوب نظریه‌ی بازی‌های رقابتی کار می‌کنند. تابع هزینه‌ی (Loss Function) آن‌ها به‌صورت زیر تعریف می‌شود:



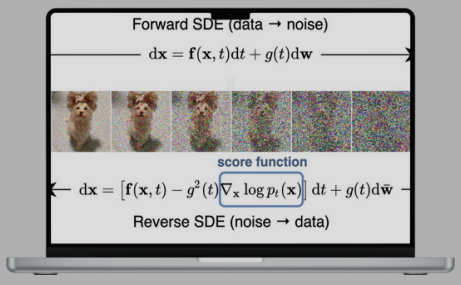
GAN ها به‌تدریج با یادگیری از داده‌های واقعی و اصلاح ضرایب خود، توانایی تولید تصاویر بسیار واقعی را کسب می‌کنند.

مدل‌های انتشار (Diffusion Models)

مدل‌های انتشار که اخیراً محبوبیت زیادی پیدا کرده‌اند، با افزودن نویز تصادفی به تصاویر و سپس یادگیری فرایند معکوس برای حذف نویز، قادر به تولید تصاویر دقیق و با جزئیات بالا هستند. مدل‌هایی مانند DALL·E 2 و Stable Diffusion نمونه‌هایی موفق از این روش هستند.

ریاضیات مدل‌های انتشار

مدل‌های انتشار بر فرایند تصادفی مارکوف متکی هستند که با استفاده از معادلات زیر توصیف می‌شود:



با آموزش مدل برای تخمین عکس نویز افزوده‌شده در هر مرحله، امکان بازسازی تصاویر واضح و واقعی فراهم می‌شود.

چگونگی خلق یک تصویر با هوش مصنوعی مولد

برای درک بهتر فرایند خلق تصویر، به مثالی از تولید تصویر چهره با استفاده از یک GAN توجه کنید:

- ابتدا نویزی تصادفی «مثلاً برداری از اعداد نرمال» به شبکه داده می‌شود.
- شبکه‌ی مولد این نویز را پردازش کرده و تصویری تولید می‌کند.
- شبکه‌ی متمایزکننده تصویر را تحلیل کرده و تشخیص می‌دهد که واقعی است یا جعلی.
- اگر تصویر غیرواقعی باشد، خطای محاسبه‌شده به مولد ارسال شده و آن را اصلاح می‌کند.
- این فرایند به‌صورت تکراری انجام می‌شود تا کیفیت تصویر به حد مطلوبی برسد.

کاربردهای هوش مصنوعی مولد در خلق تصاویر

هوش مصنوعی مولد در خلق تصویر کاربردهای متعددی در حوزه‌های مختلف دارد:

۱- هنر دیجیتال: هنرمندان از این فناوری برای خلق آثار منحصربه‌فرد و نوآورانه بهره می‌برند.

۲- صنعت بازی و فیلم‌سازی: تولید شخصیت‌ها، محیط‌ها و جلوه‌های ویژه با استفاده از AI موجب تسریع فرایند طراحی می‌شود.

۳- بازاریابی و تبلیغات: ایجاد محتوای بصری جذاب برای تبلیغات بدون نیاز به عکاسی سنتی.

۴- پزشکی: بازسازی تصاویر پزشکی برای تشخیص دقیق‌تر و شبیه‌سازی داده‌های بیمار.

۵- بازسازی تصاویر تاریخی: تصاویر قدیمی و بی‌کیفیت را می‌توان با استفاده از AI بازسازی و وضوح آن‌ها را افزایش داد.

چالش‌های هوش مصنوعی مولد

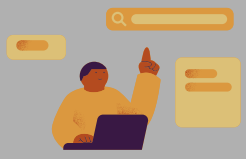
علی‌رغم پیشرفت‌های شگفت‌انگیز، این فناوری با چالش‌هایی نیز مواجه است:

۱- سوگیری‌های داده‌ای: مدل‌ها ممکن است داده‌های جانب‌دارانه را بازتولید کنند و تنوع فرهنگی و نژادی را به‌درستی منعکس نکنند.

۲- نقض حقوق مالکیت فکری: برخی مدل‌ها از آثار هنری موجود برای آموزش استفاده می‌کنند، که می‌تواند منجر به مسائل حقوقی شود.

۳- استفاده‌ی نادرست: تولید تصاویر جعلی یا دیپ‌فیک‌ها (Deepfakes) می‌تواند مشکلاتی در حوزه‌ی حریم خصوصی و اطلاعات نادرست ایجاد کند.

هوش مصنوعی مولد در زمینه‌ی خلق تصویر، دنیای جدیدی از امکانات را به روی ما گشوده‌است. مدل‌هایی مانند GAN و Diffusion توانسته‌اند تصاویری با جزئیات و وضوح بالا تولید کنند. با پیشرفت فناوری و بهبود مدل‌ها، انتظار می‌رود که کیفیت و دقت تولید تصاویر به سطحی بی‌سابقه برسد. با این حال، برای بهره‌برداری بهینه از این فناوری، توجه به مسائل اخلاقی و حقوقی نیز ضروری خواهد بود.



منابع:

1. Goodfellow, I., et al. (2014). **Generative adversarial networks**. *NeurIPS*.
2. Ho, J., et al. (2020). **Denoising diffusion probabilistic models**. *NeurIPS*.
3. Ramesh, A., et al. (2021). **Zero-shot text-to-image generation**. *ICML*.
4. Elgammal, A. (2019). **AI Art: History, Aesthetics, and Ethics**. *Leonardo Journal, MIT Press*.

مطهره عاشوری
دانشجوی کارشناسی مهندسی کامپیوتر

آیا می‌دانید میانگین جهانی هزینه‌ی نقض داده‌ها (Data Breach) در سال ۲۰۲۲ معادل ۳۵/۴ میلیون دلار بوده‌است؟ این آمار اهمیت امنیت شبکه‌های کامپیوتری را نشان می‌دهد. شبکه مجموعه‌ای از دو یا چند دستگاه محاسباتی متصل به هم است که به‌منظور اشتراک‌گذاری سخت‌افزار، نرم‌افزار، داده‌ها و اطلاعات و همچنین تسهیل در ارتباطات استفاده می‌شود.

تقریباً همه‌ی مشاغل امروزی برای مولد بودن به نوعی از شبکه متکی هستند؛ خواه یک شبکه‌ی LAN باشد که به کارمندان اجازه‌ی دسترسی به اینترنت را می‌دهد یا یک WAN که مکان‌های مختلف اداری را به هم متصل می‌کند یا یک شبکه به‌عنوان یک سرویس (Network as a Service – NaaS) که این عملکرد را در فضای ابری انجام می‌دهد. تأمین امنیت شبکه برای جلوگیری از دسترسی غیرمجاز به بخش‌های مختلف شبکه از مهم‌ترین کارهایی است که باید توسط سازمان‌ها انجام شود. حتماً می‌پرسید امنیت شبکه چیست؟ در این مقاله درباره‌ی امنیت شبکه (Network Security)، انواع و راه‌های تأمین آن صحبت خواهیم کرد.

امنیت شبکه چیست؟

امنیت شبکه (Network Security) مجموعه‌ای از شیوه‌ها و فناوری‌ها است که از زیرساخت شبکه در برابر حملات، دسترسی غیرمجاز و نقـــض داده‌ها محافظت می‌کند. امنیت شبکه را می‌توانیم به‌عنوان حوزه‌ای از امنیت سایبری مطرح کنیم که بر حفاظت از شبکه‌های کامپیوتری در برابر تهدیدهای سایبری متمرکز است.

سه هدف اصلی امنیت شبکه‌های کامپیوتری عبارت‌اند از:

- جلوگیری از دسترسی غیرمجاز به منابع شبکه
- شناسایی و متوقف کردن حملات سایبری و نقض امنیت داده‌ها
- اطمینان از دسترسی ایمن کاربران مجاز به منابع شبکه‌ی مورد نیازشان

معماری امنیت شبکه از ابزارهایی تشکیل شده‌است که از خود شبکه و اپلیکیشن‌هایی که روی آن اجرا می‌شوند، محافظت می‌کند. استراتژی‌های مؤثر امنیت شبکه از چندین خط دفاعی استفاده می‌کنند که مقیاس‌پذیر و خودکار هستند. هر لایه‌ی دفاعی مجموعه‌ای از سیاست‌های امنیتی تعیین‌شده توسط مدیر (Administrator) را اعمال می‌کند. امنیت شبکه با محافظت از یکپارچگی زیرساخت شبکه، منابع و ترافیک حملات سایبری را خنثی می‌کند و تأثیر مالی و عملیاتی آن‌ها را به حداقل می‌رساند.

چرا امنیت شبکه‌های کامپیوتری حائز اهمیت است؟

با بزرگ‌تر و پیچیده‌تر شدن شبکه‌ها خطر حملات سایبری نیز افزایش پیدا می‌کند. در دنیای امروز که اپلیکیشن‌ها کسب‌وکارهای بیشتری به‌سمت ابرهای خصوصی و عمومی در حال حرکت هستند و خرید سرور ابری رواج بیشتری پیدا کرده، امنیت شبکه‌های کامپیوتری نیز با چالش‌های بزرگ‌تری همراه شده‌است.

علاوه بر این، خود اپلیکیشن‌ها نیز به‌سمت مجازی‌سازی و توزیع در مکان‌های مختلف کشیده می‌شوند که برخی از آن‌ها خارج از کنترل فیزیکی تیم امنیت IT هستند. با افزایش روزافزون حملات سایبری به کسب‌وکارها و زیرساخت‌های سازمان‌ها، حفاظت از ترافیک شبکه و زیرساخت به یک امر ضروری و حیاتی تبدیل شده‌است.

امنیت شبکه چه مزایایی را به وجود می‌آورد؟

امنیت شبکه کلید توانایی سازمان در ارائه‌ی محصولات و سرویس‌ها به مشتریان و کارکنان است. از فروشگاه‌های آنلاین گرفته تا اپلیکیشن‌های سازمانی و دسکتاپ‌های از راه دور (Remote Desktops)، محافظت از اپلیکیشن‌ها و داده‌های روی شبکه برای پیشرفت و ترقی کسب‌وکار و همچنین اعتبار یک سازمان ضروری است.

نحوه‌ی عملکرد امنیت شبکه چگونه است؟

امنیت شبکه چندین لایه‌ی دفاعی را در لبه و شبکه ترکیب می‌کند، به‌طوری‌که هر لایه‌ی امنیتی شبکه سیاست‌ها و کنترل‌ها را پیاده‌سازی می‌کند. عناصر معماری امنیتی کامل و چند لایه که امنیت شبکه را در سراسر یک سازمان پیاده‌سازی می‌کنند، به دو دسته‌ی کلی تقسیم می‌شوند؛ کنترل دسترسی و کنترل تهدید که در ادامه به بررسی آن‌ها خواهیم پرداخت:

۱- کنترل دسترسی (Access Control): امنیت شبکه با کنترل دسترسی شروع می‌شود. در بخش کنترل دسترسی، دسترسی به داده‌ها و نرم‌افزارهای مورد استفاده برای جلوگیری از دست‌کاری آن داده‌ها محدود می‌شود. کنترل دسترسی برای جلوگیری از دسترسی غیرمجاز و کاهش خطر تهدیدهای داخلی بسیار مهم است. اگر عوامل مخرب به یک شبکه دسترسی پیدا کنند، می‌توانند با نظارت بر ترافیک و نقشه‌برداری از زیرساخت، اقدام به حمله‌ی DDoS کرده یا بدافزار وارد کنند.

۲- کنترل تهدید (Threat Control): حتی باوجود کنترل دسترسی نیز ممکن است مشکلاتی ایجاد شود. به‌عنوان‌مثال، یک عامل بد ممکن است از اعتبار یک کارمند برای ورود به شبکه استفاده کند. بنابراین نیاز به کنترل تهدید (Threat Control) کاملاً احساس می‌شود که در ترافیکی که قبلاً مجاز اعلام شده‌است عمل کند. کنترل تهدید از اقدامات عوامل مخرب برای آسیب رساندن به شبکه جلوگیری می‌کند.

فناوری‌های کنترل تهدید با فایروال ولود بالنسر (Load Balancer) شروع می‌شود. این دستگاه‌ها از شبکه در برابر حملات DoS و DDoS محافظت می‌کنند. در مرحله‌ی بعد، IDS/IPS با حملات شناخته‌شده که از طریق شبکه انجام می‌شود، مقابله می‌کند. درنهایت اشیای بدافزار ناشناخته‌ای که در شبکه حرکت می‌کنند، با فناوری‌های Sandbox گرفته می‌شوند؛ در حالی که ناهنجاری‌ها در ترافیک شبکه که ممکن است نشانه‌هایی از یک تهدید باشند، با NTA/NDR شناسایی می‌شوند.

انواع امنیت شبکه از نظر تکنولوژی

سیستم‌های امنیتی شبکه در دو سطح کار می‌کنند؛ در محیط و در منابع داخلی شبکه. کنترل‌های امنیتی در محیط تلاش می‌کنند تا از ورود تهدیدهای سایبری به شبکه جلوگیری کنند. اما گاهی اوقات مهاجمان شبکه موفق به نفوذ می‌شوند؛ بنابراین تیم‌های امنیت IT باید کنترل‌هایی را در اطراف منابع داخل شبکه مانند لپ‌تاپ‌ها یا داده‌ها نیز اعمال کنند. این استراتژی یعنی لایه‌بندی کنترل‌های چندگانه بین هکرها و آسیب‌پذیری‌های احتمالی را (Defense in Depth) می‌نامند.

IDPS / IDS / IPS

IDS بر اساس میزان ترافیک شبکه تعیین می‌کند که آیا نیاز به حضور یک نیروی انسانی به‌صورت تمام‌وقت وجود دارد یا خیر؛ IPS با ارائه‌ی همکاری حرفه‌ای‌تر، نیاز به نیروی انسانی را کاهش می‌دهد. IPS با توانایی شناسایی و منهدم کردن بسته‌های خطرناک قبل از اینکه وارد عملیات شوند امنیت سایبری شبکه را افزایش می‌دهد.

IDS چیست؟

تکنولوژی IDS مخفف Intrusion Detection System است که یک نوع سیستم تشخیص نفوذ بسته‌های ارسالی به حساب می‌آید؛ یعنی هر بسته‌ای که به شبکه ارسال شود توسط این سیستم تجزیه و تحلیل می‌شود تا عامل ایجاد اخلال نباشد. اگر هر گونه مورد مشکوکی را در آن ببیند حتماً برای مدیر شبکه هشدارهایی را ارسال می‌کنند تا در این خصوص چاره‌ای بیندیشند. این سیستم IDS باعث تجزیه و تحلیل ترافیک شبکه می‌شود و در این زمینه IPS شباهت بسیار زیادی دارد یعنی هر گونه بسته‌ی مشکوک توسط آن‌ها شناسایی می‌شود و کاری می‌کنند تا دیگر ادامه‌ی فعالیت نداشته باشد.

IPS چیست؟

وظیفه‌ی این تکنولوژی برقراری امنیت است. IPS هم دقیقاً همین کار را می‌کند؛ یعنی این سیستم‌ها از نفوذ مطالب بیگانه جلوگیری می‌کنند و یک زیرساخت عالی برای شبکه هستند و امنیت کار را تنظیم می‌کنند. اگر قرار باشد حملات سایبری اتفاق بیفتد هر دو تکنولوژی از این اتفاق جلوگیری می‌کنند. درواقع تشخیص آن‌ها از طریق مطابقت اطلاعات و مشخصات داخل دیتابیس انجام می‌شود تا متوجه شود که کدام اطلاعات نفوذی است. IDS باعث تغییر شبکه نمی‌شود و فقط آن را اعلام می‌کند اما در مورد IPS شرایط کمی متفاوت است. اگر مشکلی در بسته ببیند سریعاً وارد کار شده و مانع از تحویل آن بسته خواهد شد.

تفاوت این دو تکنولوژی این است که هر دو برای ردیابی و نظارت استفاده می‌شوند؛ به عبارتی IDS به‌عنوان یک سیستم کنترلی معرفی می‌شود که بر اساس یکسری از قوانین مشخص می‌کند که آیا فلان بسته مورد تأیید بوده یا باید آن را رد کرد. از طرفی به یک نیروی انسانی نیاز دارد تا بتواند تمامی نتایج را مورد بررسی قرار دهد و آن نیروی انسانی هم مشخص می‌کند که اکنون باید چه اقداماتی صورت گیرد، در حالی که در IDS نیاز به نظارت دائمی انسان بر مانیتورینگ شبکه وجود دارد. IPS چنین نیازی را از بین می‌برد.

IPS با توانایی شناسایی منهدم کردن بسته‌های خطرناک قبل از اینکه وارد عملیات شوند امنیت سایبری شبکه را افزایش می‌دهد. این ویژگی باعث می‌شود که IPS نسبت به IDS یک گزینه‌ی بسیار کارآمد و امن‌تر باشد. بنابراین اگر به‌دنبال یک راه‌کار امنیتی، کارآمد و خودکار برای شبکه خود هستید، IPS می‌تواند یک گزینه‌ی مناسب برای کار شما باشد. به‌طورکلی انتخاب بین IDS و IPS بستگی به نیازهای خاص شبکه‌ی شما دارد.

یک سیستم تشخیص و جلوگیری از نفوذ (IDPS) که گاهی اوقات IPS نامیده می‌شود، می‌تواند به‌طور مستقیم پشت فایروال «نرم‌افزار یا سخت‌افزاری که از دسترسی به کامپیوتر جلوگیری می‌کند» مستقر شود تا ترافیک ورودی برای تهدیدهای امنیتی را اسکن کند. ابزارهای امنیتی IDPS از سیستم‌های تشخیص نفوذ (IDS) تکامل پیدا کرده‌اند که فقط فعالیت‌های مشکوک را برای بررسی علامت‌گذاری می‌کنند. این قابلیت به IDPS ها اضافه شده‌است که به‌صورت خودکار به نقض‌های احتمالی مانند مسدود کردن ترافیک یا تنظیم مجدد اتصال پاسخ دهند. IDPS ها به‌ویژه در تشخیص و مسدود کردن حملات DoS، Brute Force و DDoS مؤثر هستند.

خطرات رایج امنیت شبکه

شبکه‌های کامپیوتری مانند هر دارایی تجاری دیگری به روش‌های مختلفی در معرض خطر قرار دارند. تهدیدهایی که شبکه‌ها به‌طور معمول باید برای آن آماده شوند، عبارت‌اند از:

۱- دسترسی غیرمجاز: اگر یک کاربر غیرمجاز به یک شبکه دسترسی پیدا کند، می‌تواند اطلاعات محرمانه‌ی آن شبکه را مشاهده کند. عوامل مخرب با دسترسی غیرمجاز به شبکه‌های کامپیوتری می‌توانند داده‌های محرمانه را افشا کنند یا سیستم‌های داخلی را به خطر بیندازند.

۲- حملات DDoS: حملات DDoS با ارسال ترافیک ناخواسته به مقدار زیاد باعث کندی یا از دسترس خارج شدن سرویس برای کاربران مجاز می‌شود.

۳- سوءاستفاده از آسیب‌پذیری: مهاجمان می‌توانند از آسیب‌پذیری شبکه در پرتال‌های ورود، برنامه‌ها، سخت‌افزار یا سایر مناطق برای نفوذ به شبکه برای اهداف مخرب مختلف استفاده کنند.

۴- آلودگی‌های بدافزار (Malware infections): از آلودگی‌های رایج بدافزاری می‌توان به باج‌افزارها (Ransomware) اشاره کرد که داده‌ها را رمزگذاری می‌کنند یا از بین می‌برند و با این عمل دسترسی کاربران به شبکه را محدود می‌کنند. کرم‌ها (Worms) بدافزارهایی هستند که می‌توانند به‌سرعت در سراسر شبکه تکثیر شوند. نرم‌افزارهای جاسوسی (Spyware) که به مهاجمان اجازه می‌دهند تا اقدامات کاربر را ردیابی کنند نیز از انواع دیگر بدافزار هستند. بدافزار می‌تواند از منابع مختلفی از جمله وب‌سایت‌های ناامن، دستگاه‌های آلوده‌ی کارمندان یا حملات خارجی هدفمند وارد شبکه شود.

۵- تهدیدات داخلی: کارمندان یا پیمان‌کاران داخلی می‌توانند به‌طور ناخواسته امنیت شبکه را تضعیف کنند یا در صورت ناآگاهی از شیوه‌های امنیتی، داده‌ها را افشا کنند. در موارد دیگر، کاربران ممکن است عمداً یک شبکه را به خطر بیندازند یا باتوجه‌به دلایل شخصی خود باعث افشای اطلاعات شوند.

راه‌های تأمین امنیت شبکه‌های کامپیوتری

در این بخش قرار است به بررسی راه‌های تأمین امنیت شبکه بپردازیم تا بتوانیم تا حد قابل‌توجهی از حمله به شبکه داده‌ها و اطلاعات مهم سازمان‌ها جلوگیری کنیم:

۱- پشتیبان‌گیری از داده‌ها و ذخیره‌ی چند فایل پشتیبان: حتی شبکه‌ای که امنیت بسیار بالایی دارد نیز ممکن است در معرض حمله قرار گیرد. از دست دادن دسترسی جزئی یا کامل به داده‌ها و سیستم‌های داخلی می‌تواند برای یک کسب‌وکار مخرب باشد. نگه داشتن نسخه‌های پشتیبان از داده‌ها به کاهش تأثیر چنین حمله‌ای کمک می‌کند. بسیاری از مشکلات داده‌ها و آلودگی‌های بدافزاری به این دلیل اتفاق می‌افتند که کاربر به‌سادگی مرتکب اشتباه شده‌است. این اشتباه می‌تواند با باز کردن تصادفی پیوست ایمیل ناامن، ارائه‌ی اعتبار ورود به سیستم خود در نتیجه‌ی حمله‌ی فیشینگ (Phishing) یا اجازه‌ی دسترسی خارجی به روشی دیگر توسط کاربر اتفاق بیفتد. کارکنان داخلی و پیمان‌کاران باید از نحوه‌ی ایمن ماندن و محافظت از شبکه آگاه شوند.

۲- به‌کارگیری رویکرد اعتماد صفر (Zero Trust): شبکه‌های سنتی به‌صورت متمرکز طراحی و ایجاد می‌شدند و نقاط پایانی (Endpoints) کلیدی، داده‌ها و اپلیکیشن‌ها در محل قرار داشتند. سیستم‌های امنیتی شبکه سنتی روی جلوگیری از نفوذ تهدیدها به محیط شبکه متمرکز بودند؛ به طوری که درصورت ورود یک کاربر به شبکه، کاربر قابل‌اعتماد تلقی می‌شد و عملاً دسترسی نامحدودی به کل شبکه داشت.

با فراگیر شدن تحول دیجیتال و مهاجرت به محیط‌های ابری، شبکه‌های سنتی نیز در حال غیرمتمرکز شدن هستند. در حال حاضر، منابع شبکه در مراکز داده‌ی ابری، نقاط پایانی در محل و از راه دور و همچنین دستگاه‌های موبایل و اینترنت اشیا (IoT) وجود دارند.

پروتکل‌های امنیتی شبکه

پروتکل‌های امنیت شبکه مجموعه‌ی پروتکل‌هایی است که برای حفاظت از اطلاعاتی که در یک شبکه جریان دارد، استفاده می‌شود.

۱- IPSec: پروتکل IPSec یا همان (IP Security) احراز هویت داده‌ها، یکپارچگی و همچنین حریم خصوصی بین دو موجودیت را ارائه می‌دهد.

۲- SSL (Secure Sockets Layer): لایه‌ی سوکت ایمن یک مکانیزم امنیتی استاندارد است که برای حفظ یک اتصال اینترنتی امن بین سرویس‌گیرنده و سرویس‌دهنده استفاده می‌شود. در این پروتکل امنیتی با استفاده از رمزنگاری از تغییر داده‌های شخصی، بسته‌ها و جزئیات در حین ارسال و همچنین خواندن آن‌ها توسط مجرمان جلوگیری می‌شود.

۳- SSH (Secure Shell): پروتکل SSH یک پروتکل امنیتی شبکه است که ارتباطات و داده‌های شبکه را رمزنگاری می‌کند. این پروتکل به خط فرمان اجازه می‌دهد تا از راه دور وارد سیستم شود و وظایف خاصی را از راه دور انجام دهد. عملکردهای مختلف FTP در SSH گنجانده شده‌است. SSH-1 و SSH-2 جدیدترین نوع پروتکل‌های SSH هستند.

۴- استفاده از HTTPS: پروتکل HTTPS یا همان HyperText Transfer Protocol Secure یک پروتکل امنیت شبکه است که برای ایمن‌سازی ارتباطات داده بین دو یا چند سیستم استفاده می‌شود. از آن‌جایی که داده‌های منتقل‌شده از طریق HTTPS رمزگذاری می‌شوند، مجرمان سایبری قادر به تغییر داده‌ها در طول انتقال از مرورگر به وب‌سرور نیستند. حتی زمانی که مجرمان سایبری به بسته‌های داده دسترسی پیدا می‌کنند، به‌دلیل رمزگذاری قوی بسته‌ها قادر به خواندن و تفسیر آن‌ها نخواهند بود.

اطمینان خاطر از امنیت شبکه با سرویس امنیت ابری اَبر دِراک

امنیت ابری یکی از سرویس‌های ارائه‌شده توسط ابر دراک است که از شبکه شما در برابر حملات DDoS، بدافزارها و تهدیدهای سایبری محافظت می‌کند. ابر دراک شبکه ما را به‌صورت روزانه اسکن کرده و ترافیک ورودی را بررسی می‌کند. این ارائه‌دهنده‌ی سرویس امنیت ابری با استفاده از فایروال، ترافیک ورودی را فیلتر کرده و از ورود ترافیک مخرب قبل از رسیدن به شبکه‌ی شما جلوگیری می‌کند. ابر دراک حملات DDoS را نیز به‌صورت هوشمند تشخیص داده و دفع می‌کند.

با سلام و عرض ادب، سال نو «۱۴۰۴» شمسی یا به‌عبارتی عید نوروز باستانی را خدمت شما دانشجویان و دانش‌دوستان عزیز تبریک عرض می‌کنم. یک سال دیگر گذشت و ما همچنان در نشریه‌ی گیلانو پر قدرت در کنار شما هستیم و به انتشار اندک آگاهی‌مان ادامه می‌دهیم. امیدوارم سال جدید پر از موفقیت و دستاورد برای شما عزیزان باشد.

در این مقاله به بررسی اسکریپت (X-UI) خواهیم پرداخت. این اسکریپت با نام V2ray نیز معروف است. با شروع موج گسترده‌ی محدودیت اینترنت در ایران، حرکت کاربران به‌سمت استفاده از شبکه‌ی مجازی خصوصی (VPN) به‌عنوان محدودیت‌شکن یا به‌عبارتی فیلترشکن رفته‌رفته بیشتر شد. VPN هایی که از نوع PPTP، SSTP، OVPN، L2TP و... در بین کاربران ایرانی رواج داشت و با شدیدتر شدن محدودیت‌ها، کاهش پهنای باند، شناسایی این سرویس‌ها، کندی بیش از حد به‌دلیل کاهش پهنای باند و رمزنگاری قوی این نوع از VPN ها دیگر جواب نبود و اسکریپت جدید به اسم X-UI به بازار آمد که کانفیگ‌های مختلف با نوع اتصال گوناگون را شامل می‌شود که به کانکشن‌های آن V2ray گفته‌می‌شود.

X-UI چیست و چه هدفی دارد؟

X-UI یک پنل مدیریتی تحت وب «اسکریپت تحت وب» است که برای مدیریت هسته و کانفیگ‌های V2Ray و Xrayطراحی شده‌است. Xray نسخه‌ی ارتقاءیافته‌ی V2ray است که علاوه بر امکانات V2ray، قابلیت‌های بیشتری را نیز دارا می‌باشد. این ابزار به کاربران اجازه می‌دهد تا کانکشن‌های امن و خصوصی را با استفاده از پروتکل‌های مختلف مانند، Trojan، VLESS، VMess Shadowsocks و... ایجاد و مدیریت کنند.

هدف X-UI

هدف اصلی این پنل، سهولت در مدیریت و پیکربندی کانفیگ‌های V2ray/Xray است. در حالت عادی، مدیریت این اسکریپت و کانفیگ‌ها نیازمند ویرایش دستی فایل‌های JSON و اجرای دستورات پیچیده در ترمینال است؛ اما X-UI این فرایند را ساده کرده و یک رابط گرافیکی کاربرپسند برای انجام تنظیمات فراهم می‌کند.

ویژگی‌های کلیدی X-UI

۱- مدیریت آسان کانفیگ‌های V2ray/Xray بدون نیاز به خط فرمان.
۲- پشتیبانی از چندین پروتکل مانند ،VLESS، VMess Trojan و Shadowsocks.
۳- کنترل و نظارت بر کاربران از طریق داشبورد.
۴- اتصال امن و پایدار برای دور زدن فیلترینگ و افزایش حریم خصوصی.
۵- امکان تنظیم TLS و WebSocket برای امنیت بیشتر.
۶- قابلیت صدور لینک اشتراک (Subscription Link) برای کاربران.

بررسی کانکشن‌های پشتیبانی‌شده در X-UI

اسکریپت X-UI بر پایه‌ی Xray/V2ray ساخته شده‌است و از پروتکل‌های مختلفی برای اتصال امن و عبور از محدودیت‌ها پشتیبانی می‌کند. این پروتکل‌ها شامل موارد زیر هستند:
۱- VMess: پروتکل اختصاصی V2ray که برای رمزگذاری و تغییر مسیر ترافیک استفاده می‌شود.
۲- VLESS: نسخه‌ی بهینه‌شده و سبک‌تر از VMess که سرعت و کارایی بهتری دارد.
۳- Trojan: یک پروتکل شبیه به Shadowsocks، اما با امنیت بالاتر و امکان استفاده از TLS.

۴- Shadowsocks (SS): یک پروتکل پروکسی سبک و امن برای عبور از فیلترینگ.
۵- SOCKS5: پروتکل پروکسی که از احراز هویت و انتقال UDP پشتیبانی می‌کند.
۶- HTTP Proxy: یک پروتکل ساده برای تغییر مسیر ترافیک از طریق HTTP.

آیا اتصال‌های X-UI مبتنی بر VPN هستند یا پروکسی؟

اتصالات در X-UI مبتنی بر پروکسی هستند، نه VPN؛ اما در برخی موارد، این اتصال‌ها می‌توانند عملکردی مشابه VPN داشته باشند.

X-UI از پروتکل‌های پروکسی مانند VLESS، VMess، Trojan و Shadowsocks استفاده می‌کند، که همگی نوعی پروکسی پیشرفته محسوب می‌شوند و عملکرد متفاوت از VPN دارند.

تفاوت کلیدی

VPN هایی مثل OVPN، L2tp، OpenVPN یا WireGuard تمام ترافیک اینترنتی دستگاه را رمزگذاری و از یک تونل عبور می‌دهد.

پروکسی‌های X-UI مثل VMess و Shadowsocks فقط ترافیک برنامه‌های مشخصی را عبور می‌دهند، مگر اینکه از یک Global Mode استفاده شود که تمام ترافیک را به پروکسی هدایت کند. این ابزار بیشتر شبیه پروکسی‌های پیشرفته هستند که امکان دور زدن فیلترینگ و افزایش امنیت را فراهم می‌کنند.

ویژگی	پروکسی (X-UI)	VPN
شیوه‌ی کار	تغییر مسیر ترافیک از طریق یک سرور واسط	ایجاد یک تونل رمزگذاری‌شده برای تمام ترافیک
پوشش ترافیک	می‌تواند فقط ترافیک برخی برنامه‌ها را هدایت کند.	تمام ترافیک اینترنت را عبور می‌دهد.
امنیت	رمزگذاری دارد، اما به سطح VPN های قوی نمی‌رسد.	رمزگذاری بسیار قوی و جامع
سرعت	معمولاً سریع‌تر، مخصوصاً VLESS و Trojan	کندتر به‌دلیل رمزگذاری سنگین‌تر
دور زدن فیلترینگ	بسیار مؤثر، مخصوصاً در VMess و Trojan	در برخی موارد قابل شناسایی است.
یاز به نصب کلاینت خاص	بله، نیاز به نرم‌افزارهایی مثل V2rayN، Clash، NapsternetV و...	بله، نیاز به OpenVPN، WireGuard و...

- اگر به حداکثر امنیت و رمزگذاری کامل ترافیک نیاز دارید، VPN بهتر است.
- اگر به سرعت بالاتر، پایداری بیشتر و دور زدن فیلترینگ بهتر نیاز دارید، پروکسی‌های X-UI گزینه‌ی مناسب‌تری هستند.
- با استفاده از Global Mode در کلاینت‌ها، می‌توان Xray/V2ray را به‌گونه‌ای تنظیم کرد که مانند یک VPN عمل کند و کل ترافیک سیستم را از طریق پروکسی عبور دهد.

نحوه‌ی مدیریت کاربران در X-UI

X-UI امکانات مختلفی برای مدیریت کاربران دارد، از جمله:
۱- ایجاد کاربران جدید: می‌توان برای هر کاربر یک کانکشن اختصاصی تعریف کرد.
۲- تعیین حجم مصرفی (Traffic Limit): امکان مشخص کردن میزان حجم مصرفی کاربران و قطع دسترسی پس از رسیدن به سقف مجاز.
۳- تاریخ انقضاء (Expiration Date): تعیین مدت‌زمان اعتبار کانکشن کاربران «مثلاً ۳۰ روزه».
۴- مشاهده‌ی میزان مصرف کاربران: در بخش Statistics می‌توان مصرف پهنای باند کاربران را بررسی کرد.
۵- مسدودسازی کاربران (Disable/Delete): امکان غیرفعال کردن یا حذف کاربران درصورت نیاز.

نحوه‌ی تنظیم و استفاده از داشبورد گرافیکی X-UI

بعد از نصب X-UI، می‌توان به داشبورد تحت وب آن دسترسی داشت و سرور را به‌صورت گرافیکی مدیریت کرد.

مراحل ورود به داشبورد X-UI

۱- ابتدا با استفاده از SSH وارد سرور شوید.
۲- بررسی کنید که X-UI روی چه پورتی اجرا شده‌است. معمولاً پورت پیش‌فرض 54321 است.
۳- وارد مرورگر شوید و آدرس زیر را باز کنید:
http://your-server-ip:54321
۴- نام کاربری و رمز عبور را وارد کنید. «در اولین ورود، باید اطلاعات پیش‌فرض را تغییر دهید.»

امکانات مدیریتی در داشبورد X-UI

داشبورد X-UI امکانات مختلفی برای مدیریت سرور و کانکشن‌ها ارائه می‌دهد:

۱- ایجاد و مدیریت کانکشن‌ها

۱- انتخاب پروتکل مورد نظر (Trojan، VLESS، VMess، Shadowsocks) و...
۲- تعیین پورت، آی‌پی و روش رمزگذاری برای هر کانکشن.
۳- تنظیم TLS و WebSocket برای امنیت بیشتر.
۴- ارائه‌ی لینک اشتراک (Subscription Link) برای کاربران.

۲- مانیتورینگ و گزارش‌گیری

۱- مشاهده‌ی میزان پهنای باند مصرفی کاربران.
۲- بررسی وضعیت سرور و تعداد اتصالات فعال.
۳- امکان مشاهده لاگ‌های سیستم برای خطایابی.

۳- تنظیمات پیشرفته‌ی سرور

۱- تغییر پورت مدیریتی داشبورد برای افزایش امنیت.
۲- ایجاد گواهی‌نامه‌ی SSL برای رمزگذاری ترافیک.
۳- تعیین حداکثر تعداد کانکشن‌های همزمان برای کاربران.

بررسی سطح امنیت کانکشن‌ها در X-UI

X-UI که بر پایه‌ی Xray/V2ray ساخته شده‌است، از چندین روش رمزگذاری و پروتکل امن برای ایجاد کانکشن‌های رمزگذاری‌شده استفاده می‌کند. این ابزار به‌خوبی قادر است امنیت ارتباطات اینترنتی را تأمین کند و از دور زدن فیلترینگ به‌شکلی امن پشتیبانی کند.

۱- پروتکل‌های رمزگذاری‌شده در X-UI

X-UI از چندین پروتکل مختلف پشتیبانی می‌کند که هر کدام امنیت خاص خود را دارند. این پروتکل‌ها شامل:
۱- VMess: این پروتکل رمزگذاری قوی دارد و به‌طور ویژه برای استفاده در شبکه‌های محدود و تحت نظارت طراحی شده‌است و امنیت آن در برابر حملات MITM (Man-In-The-Middle) بسیار بالا است.
۲- VLESS: این پروتکل مشابه VMess است، اما بدون چک‌سام در فرایند ارتباط، که آن را برای عملکرد بهینه و سریع‌تر مناسب می‌کند. این پروتکل از TLS (Transport Layer Security) برای رمزگذاری استفاده می‌کند و امنیت بالایی دارد.
۳- Trojan: یک پروتکل که برای دور زدن فیلترینگ طراحی شده‌است و با استفاده ا زTLS تمام ترافیک را به‌طور امن رمزگذاری می‌کند. Trojanبه‌ویژه برای عبور از فیلترهای دقتی (Deep Packet Inspection) بسیار مؤثر است.

۲- روش‌های امنیتی در X-UI

۱- TLS (Transport Layer Security): این روش برای رمزگذاری ترافیک و محافظت از آن در برابر حمله‌ی مرد میانی (MITM) استفاده می‌شود.

۲- WebSocket: این فناوری برای عبور از فیلترهای شبکه و بهبود ارتباطات در شرایط خاص شبکه استفاده می‌شود.
۳- XTLS: یک روش بهینه‌شده در Xray که سرعت بیشتر و رمزگذاری بهتری نسبت به TLS ارائه می‌دهد.
۴- HTTP/2 و QUIC: این پروتکل‌ها می‌توانند برای بهبود عملکرد و افزایش امنیت استفاده شوند.
۵- Shadowsocks: این پروتکل به‌دلیل سبک بودن و سرعت بالا در بین کاربران محبوب است، اما امنیت آن نسبت به VMess و VLESS پایین‌تر است.
۶- SOCKS5: یکی از پروتکل‌های قدیمی پروکسی است که برای انتقال ترافیک اینترنت به‌صورت امن و با رمزگذاری نسبی استفاده می‌شود.

۳- مزایا و معایب X-UI نسبت به دیگر روش‌های مشابه

- مزایا

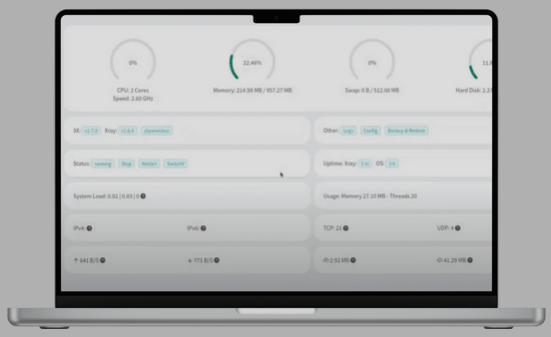
۱- امنیت بالا: استفاده از پروتکل‌های VMess، VLESS،Trojan و دیگر روش‌های رمزگذاری در X-UI امنیت بسیار بالایی را برای کاربران فراهم می‌کند. این ابزار در برابر حملات مختلف مانند MITM مقاوم است و ترافیک را به‌طور کامل رمزگذاری می‌کند.
۲- سهولت در استفاده: داشبورد گرافیکی X-UI این امکان را به کاربران می‌دهد که بدون نیاز به دستورات پیچیده‌ی ترمینال، تنظیمات امنیتی مختلف را پیکربندی کنند.
۳- پشتیبانی از پروتکل‌های مختلف: X-UI از پروتکل‌های متنوعی مثل Trojan، VLESS، VMess و Shadowsocks پشتیبانی می‌کند که هر کدام برای شرایط خاص و نیازهای متفاوت مناسب است.
۴- امنیت در برابر فیلترینگ: استفاده از WebSocket و TLS و XTLS به X-UI کمک می‌کند تا از فیلترهای شبکه عبور کند و حریم خصوصی کاربران را حفظ کند.
۵- افزایش سرعت: X-UI به کاربران این امکان را می‌دهد که با استفاده از پروتکل‌های بهینه‌شده مانند VLESS و XTLS، سرعت ارتباط خود را افزایش دهند.

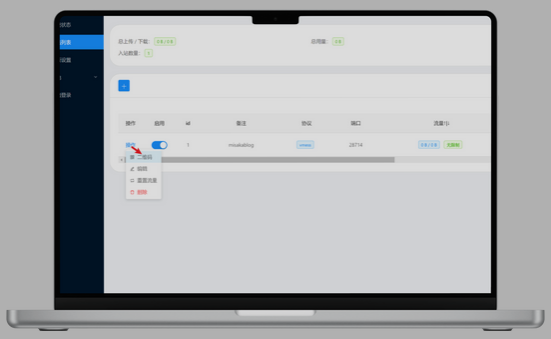
- معایب

۱- پیچیدگی تنظیمات برای مبتدیان: برای کسانی که آشنایی زیادی با مفاهیم شبکه و رمزگذاری ندارند، تنظیمات اولیه X-UI می‌تواند کمی پیچیده به نظر برسد، هرچند داشبورد گرافیکی این مشکل را تا حد زیادی کاهش می‌دهد.
۲- وابستگی به سرورهای خارجی: چون X-UI نیاز به سرور برای اجرای V2ray/Xray دارد، مشکلاتی مانند اختلال در سرور یا نصب و نگهداری سرور می‌تواند برای کاربران پیش بیاید.
۳- امنیت پایین‌تر در مقایسه با VPN: در حالی که پروتکل‌های X-UI مانند VMess و Trojan امنیت بسیار خوبی دارند، در مقایسه با VPN ها، که رمزگذاری و تونلینگ تمامی ترافیک اینترنتی را پوشش می‌دهند، ممکن است برای برخی موارد امنیت کمتری داشته باشند.
۴- نیاز به نرم‌افزار کلاینت خاص: برای استفاده از X-UI باید از نرم‌افزارهای کلاینت خاص مانند V2rayN، V2rayNG، یا Clash استفاده کنید که این ممکن است برای بعضی کاربران کمی دردسرساز باشد.

جمع‌بندی

X-UI یک ابزار قدرتمند برای مدیریت هسته و کانفیگ‌های V2ray و Xray است که امکان ایجاد کانکشن‌های امن با استفاده از پروتکل‌های مختلف را فراهم می‌کند. این ابزار امنیت بالایی را ارائه می‌دهد و به‌راحتی از طریق داشبورد گرافیکی قابل‌مدیریت است؛ اگرچه برای مبتدیان ممکن است پیچیدگی‌هایی داشته باشد و نسبت به VPN ها در پوشش کامل ترافیک محدودیت‌هایی دارد، اما برای کسانی که به‌دنبال امنیت بالا و دور زدن فیلترینگ با سرعت خوب هستند، X-UI یک گزینه‌ی بسیار مناسب است.





حجت آزادروش
دانشجوی دکتری مهندسی کامپیوتر – گرایش نرم‌افزار

در دنیای امروز، باتوجه‌به اهمیت بالای رقابت در فضای آنلاین، موفقیت سایت‌ها در موتورهای جست‌وجو به فاکتورهای مختلفی بستگی دارد. یکی از مهم‌ترین این فاکتورها، کیفیت محتوا و اعتبار سایت است که مستقیماً بر تجربه‌ی کاربری و رتبه‌بندی آن در نتایج جست‌وجو تأثیر می‌گذارد. گوگل برای ارزیابی کیفیت سایت‌ها از معیاری به نام E-A-T «تخصص، اعتبار، اعتماد» استفاده می‌کند که به سایت‌ها کمک می‌کند تا بر اساس این سه معیار مهم، در نتایج جست‌وجو دیده شوند. در این مقاله، به مفهوم E-A-T و روش‌های سنجش آن پرداخته و چک‌لیستی برای ارزیابی و بهبود این سه فاکتور مهم در سایت‌ها ارائه خواهیم کرد.

با آغاز سال نو و فرا رسیدن عید نوروز، امیدوارم این سال جدید برای شما فرصت‌های جدیدی به همراه داشته باشد. همان‌طور که بهار، سرزندگی و نو شدن را به همراه می‌آورد، بیایید با انگیزه‌ای نو و انرژی مضاعف، به‌سوی موفقیت‌های بزرگ‌تر قدم برداریم.

EAT چیست؟

مفهوم E-A-T یکی از اصول کلیدی در ارزیابی کیفیت محتوا در الگوریتم‌های گوگل است. این سه اصل به گوگل کمک می‌کنند تا معتبرترین و بهترین نتایج را برای کاربران فراهم کند. این اصول عبارت‌اند از تخصص (Expertise)، اعتبار (Authority) و اعتماد (Trust).

تخصص (Expertise)

تخصص به معنای داشتن دانش و تجربه در یک حوزه‌ی خاص است. گوگل صفحات وب را که توسط متخصصان آن حوزه نوشته شده باشند، معتبرتر از صفحاتی می‌داند که توسط افرادی بدون تخصص مناسب تهیه شده‌اند. به‌عنوان‌مثال، یک وب‌سایت آموزشی در زمینه‌ی برنامه‌نویسی که مقالات و مطالب خود را توسط توسعه‌دهندگان نرم‌افزار حرفه‌ای منتشر می‌کند، از نظر گوگل ارزش بیشتری نسبت به وب‌سایتی دارد که همان مطالب را توسط یک نویسنده‌ی بدون تجربه در این زمینه می‌نویسد.

اعتبار (Authority)

اعتبار به این معنی است که دیگران چقدر یک سایت یا برند را به‌عنوان یک مرجع معتبر در نظر می‌گیرند. این امر معمولاً از طریق لینک‌دهی از سایت‌های معتبر، ذکر برند در مقالات تخصصی، و حضور در بحث‌های صنعت مرتبط قابل‌ارزیابی است. به‌عنوان‌مثال، وب‌سایتی که در زمینه‌ی هوش مصنوعی فعالیت می‌کند و مقالات آن توسط دیگر منابع معتبر مانند آکادمی‌ها یا نشریات علمی ارجاع داده می‌شود، به‌طور طبیعی از نظر گوگل اعتبار بیشتری دارد.

اعتماد (Trust)

اعتماد، به سطح اطمینانی اشاره دارد که کاربران به یک سایت دارند. گوگل به سایت‌هایی که اطلاعات دقیقی ارائه می‌دهند و از شفافیت بالایی برخوردارند، رتبه‌ی بالاتری می‌دهد. به‌طور مثال، در دنیای سایت‌های فروش آنلاین، یک فروشگاه که دارای سیاست‌های بازگشت کالا، توضیحات شفاف درباره‌ی محصولات و نظرات مشتریان است، بیشتر از فروشگاهی که اطلاعات تماس خود را پنهان کرده و روند خرید نامشخصی دارد، به چشم گوگل سایت قابل‌اعتمادی به حساب می‌آید.

تخصص یا Expertise چیست؟

همان‌طور که گفتیم، تخصص به معنای داشتن دانش عمیق و تجربه در یک حوزه‌ی خاص است. در دنیای سئو (SEO)، گوگل به محتوایی که توسط افراد با صلاحیت و تجربه‌ی واقعی در آن زمینه نوشته شده‌است، اهمیت بیشتری می‌دهد. اگر کاربری عبارتی مانند «چگونه می‌توانم نرم‌افزار خود را بهینه کنم؟» را جست‌وجو کند، گوگل به‌طور طبیعی اولویت را به مطالبی می‌دهد که توسط برنامه‌نویسان باتجربه یا متخصصان بهینه‌سازی موتور جست‌وجو نوشته شده باشد.

برای مثال، سایت‌هایی که مقالات خود را توسط مهندسان نرم‌افزار یا متخصصان باتجربه در بهینه‌سازی وب منتشر می‌کنند، از نظر گوگل بیشتر شایسته‌ی اعتماد هستند تا سایت‌هایی که حاوی مطالب مشابه بوده، ولی توسط نویسندگانی با دانش عمومی در این زمینه نوشته شده باشند. برای اینکه سایت شما نشان‌دهنده‌ی تخصص باشد، باید محتوای آن علاوه بر دقت، از نظر علمی و حرفه‌ای نیز معتبر باشد. این کار را می‌توان از روش‌های مختلفی انجام داد:

۱- محتوای اختصاصی و جامع: بدان معنا که به‌جای مطالب سطحی، نوشتن مقالات با جزئیات دقیق و تخصصی که برای کاربران حرفه‌ای ارزش داشته باشد. به‌طور مثال، اگر در زمینه تکنولوژی و برنامه‌نویسی مطلب می‌نویسید، باید کدهای پیچیده و تحلیل‌های عمیق‌تری ارائه دهید تا نشان دهید که موضوع را به‌طور کامل درک کرده‌اید.

۲- بیوگرافی نویسنده: به معنای ذکر رزومه و سوابق علمی و حرفه‌ای نویسنده است که به‌طور خاص در همان زمینه مرتبط با موضوع محتوا فعالیت کرده باشد. به‌عنوان‌مثال، اگر در حال نوشتن درباره‌ی مدیریت پروژه‌های پیچیده هستید، اشاره به تجربه‌ی مدیر پروژه‌های بین‌المللی می‌تواند اعتبار محتوای شما را بالا ببرد.

۳- ارجاع به منابع علمی و تخصصی: به معنای استفاده از مقالات و منابع قابل‌استناد است که در جامعه‌ی علمی یا صنعتی شناخته‌شده باشند. فرضاً اگر مقاله‌ای در زمینه‌ی شبکه‌های عصبی می‌نویسید، به مقالات معتبر از نشریات علمی یا کتاب‌های معتبر در این حوزه ارجاع دهید.

۴- به‌روزرسانی مرتب محتوای سایت: مطالبی که در سایت منتشر می‌شوند باید به‌طور مرتب با آخرین پیشرفت‌ها و تغییرات در آن زمینه به‌روزرسانی شوند. برای مثال، در دنیای برنامه‌نویسی، نسخه‌های جدید زبان‌های برنامه‌نویسی و فریم‌ورک‌ها باید در مقالات شما منعکس شود تا از اعتبار بالاتری برخوردار باشید.

اعتبار یا Authority چیست؟

اعتبار به معنای میزان شهرت، نفوذ و مرجعیت یک سایت یا فرد در حوزه‌ای خاص است. هر چقدر یک سایت یا فرد به‌عنوان یک منبع معتبر شناخته شود، گوگل نیز محتوای آن را دارای ارزش بالاتری می‌داند. درواقع، اعتبار یک سایت می‌تواند به‌طور مستقیم بر رتبه‌بندی آن در نتایج جست‌وجو تأثیر بگذارد.

برای مثال، در صنعت موبایل، برند «اپل» آن‌قدر اعتبار دارد که بسیاری از افراد وقتی به‌دنبال گوشی‌های هوشمند می‌روند، نام اپل را پیش از هر برند دیگری در نظر می‌گیرند. همین امر در دنیای وب نیز صادق است. به‌عنوان‌مثال، اگر سایت شما در زمینه‌ی توسعه‌ی وب یا طراحی سایت به‌قدری شناخته‌شده باشد که دیگران به‌طور مداوم به مقالات شما لینک دهند یا به شما استناد کنند، یعنی اعتبار (Authority) بالایی در آن حوزه دارید.

راهکارهای نشان دادن اعتبار کافی

برای اینکه گوگل و کاربران سایت شما را به‌عنوان یک منبع معتبر بشناسند، باید اقداماتی انجام دهید که این اعتبار را به‌وضوح نمایان کند. در اینجا برخی از روش‌ها آورده شده‌است:

۱- دریافت لینک‌های معتبر (Backlinks): یکی از راه‌های اصلی برای افزایش اعتبار سایت، دریافت لینک از منابع معتبر و شناخته‌شده است. به‌عنوان‌مثال، اگر سایت شما در زمینه‌ی امنیت سایبری فعالیت می‌کند و وب‌سایت‌های دانشگاهی یا نشریات معتبر در این حوزه به مقالات شما لینک دهند، اعتبار شما در نظر گوگل افزایش خواهد یافت.
۲- مشارکت در مباحث تخصصی و شبکه‌سازی آنلاین: مشارکت فعال در انجمن‌ها، وبینارها و رویدادهای آنلاین می‌تواند به شما کمک کند تا به‌عنوان یک مرجع شناخته‌شده در صنعت خود معرفی شوید. به‌عنوان‌مثال، اگر در حوزه‌ی هوش مصنوعی فعالیت می‌کنید، صحبت کردن در کنفرانس‌های مرتبط و انتشار مقالات در نشریات علمی معتبر می‌تواند اعتبار شما را در این زمینه افزایش دهد.
۳- ایجاد محتوای معتبر و اصیل: برای اینکه سایت شما به‌عنوان یک منبع معتبر شناخته شود، باید محتوای اصلی و تخصصی تولید کنید که دیگران را به خود جلب کند. این نوع محتوا معمولاً اطلاعات جدید، تحلیل‌های عمیق و جزئیات مفیدی را شامل می‌شود که به مشکلات واقعی کاربران پاسخ می‌دهد.
۴- سابقه و تاریخچه‌ی سایت: سایت‌هایی که مدت‌زمان طولانی‌تری به‌طور مداوم و با کیفیت بالا محتوا تولید کرده‌اند، به‌طور طبیعی اعتبار بیشتری خواهند داشت. برای مثال، اگر سایتی بیش از ده سال است که در زمینه‌ی مشاوره‌ی مالی فعالیت می‌کند و سابقه‌ای در انتشار مقالات تخصصی و مفید دارد، گوگل این سایت را به‌عنوان یک مرجع معتبر در نظر می‌گیرد.

اعتماد یا Trust چیست؟

اعتماد به معنای سطح اطمینانی است که کاربران و گوگل به یک سایت دارند. هر چقدر یک سایت قابل‌اعتمادتر باشد، کاربران با راحتی بیشتری از اطلاعات آن استفاده کرده و به آن استناد می‌کنند. اعتماد در بستر E-A-T نقش حیاتی دارد، زیرا نشان‌دهنده‌ی امنیت و صداقت سایت است. اگر کاربران نسبت به سایت شما اعتماد نداشته باشند، نه‌تنها تعاملات کمتری با آن خواهند داشت، بلکه گوگل نیز این سایت را در نتایج جست‌وجو به رتبه‌های پایین‌تر منتقل می‌کند.

برای مثال، فرض کنید دو فروشگاه آنلاین وجود دارد. فروشگاه اول دارای گواهی SSL، اطلاعات تماس واضح، نظرات مثبت از مشتریان و سیاست‌های شفاف بازگشت کالا است. فروشگاه دوم نه‌تنها اطلاعات تماس دقیقی ندارد، بلکه نظرات منفی زیادی از کاربران دارد و هنگام پرداخت، امنیت سایتی که پرداخت را انجام می‌دهید، نامشخص است. طبیعی است که کاربران بیشتر به فروشگاه اول اعتماد می‌کنند و گوگل نیز به‌خاطر امنیت و شفافیت بیشتر، آن را در نتایج جست‌وجو جایگاه بهتری می‌دهد.

اعتماد یکی از ارکان اصلی E-A-T است. سایت‌هایی که به‌طور مستمر اعتماد کاربران را جلب می‌کنند، معمولاً نرخ کلیک (CTR) بالاتری دارند، نرخ پرش (Bounce Rate) کمتری ثبت می‌کنند و در تعاملات کاربری موفق‌تر هستند. همه‌ی این‌ها به بهبود E-A-T سایت و موفقیت آن در سئو کمک می‌کنند.

راهکارهای نشان دادن اعتماد کافی

برای اینکه کاربران و گوگل به سایت شما اعتماد کنند، باید چندین اقدام اساسی انجام دهید:
۱- استفاده از گواهی SSL (Secure Sockets Layer): داشتن گواهی SSL که نشان‌دهنده‌ی امنیت سایت در حین انتقال اطلاعات است، یکی از مهم‌ترین فاکتورها در جلب اعتماد کاربران است. گوگل نیز سایت‌هایی که از این گواهی استفاده می‌کنند را به‌عنوان سایت‌های امن می‌شناسد و در رتبه‌بندی آن‌ها لحاظ می‌کند.

۲- شفافیت در اطلاعات تماس و سیاست‌ها: اگر سایت شما اطلاعات تماس مشخص و سیاست‌های واضحی مانند نحوه‌ی بازگشت کالا یا ضمانت‌ها دارد، کاربران احساس امنیت بیشتری خواهند کرد. به‌عنوان‌مثال، نمایش آدرس فیزیکی، شماره‌ی تماس معتبر و ایمیل‌های پاسخ‌گو باعث می‌شود که کاربران احساس کنند شما یک برند معتبر و قابل‌اعتماد هستید.
۳- نظرات و نقدهای مثبت: نظرات کاربران و نقدهایی که در سایت شما قرار می‌گیرد، می‌تواند تأثیر زیادی در جلب اعتماد دیگر کاربران داشته باشد. سایتی که نظرات کاربران واقعی و مثبت را به‌طور مستمر دریافت می‌کند، اعتبار بیشتری در نظر گوگل خواهد داشت.
۴- استانداردهای امنیتی بالا: استفاده از ابزارها و پلاگین‌های امنیتی برای محافظت از سایت و داده‌های کاربران از هک شدن یا سرقت اطلاعات، علاوه بر ایجاد اعتماد میان کاربران، برای گوگل نیز مهم است. این اقدامات باعث می‌شود تا سایت شما به‌عنوان یک سایت ایمن شناخته شود و رتبه بهتری کسب کند.
۵- سیاست حریم خصوصی و استفاده شفاف از داده‌ها: اطلاع‌رسانی دقیق و شفاف درخصوص نحوه‌ی جمع‌آوری و استفاده از اطلاعات کاربران و رعایت اصول حریم خصوصی، به‌ویژه در فروشگاه‌های آنلاین یا سایت‌هایی که اطلاعات حساس دارند، اعتماد بیشتری را جلب می‌کند. کاربران باید احساس کنند که اطلاعاتشان در امان است.

روش‌های سنجش E-A-T

برای ارزیابی دقیق سطح اعتماد (Trust)، اعتبار (Authority) و تخصص (Expertise)، ابزارهای متعددی وجود دارد که برخی از آن‌ها امتیازات عددی برای این معیارها ارائه می‌دهند و به کمک آن‌ها می‌توان کیفیت سایت و محتوا را ارزیابی کرد.

۱- Trust Flow در Majestic SEO: جریان اعتماد (Trust Flow)، یک معیار عددی است که میزان اعتماد سایت را در مقیاس ۰ تا ۱۰۰ نشان می‌دهد. هر چه این عدد بالاتر باشد، سایت به‌عنوان یک منبع معتبر و قابل‌اعتماد در نظر گرفته می‌شود. Trust Flow بالا معمولاً نشان‌دهنده‌ی این است که سایت از منابع معتبر و باکیفیت لینک دریافت کرده‌است.

برای مثال، اگر یک سایت آموزشی در زمینه‌ی یادگیری زبان انگلیسی لینک‌هایی از دانشگاه‌های معتبر یا مؤسسات آموزشی شناخته‌شده دریافت کند، Trust Flow آن بالاتر خواهد بود. این موضوع نشان می‌دهد که این سایت از منابع بااعتماد لینک دریافت کرده و به این ترتیب از نظر گوگل ارزش بیشتری دارد.

۲- Trust در LRT (LinkResearchTools): ابزار LinkResearchTools (LRT) نیز به‌طورخاص به ارزیابی میزان اعتماد لینک‌های ورودی به سایت می‌پردازد. این ابزار با بررسی کیفیت و اعتبار لینک‌ها، Trust Score را محاسبه می‌کند. به‌طورمعمول، Trust Score مناسب برای سایت‌های معتبر باید بین ۵ تا ۱۰ باشد. سایت‌هایی که از لینک‌های کم‌کیفیت، اسپم یا از منابع نامعتبر استفاده می‌کنند، به‌طورطبیعی امتیاز پایین‌تری خواهند داشت.

برای مثال، یک وب‌سایت خبری که لینک‌هایی از منابع خبری معتبر و شناخته‌شده مانند BBC یا Reuters دریافت کرده‌است، امتیاز Trust بالاتری خواهد داشت. این لینک‌ها نشان‌دهنده‌ی اعتبار بالای سایت و منابع معتبر آن است، که باعث افزایش اعتماد به سایت می‌شود.

۳-Domain Authority (DA) در Moz: اعتبار دامنه Domain Authority (DA)، یک معیار عددی است که بین ۰ تا ۱۰۰ نمره می‌دهد و هر چه این عدد بالاتر باشد، سایت از اعتبار بیشتری برخوردار است. به‌طورکلی، سایت‌هایی که نمره‌ی DA بالای ۴۰ دارند، از اعتبار خوبی در نظر گوگل و کاربران برخوردارند.

۴- Domain Rating (DR) در Ahrefs: رتبه‌بندی دامنه Domain Rating (DR) در Ahrefs مشابه DA است، با این تفاوت که برای محاسبه‌ی DR بیشتر بر کیفیت بک‌لینک‌ها (Backlinks) و لینک‌دهی‌های دریافت‌شده از سایت‌های معتبر و شناخته‌شده تمرکز دارد. هر چه کیفیت لینک‌های ورودی بهتر باشد، DR سایت بالاتر خواهد بود.

چک‌لیست ارزیابی و بهبود E-A-T سایت

در این بخش، به شما یک چک‌لیست جامع و کاربردی ارائه می‌دهیم که می‌توانید از آن برای ارزیابی و بهبود E-A-T سایت خود استفاده کنید. با پیاده‌سازی این مراحل، تأثیر مستقیم معیارهای تخصص (Expertise)، اعتبار (Authority) و اعتماد (Trust) را در رشد کسب‌وکار خود مشاهده خواهید کرد و می‌توانید جایگاه سایتتان را در نتایج جست‌وجو ارتقا دهید.

تخصص (Expertise)

برای ارزیابی تخصص سایت خود، باید به این موارد توجه کنید:

- آیا محتوای سایت شما توسط افراد متخصص در حوزه‌های مربوطه نوشته شده‌است؟

بررسی کنید که آیا نویسندگان شما دارای مدرک و تجربه‌ی کافی در زمینه‌ای که محتوا تولید می‌کنند، هستند؟

- آیا نویسندگان شما رزومه حرفه‌ای و سوابق مشخصی دارند که در سایت ذکر شده‌است؟

اگر نویسنده‌ی مقاله یا محتوای شما یک پزشک است، مقاله باید شامل جزئیات رزومه‌ی آن پزشک باشد تا اعتبار بیشتری پیدا کند.

- آیا اطلاعات ارائه‌شده در سایت شما دقیق، مستند و به‌روز است؟

از به‌روزرسانی منظم مطالب سایت و استفاده از منابع معتبر برای ارائه‌ی اطلاعات اطمینان حاصل کنید.

- آیا منابع معتبر و مستند را برای پشتیبانی از ادعاهای خود ذکر کرده‌اید؟

به‌عنوان‌مثال، اگر مقاله‌ای در مورد داروهای جدید نوشته‌اید، از مقالات علمی و تحقیقاتی معتبر برای پشتیبانی از مطالب خود استفاده کنید.

اعتبار (Authority)

برای سنجش اعتبار سایت، موارد زیر را بررسی کنید:

- آیا سایت شما از منابع معتبر لینک دریافت کرده یا می‌کند؟

بررسی کنید که آیا سایت شما لینک‌هایی از منابع معتبر مانند دانشگاه‌ها، مؤسسات تحقیقاتی یا رسانه‌های شناخته‌شده دریافت کرده‌است.

- آیا برند شما در رسانه‌ها یا سایت‌های معتبر به‌طور مکرر ذکر شده‌است؟

اگر برند شما در مقالات معتبر، رسانه‌های شناخته‌شده یا وب‌سایت‌های تخصصی ذکر شود، نشان‌دهنده‌ی اعتبار بالای آن است.

- آیا محتوای شما به‌عنوان مرجع توسط دیگران استناد می‌شود؟

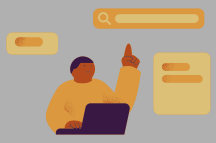
بررسی کنید که آیا وب‌سایت‌ها و منابع دیگر به مقالات و محتوای شما لینک می‌دهند یا از آن به‌عنوان منبع معتبر استفاده می‌کنند.

- آیا در شبکه‌های اجتماعی فعالیت مستمر و تعامل دارید؟
برند شما باید در شبکه‌های اجتماعی فعال باشد و با دنبال‌کنندگان خود تعامل داشته باشد تا اعتبار بیشتری پیدا کند.

اعتماد (Trust)

برای ارزیابی سطح اعتماد سایت، موارد زیر را بررسی کنید:
- آیا سایت شما گواهی SSL دارد؟
سایت‌هایی که دارای گواهی SSL هستند، از نظر گوگل امن‌تر و معتبرتر به نظر می‌آیند. این گواهی نشان‌دهنده‌ی امنیت داده‌ها در سایت شما است.
- آیا اطلاعات تماس و جزئیات شرکت به‌وضوح در سایت درج شده‌است؟
داشتن اطلاعات تماس واضح و شفاف، از جمله آدرس فیزیکی، شماره‌ی تلفن و ایمیل معتبر، اعتماد کاربران را جلب می‌کند.
- آیا سیاست‌های حفظ حریم خصوصی و شرایط استفاده شفاف و واضح هستند؟
سیاست‌های حریم خصوصی سایت باید به‌طورکامل و قابل‌فهم بیان شده باشند تا کاربران احساس کنند که اطلاعاتشان در امان است.
- آیا کاربران نظرات مثبتی درباره‌ی برند شما دارند؟
نظرات و بازخوردهای مثبت کاربران در سایت و شبکه‌های اجتماعی می‌تواند به نشان دادن سطح بالای اعتماد به برند شما کمک کند.
- آیا پرداخت‌های امن و روش‌های پشتیبانی قابل‌اعتماد ارائه می‌دهید؟
از ارائه‌ی سیستم‌های پرداخت امن و خدمات پشتیبانی باکیفیت مطمئن شوید تا کاربران بتوانند به راحتی و بدون نگرانی از سایت شما خرید کنند.

برای موفقیت در سئو و بهبود جایگاه سایت در نتایج جست‌وجو، رعایت معیارهای E-A-T «تخصص، اعتبار، اعتماد» بسیار اهمیت دارد. تخصص به این معناست که محتوای سایت باید توسط افراد باتجربه و دانش کافی در آن حوزه نوشته شود و از منابع معتبر پشتیبانی کند. اعتبار به دریافت لینک‌های معتبر از منابع شناخته‌شده و استناد به محتوا در سایت‌های دیگر مربوط می‌شود که نشان‌دهنده‌ی قدرت و مرجعیت سایت است. اعتماد به سایت نیز با ارائه‌ی اطلاعات شفاف مانند گواهی SSL، جزئیات تماس و سیاست‌های حفظ حریم خصوصی ایجاد می‌شود. این معیارها باعث جلب اعتماد کاربران، بهبود تجربه‌ی کاربری و ارتقای رتبه‌ی سایت در موتور جست‌وجو می‌شوند. همچنین، استفاده از ابزارهایی مثل Majestic و Ahrefs برای ارزیابی Trust Flow و Domain Rating می‌تواند به سنجش عملکرد و بهبود این معیارها کمک کند.



منابع

https://www.semrush.com/blog/eeat

https://searchengineland.com/entities-eat-authority-trust-385156

https://blog.hubspot.fr/marketing/eeat-google

با آغاز سال تحصیلی جدید، انجمن علمی مهندسی کامپیوتر برنامه‌های متنوعی را در راستای ارتقای فعالیت‌های علمی و دانشجویی در دستور کار خود قرار داده‌است. در این راستا، فرایند ثبت نام نودانشجویان نیم‌سال بهمن ۱۴۰۳ با تلاش و هماهنگی تیم آپلود مدارک به پایان رسید.

این تیم متشکل از دانشجویان متعهد و پرتلاشی بود که طی یک ماه متوالی، در شرایط سخت جوی و سرمای زمستانی، با دقت و نظم مثال‌زدنی وظایف خود را به انجام رساندند. باوجود بارش برف و کاهش دمای شدید، اعضای تیم بدون وقفه در محل ثبت نام حضور یافتند و مراحل بارگذاری مدارک و تأییدیه‌ی تحصیلی را انجام دادند.

اعضای تیم و مسئولیت‌های آنان:

۱- سورنا کریمی سلیمی «دبیر انجمن» – دانشجوی ترم ششم کارشناسی مهندسی کامپیوتر: نظارت بر کلیت پروژه و هماهنگی فرایندها

۲- مصطفی محسن‌خواه املشی «خزانه‌دار انجمن» – دانشجوی ترم چهارم کارشناسی مهندسی کامپیوتر: مسئول نوبت‌دهی و مسئول فنی تیم

۳- فرهاد فخری «مسئول مستندات انجمن» – دانشجوی ترم چهارم کارشناسی مهندسی کامپیوتر: هماهنگی‌های اداری فرایند

۴- رحیم عطار «عضو تیم اجرایی انجمن» – دانشجوی ترم دوم کارشناسی مهندسی کامپیوتر: انجام تأییدیه‌ی تحصیلی، مستقر در سیستم

۵- وفا رسولی املشی «عضو تیم اجرایی انجمن» – دانشجوی ترم دوم کارشناسی مهندسی کامپیوتر: انجام بارگذاری مدارک، مستقر در سیستم

۶- درسا حیدری «عضو تیم اجرایی انجمن» – دانشجوی ترم دوم کارشناسی مهندسی کامپیوتر: انجام بارگذاری مدارک، مستقر در سیستم

۷- فاطمه حسن‌زاده «عضو تیم اجرایی انجمن» – دانشجوی ترم دوم کارشناسی مهندسی کامپیوتر: انجام بارگذاری مدارک، مستقر در سیستم

۸- هانیه پورشیخ «عضو تیم اجرایی انجمن» – دانشجوی ترم چهارم کارشناسی مهندسی کامپیوتر: مسئول مالی فرایند و مستندسازی اطلاعات

این فرایند، که با استقبال نودانشجویان همراه بود، درنهایت با دقت و هماهنگی تیم اجرایی به سرانجام رسید. خوش‌بختانه، مسئولین دانشگاه نیز از کیفیت و سرعت انجام ثبت نام ابراز رضایت کردند و نقش ارزنده‌ی تیم آپلود مدارک را در تسهیل این فرایند مورد تقدیر قرار دادند.

گیلانو

SCC_LIAU scc.liau@gmail.com

گیلانو نشریه‌ای دانشجویی در زمینه‌ی علمی‌تخصصی با صاحب امتیازی انجمن علمی مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد لاهیجان است که با ترتیب انتشار ماهانه منتشر می‌گردد.

گیلانو از اردیبهشت ۱۴۰۰ شروع به فعالیت کرد و در آن به موضوعات مرتبط با تمام گرایش‌های مهندسی کامپیوتر نظیر هوش مصنوعی، رباتیک، نرم‌افزار، سخت‌افزار، شبکه و موضوعات بین‌رشته‌ای پرداخته می‌شود.

هیأت تحریریه‌ی گیلانو شامل دانشجویانی از رشته‌های مختلفی چون مهندسی کامپیوتر، مهندسی برق، مهندسی پزشکی، میکروبیولوژی، روان‌شناسی، پرستاری و... است.