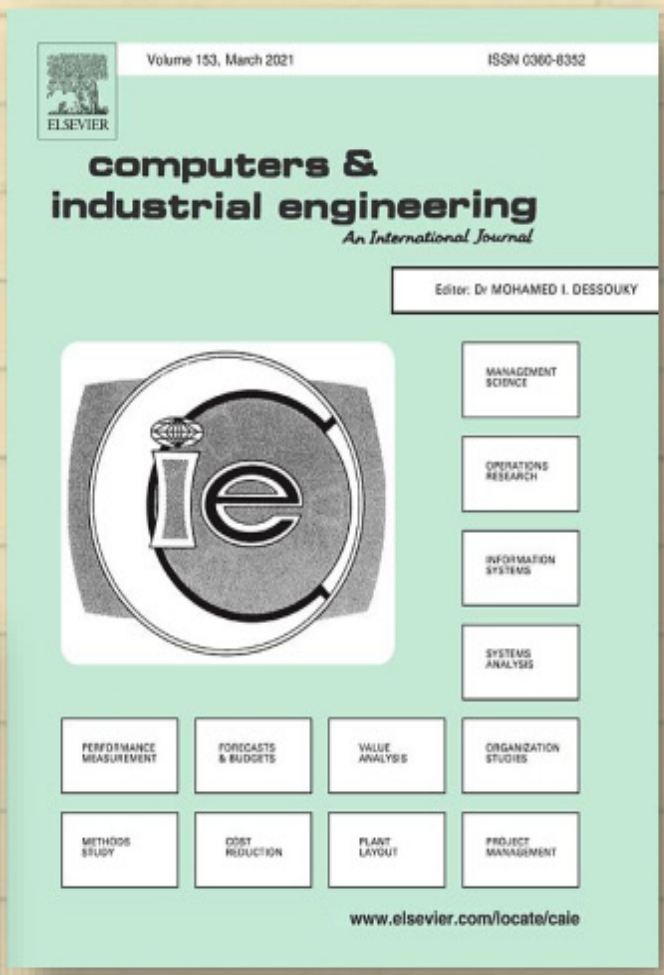
فصلنامه علمی – تخصصی کامپیوتر / آموزشکده فنی و حرفه‌ای دختران مراغه فاطمه الزهرا (س)
سال سوم / شماره هفتم / تابستان ۹۹

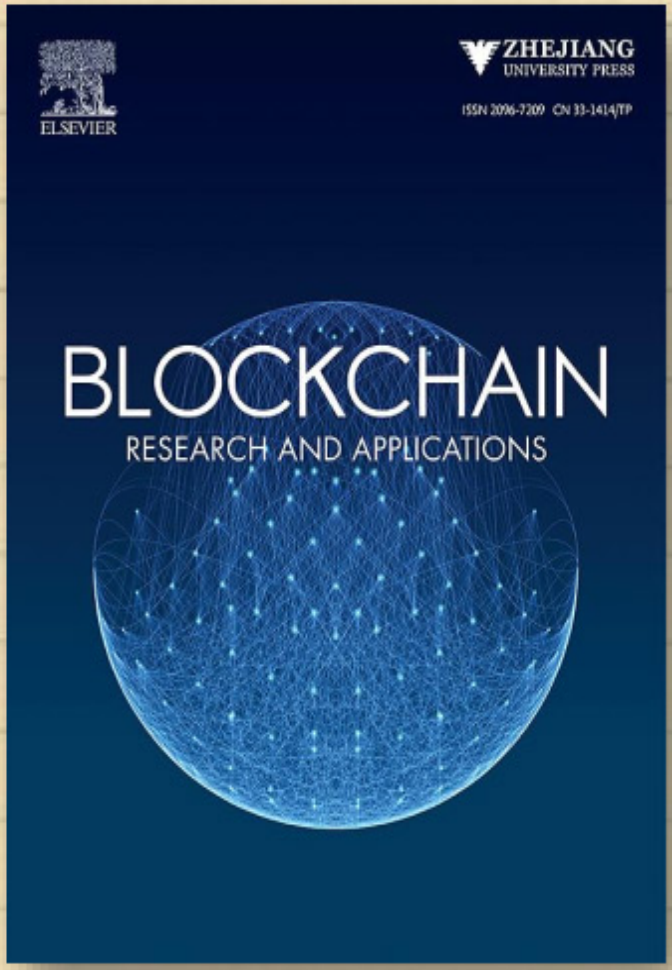
اعتبارسنجی

هوش تجاری

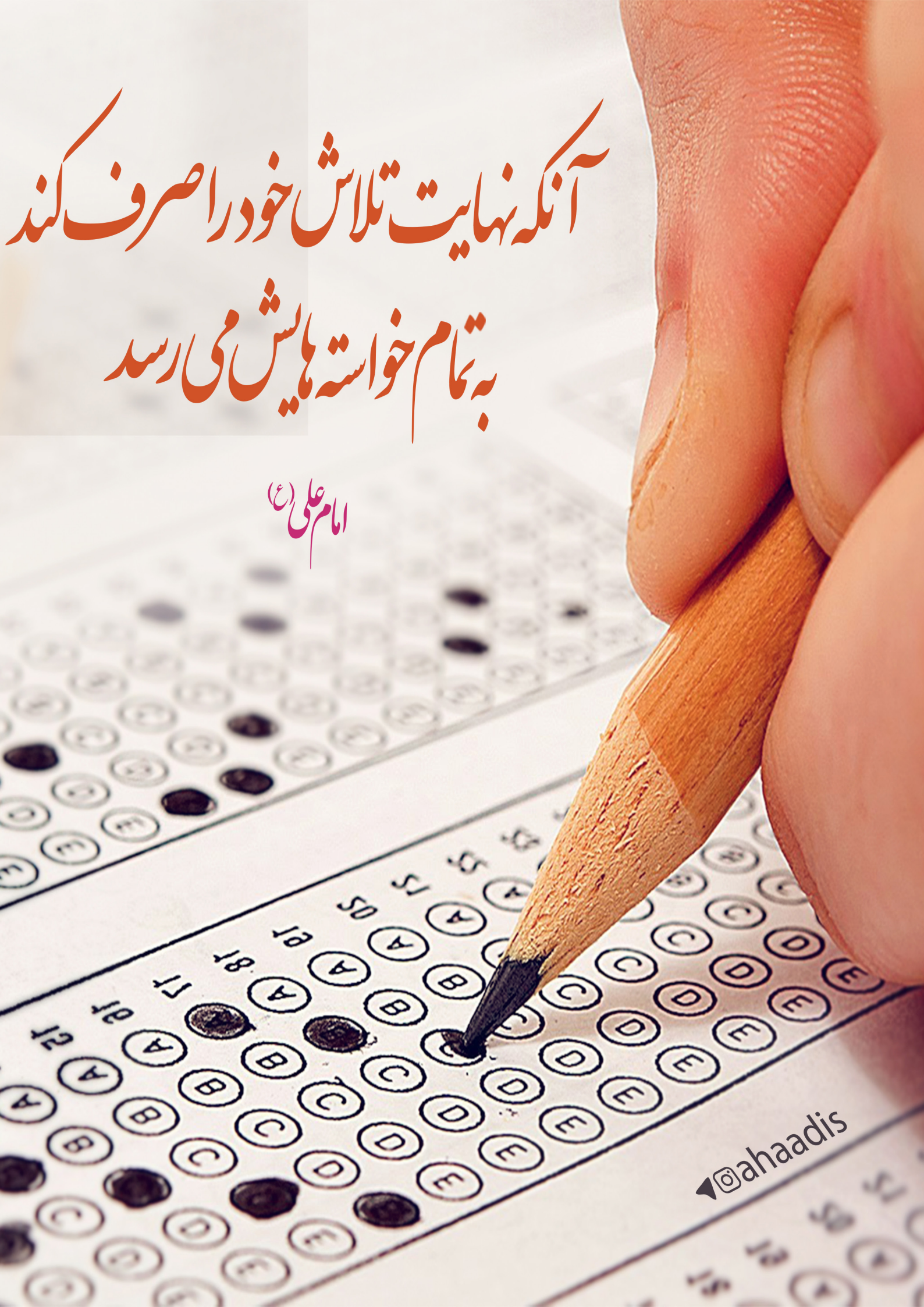
شبکه های نرم‌افزار محور



ژورنال مهندسی کامپیوتر و صنایع



ژورنال بلاک‌چین: تحقیقات و کاربردها


آنکه نهایت تلاش خود را صرف کند
به تمام خواسته هایش می رسد
امام علی(ع)
@ahaadis

بسم الله الرحمن الرحیم

مقام معظم رهبری(مدظله العالی)

این آموزشکده‌های فنی و حرفه‌ای باید توسعه یابند. کشور به موازات نیاز به علم، به پنجه‌های کارآمد هم نیاز دارد.

فهرست مطالب

صاحب امتیاز:
آموزشکده فاطمه الزهرا مراغه
مدیر مسئول:
الناز آشنا
سردبیر:
پریسا مردانی
همکاران تحریریه در این شماره:
مسعود صدقی‌وش / الناز آشنا /
نرگس فردوسی / ساحل نصر / پریسا رنجبر
فاطمه محمدی/ مریم زاهدی/
ویراستار:
ژیلا درخشان فرد
صفحه آرایی:
پریسا مردانی

ارتباط با ما:
پست الکترونیکی: Technoup.maragheh@gmail.com
آدرس: مراغه- شهرک ولیعصر-کوی دانشگاه- آموزشکده فنی و حرفه ای دختران فاطمه الزهرا(س) مراغه

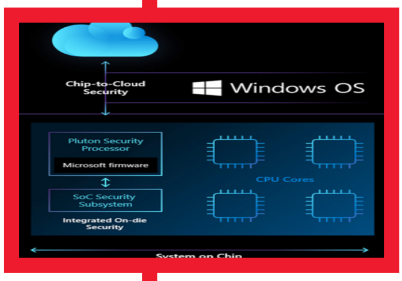
سخن سردبیر

با نام و یاد پروردگار متعال و با آرزوی سلامتی برای همه همراهان
مفهوم اعتبارسنجی از مفاهیم اصلی در حوزه امنیت در دنیای فناوری اطلاعات است. اعتبارسنجی بیان می‌کند که آیا داده‌های ما درست و معتبر هستند یا خیر. که برای این منظور یک سری قوانین مورد استفاده قرار می‌گیرند تا صحت و بامعنی بودن داده‌ها بررسی شوند. در این شماره از نشریه به مفهوم اعتبارسنجی به طور کامل پرداخته‌ایم.
هم‌چنین در این شماره مباحثی در زمینه‌های شبکه‌های نرم‌افزار محور و هوش تجاری مطرح شده‌است.
شما همراهان عزیز، می‌توانید از طریق آدرس ایمیل نشریه ما را از نظرات، پیشنهادات و انتقادات خود مطلع سازید.

سردبیر
پریسا مردانی

مایکروسافت از چیپ Pluton برای ارتقای امنیت سیستم های ویندوزی رونمایی کرد.

پریسا رنجبر- دانشجوی کارشناسی



مایکروسافت در همکاری با اینتل، AMD و کوالکام از چیپ امنیتی جدیدی به نام Pluton برای ارتقای امنیت کامپیوتری ویندوزی رونمایی کرد. Pluton نسخه تکامل یافته چیپ امنیتی TPM، بهتر، قوی تر و سریع تر از آن می باشد.

همچنین این چیپ جهت جلوگیری از سو استفاده هکرها و مسدود نفوذ آنان به سخت افزار کامپیوتر، از آسیب پذیری امنیتی پردازنده ها مثل Spectre و Meltdown طراحی شده است.

در پردازنده های آینده، Pluton جایگزین چیپ فعلی به نام Trusted Platform Module شده و به صورت یکپارچه به کار گرفته می شود. برای امنیت سیستم XBOX1 نیز از فناوری مشابه Pluton استفاده شده که هک آن را غیر ممکن کرده است.

مایکروسافت با همکاری اینتل، AMD و کوالکام جهت ساخت این چیپ امنیتی اقدام کرده و نیز از سازگاری این چیپ با لینوکس در آینده خبر داده است.

منبع: digiato.com

استفاده از هوش مصنوعی استارتاپ سوئیسی در نخستین پروژه پاکسازی زباله های فضایی

«آژانس فضایی اروپا» و استارتاپ سوئیسی(ClearSpace)، در حال توسعه فناوری جمع آوری زباله های فضایی به کمک سیستم هوش مصنوعی می باشند.

این فناوری با ۳۴۰۰۰ قطعه، قطر بیش از ۱۰ سانتی متر و سرعت ۱۰ برابر سرعت یک گلوله به دور زمین می چرخد. با افزایش زباله های فضایی احتمال برخورد با فضاپیماها افزایش می یابد که این عامل عواقب جبران ناپذیری خواهد داشت.

استارت این ماموریت در سال ۲۰۲۵ با نام ClearSpace-1 و مجهز به دوربین هوش مصنوعی جهت رصد زباله های فضایی خواهد بود. همچنین در این ماموریت آداپتور محموله موشک « وگا » به نام « وسپا » که در ارتفاع ۶۶۰ کیلومتری زمین در حال گردش است، جمع آوری خواهد شد. این محموله ۱۰۰ کیلوگرم وزن دارد

منبع: digito.com

https://digiato.com

برای دسترسی سریع و آسان به اخبار روز جهان در حوزه تکنولوژی و فناوری اطلاعات حتما به این سایت سر بزنید.

این سایت همچنین حاوی خبرهایی در مورد موبایل، خودرو، کسب و کار، علمی، استارتاپ و... می باشد.

https://darsman.com

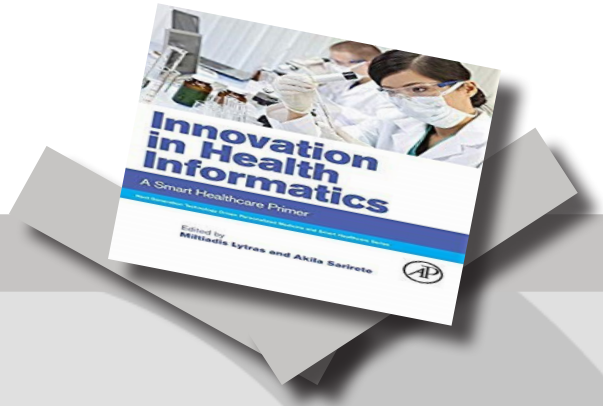
این سایت با هدف جمع‌آوری تمام دروس و همچنین برگزاری دوره‌های کاربردی برای ورود به بازار کار شکل گرفت.

دوره‌های آموزشی این سایت تنها مباحثی هستند که از طرف مایکروسافت ارائه می‌شوند. جهت‌گیری با این استانداردها باعث می‌شود که تمامی آموزش‌ها با نگرش مایکروسافت صورت گیرد و در نتیجه، دانشجوی دوره‌های درسمن میتواند برای دریافت گواهینامه‌های بین‌المللی مایکروسافت در زمینه‌های مختلف مانند MCSE، MCS و... آمادگی‌های لازم را کسب کند.

تولید کیت جدیدی که هر نوع عامل بیماری زا را در مدت کوتاهی تشخیص می دهد.

پزشکان باید قبل از درمان بیماران، با انجام آزمایش های مختلف نوع بیماری را تشخیص دهند.
در چند مدت اخیر، دانشمندان دانشگاه « کالیفرنیا، سان فرانسیسکو » یک آزمایش پزشکی واحدی را توسعه داده اند که قادر است هر نمونه را برای شناسایی DNA، پاتوژن های شناخته شده را مورد بررسی قرار دهد.
نتیجه این آزمایش در مدت زمان ۶ ساعت آماده می شود.
با توسعه این تست پزشکی از هزینه های زیاد و اتلاف وقت جلوگیری می شود و بیماران در مدت زمان و هزینه ای اندک نتیجه آزمایش خود را به دست می آورند.
با توسعه یک تست تشخیصی توسط پژوهشگران این تیم، می توان تمام DNA موجود در نمونه که شامل DNA انسان، ویروس، باکتری و قارچ با استفاده از رویکردی به نام « توالی نسل بعدی متاژنومیک » « MNGS » کار خود را شروع کرد.
سپس تمام DNA را توسط یک نرم افزار جستجو و دیتابیس و با تمام پاتوژن های شناخته شده مقایسه و تطبیق می دهد.
در انتها این پاتوژن که باعث بیماری است شناخته می شود.
در این آزمایش می توان توسط هر گونه مایع بدن بدون روش های خاص دیگر نوع بیماری را تشخیص داد.
برای شروع کار، محققان ۱۸۰ نمونه مایع از ۱۶۰ بیمار را تحلیل کردند. برای مثال بیماری ذات ریه را از طریق مایعات ریه می توان تشخیص داد.
علاوه بر این، این تست جدید توانست در زمینه شناسایی باکتری و قارچ به ترتیب به دقت ٪۷۵ و ٪۹۱ روش های سنتی دست پیدا کند. همچنین نوع عفونت ۱۲ بیماری که با استفاده از تست های عادی مشخص نشده بود، ۷ مورد آن را شناسایی کرده است.

منبع: digiato.com



Innovation In Health Informatics

کتاب Innovation in Health Informatics، اپلیکیشن‌ها و برنامه‌های کنونی و آینده را در حوزه تکنولوژی و سیستم پزشکی معرفی می‌کند. از جمله موضوعاتی که در این کتاب بررسی شده : داده‌های بزرگ، تحلیل داده‌های پزشکی، هوش مصنوعی، یادگیری ماشینی، تکنولوژی‌های واقعیت مجازی و واقعیت افزوده، سنسورها، اینترنت اشیا، نانو تکنولوژی ، بایو تکنولوژی و 5G است.

Codemurai

codemurai یک اپلیکیشن موبایلی است که جهت یاد گیری زبان های برنامه نویسی مختلف استفاده می شود. Codemuri توسط متخصصین طراحی وب ساخته شده است.
می توانید با استفاده از این اپلیکیشن کدنویسی در JavaScript، HTML، CSS، پایتون، TypeScript، Android، Node، MongoDB، ES6، Angular، SDK و ... را یاد بگیرید.

اعتبارسنجی
validation

مریم زاهدی - دانشجوی کارشناسی کامپیوتر
زیر نظر الناز آشنا

امروزه یکی از اساسی‌ترین اقدامات برای امنیت وب‌سایت‌ها، اپلیکیشن‌ها و جلوگیری از خرابکاری، «اعتبارسنجی یا Validation » است. یکی از بخش‌های مهم هر پروژهٔ نرم‌افزاری، اعتبارسنجی اطلاعات است. شما در تمامی فرم‌ها نیاز خواهید داشت که اطلاعات ورودی کاربر را بررسی کنید و از صحّت اطلاعات وارد شده اطمینان حاصل کنید. اعتبارسنجی درست اطلاعات وارد شده در فرم‌ها، بسیار مهم بوده و شما را از حملهٔ هکرها و اسپمرها در امان نگه می‌دارد. اعتبارسنجی از چند جنبه می‌تواند بررسی شود. از دیدگاه یک هکر و خرابکار و هر عامل نفوذی، بهتر است بدون مزاحمت در روند نفوذ به عمل خرابکارانه دست زده شود که در این صورت ایشان در مصرف زمان نیز برنده خواهد بود؛ چراکه در کمترین زمان می‌تواند بیشترین فرم ورودی را پر کند. درواقع هدف از اعتبارسنجی قرار دادن یک سری قوانین و شرایط برای به حداقل رساندن آسیب به داده‌های وب‌سایت‌ها، اطلاعات کاربران ذخیره شده در پایگاه داده‌های برنامه‌ها و اپلیکیشن‌ها و نیز جلوگیری از هر نوع خرابکاری توسط هکرها در فرم‌های اطلاعاتی است.

منظور از اعتبارسنجی چیست؟

منظور از اعتبارسنجی در فرم‌های وب، بررسی معتبر بودن اطلاعات با مقادیر مورد انتظار ماست که توسّط کاربر وارد شده است، یا به فرض عدم اجازهٔ ارسال فرم‌های خالی؛ به طور مثال هنگامی که کاربر بدون تکمیل فیلدهای مورد نیاز و ضروری، قصد ارسال فرم را دارد، پیام هشداری به او نشان داده شود، یا اگر در فیلدی ایمیل خود را وارد کرده و این ایمیل سهواً یا عمداً بدون علامت @ درج شده باشد، این موضوع قبل از ارسال فرم، به اطلاع او برسد. فرم طراحی شده باید توانایی این را داشته باشد، که تشخیص دهد:

آیا فیلدی خالی رها شده است یا نه؟

آیا فیلد با مقدار درستی پر شده است یا نه؟

آیا فیلدهای ضروری پر شده‌اند یا نه؟

و بسیاری مسائل دیگر.

انواع اعتبارسنجی

به صورت کلّی دو نوع اعتبارسنجی فرم وجود دارد:

اعتبارسنجی پس از تأیید: در این حالت هنگامی که کاربر تمامی اطلاعات مورد نیاز در فرم را پر می‌کند و دکمهٔ تأیید را می‌زند، اطلاعات به سمت سرور فرستاده شده و اعتبارسنجی می‌شوند و سپس نتیجهٔ اعتبارسنجی مجدداً به سمت کاربر فرستاده می‌شود. این نتیجه می‌تواند

تأیید تمامی اطلاعات باشـــد و یا خطایی به کاربر گزارش داده شود.

اعتبارسنجی آنلاین: در این حالت پیام‌های اعتبارســـنجی بلافاصله پس از تایپ کردن کاربر در کنار هر فیلد نمایش داده می‌شوند. در این روش بهترین حالت این است پیام‌ها درست کنار فیلد مورد نظر نمایش داده شود و کاربر را تشویق کند که اطّلاعات صحیح را همان لحظه وارد کند.

مدل‌های اعتبارسنجی

•اعتبارســـنجی اطلاعات یا Validating data: داده‌هایی را که در فرم نوشته می‌شوند، بررســـی می‌کند تا از درستی اطلاعات وارد شده مطمئن شود.

•اعتبارســـنجی فرم یا Form validation: به فرآیند بررســـی صحّـــت اطلاعات وارد شـــده توسّـــط کاربر در فرم گفته می‌شود. در ایـــن فرآیند اگر هنگام پر کردن فیلدهای فرم، خطایی صـــورت گیرد، به کاربر اطلاع داده می‌شـــود؛ برای مثال اگر فیلد ایمیل در فرم وجود داشـــته باشد، بررسی می‌شود که ورودی کاربر حتماً در فرمت ایمیل باشـــد، یا اینکه قبلاً بـــا آن ایمیل ثبت‌نامی صورت نگرفته باشد.

معیارهای اعتبارسنجی مناسب

در اعتبارسنجی فرم‌ها تا جایی که ممکن اســـت بایـــد از ایجاد ســـردرگمی کاربران اجتناب گـــردد. به طور کلّی برای داشـــتن اعتبارســـنجی مناسب در فرم‌ها، چهار معیار وجود دارد:

۱.زمان مناسب؛
۲.مکان مناسب؛
۳.رنگ مناسب؛
۴.زبان گویا.

حال در این قسمت هریک از این معیارها را با انواع فرم‌های ثبت‌نام بررسی می‌کنیم و به معایب و مزایای آن می‌پردازیم:

زمان مناسب

بهترین زمان بـــرای نمایش پیام موفقیت/خطا به کاربران، درســـت بعد از وارد کردن اطلاعات است. همان‌طور که قبلاً نیز به آن اشاره کردیم در اعتبارســـنجی آنلاین فرم، درســـت پس از پر کردن فیلدها به کاربران اطلاع داده می‌شـــود که اطلاعات وارد شده صحیح هســـتند یا دچار خطا شده‌اند؛ به عنوان مثال فرم زیر به زیر به خوبی این مفهوم را برایمان روشن می‌کند:

همانطور که در تصویر پیداست بلافاصله بعد از پر کردن فیلد در قالب اشتباه و یا خالی رها کردن آن، پیام خطای مربوطه نمایش داده می‌شود.

در روش اعتبارسنجی پس از ارسال، کاربر ابتدا تمامی فیلدها را پر می‌کند، پس از کلیک بر دکمهٔ ارســـال، صفحه دوباره لود می‌شود، سپس به کاربر اطلاع داده می‌شود که خطایی در ورود اطلاعات صورت گرفته است.

امّا در اعتبارســـنجی آنلاین، از اتلاف وقت کاربر جلوگیری می‌شود؛ هر چند این اتلاف وقت در حد ۳ دقیقه باشد، امّا در نتیجه تأثیر زیادی خواهد داشت.

مکان مناسب

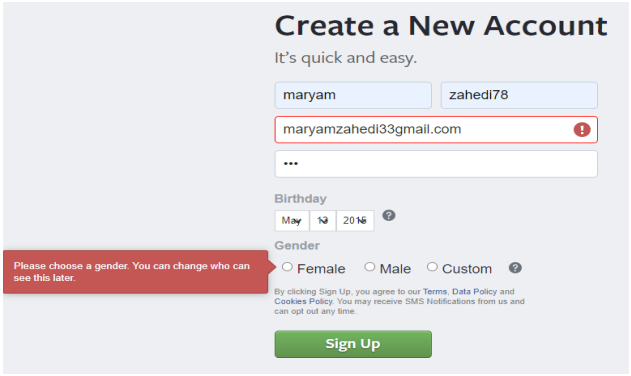
مکان نمایش پیام اعتبارســـنجی نیز به اندازهٔ زمان نمایش آن اهمیت دارد. اگر پیام خطا درســـت کنار فیلد موردنظر قرار نگیرد و در جایی دیگر مثل انتهای فرم قرارگیرد، توجّه کاربر را به همان ســـرعت به خود جلب نمی‌کند و ممکن است برای کاربر سردرگمی ایجاد شـــود و باعث شود کاربر بدون اتمام فرآیند ارسال اطلاعات، فرم را ترک کند.

همیشه بهترین جا برای قرار دادن پیام اعتبارسنجی، درست در کنار فیلدی است که کاربر قرار اســـت برای اصلاح آن کاری انجام دهد. اگر خطا در پر کردن فیلد باشد، بهتر اســـت درست کنار همان فیلد نمایش داده شود. اگر یک خطای کلی است (برای مثال خطا در ارســـال اطلاعات به سرور) و صفحه دوباره لود نشده اســـت، بهتر است در کنار دکمهٔ ارســـال قرار گیرد و اگر صفحه دوباره لود شده باشـــد، بهتر اســـت در بالای صفحه نمایش داده شود. این قضیه به نحوهٔ طرّاحی فرم‌هـــا در صفحات وب و اپلیکیشـــن‌ها برمی‌گردد که مهندس UI با کمک علم UX (تجربهٔ کاربری) بتواند مکان مناسب با ویژگی‌های بصری متناسب با هدف، طرّاحی را انجام دهد؛ به عنوان مثال به نمونه فرم زیر دقّت کنید:

همان‌طور که می‌بینید در فرم بالا، درست پس از هر فلید اشـــتباه خطای مربوط به آن نمایش داده می‌شود ولی یکی از اشکالات سایت، عدم توجه به فیلتر درست ایمیل می‌باشد که احتمالاً پس از زدن دکمهٔ ثبت خطای مربوط را نشـــان دهد که آن هم نمونه‌ای از اعتبارسنجی پس از ارسال می‌باشد. از اشکالات دیگر سایت امکان وارد کردن تاریخ به صورت دســـتی اســـت که باعث ایجاد خطا می‌شود.

به نظر می‌رســـد بهترین روش برای انتخاب تاریخ در فرم‌ها، استفاده از منوی کشویی است.

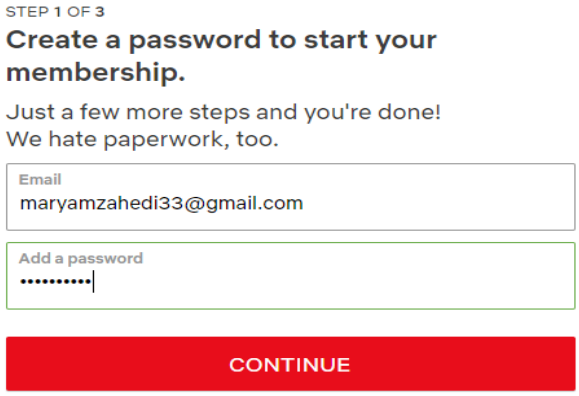
اگر طراحی فرم به شما اجازه نمی‌دهد فضای زیادی را به پیام‌های اعتبارســـنجی اختصاص دهید، نمونه فرم ثبت نام زیر را مشاهده کنید:



فرم بـــالا از Error provider برای نمایش پیام خطای خود اســـتفاده می‌کند. اگر نشانگر ماوس را بر روی علامـــت تعجب قرمز رنگ (علامت هشدار) موجود در تصویر قرار دهید، پیام خطای مربوط به آن نمایش داده می‌شود. در این مثال نیز اســـتفاده از رنگ‌های مناسب برای نمایش پیام‌ها کمک زیادی به کاربر می‌کند. پیام خطـــا با رنگ زمینه قرمز و فیلد مربوطه با قاب قرمز نمایش داده شـــده است. پیام‌های خطا نیز درست همان‌جایی نمایش داده شده‌اند که کاربر باید برای رفع خطا تغییری در اطلاعات بدهد.

رنگ مناسب

همانطور که در مثال‌های قبل دیده شـــد، به طور معمول برای نمایـــش خطا از رنگ قرمز، برای نمایش اطلاعات از رنگ آبی، برای نمایش هشـــدار از رنگ زرد و برای نمایش موفقیت از رنگ سبز استفاده می‌شود. دلیل استفاده از این رنگ‌ها این اســـت که رنگ‌هـــای قرمز و زرد، فشارخون را بالا می‌برند و توجّه کاربر را بیشتر جلب می‌کنند. به نمونه فرم زیر توجّه کنید:

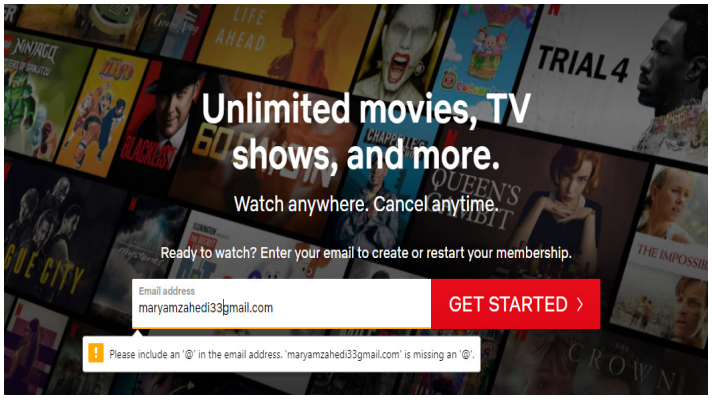


همان طور که در تصویر پیداست پس از درست وارد نمودن پسورد، کادر دور آن سبز رنگ می‌شود.

زبان گویا

یک پیام اعتبارسنجی باید به موارد زیر اشاره داشته باشد:

- چیزی که پیش آمده؛
- کاری که کاربر باید برای حل آن انجام دهد؛
- پرهیز از اصطلاحات و گویش‌های خاص در پیام‌های اعتبارسنجی؛
- قوانین اســـتفاده از زبان گویا در این پیام‌ها ساده است، امّا گاهی به راحتی فراموش می‌شـــود؛ برای مثال یک پیام خطای معمولی عبارت "ایمیل وارد شـــده صحیح نمی‌باشد!" است، بدون اینکه بیان کند چرا صحیح نیست. فرمت آن مشکل دارد؟ یا قبلاً توسط کسی استفاده شده است؟ این مسئله ممکن است کاربر را سردرگم کند.



در ســـایت فوق به خوبی این مســـئله قابل مشـــاهده است. پس از اشتباه وارد کردن فیلد ایمیل، پیام خطا نمایش داده می‌شود و به خوبی خطای مربوط را به کاربر اطلاع می‌دهد و همین امر باعث اجتناب از سردرگمی و اتلاف وقت کاربر می‌شود.

اعتبارسنجی در فریمورک‌های مختلف

در این مبحث به سه مورد از استفاده‌های اعتبارسنجی اشاره می‌شود و به صورت خلاصه‌وار در مورد کدهای هر یک توضیحاتی ارائه داده می‌شود:

۱.استفاده از اعتبارسنجی در وب (validation of form)؛
۲.استفاده از اعتبارسنجی در ویندوز؛
۳.استفاده از اعتبارسنجی در زبان‌های برنامه‌نویسی نظیر پایتون، c# و... .

اعتبارسنجی وب

اعتبارسنجی در وب می‌تواند به طور کلی در دو مرحله صورت گیرد: در سمت کاربر- که در گذشته تنها توسط کدهای java Script و یا با استفاده از یک Framework (مانند jQuery validation plugin) صورت می‌گرفت، امّا با معرفی HTML5 این رویکرد تغییر یافت- و همچنین در سمت سرور (با توجّه به تکنولوژی‌های مورد استفاده نظیر PHP, JSP, ASP .NET و...). ترکیبی از این روش‌ها نیز با استفاده از فناوری آژاکس (ajax) امکان‌پذیر است.

اعتبارسنجی سمت کاربر بهتر است یا سمت سرور؟

شاید در ذهن شما این سؤال باشد که کدام شیوهٔ اعتبارسنجی در وب بهتر است، اعتبارسنجی سمت کاربر و در مرورگر یا اعتبارسنجی سمت سرور؟ پاسخ این است که به جهت اطمینان‌بخشی، اعتبارسنجی سمت سرور مطمئن‌تر و بهتر است؛ چرا که اعتبارسنجی سمت کاربر متکی بر امکانات مرورگر است، به فرض اگر به هر دلیل جاوا اسکریپت پشتیبانی نشود یا غیر فعال باشد، این نوع اعتبارسنجی عمل نخواهد کرد، امّا اعتبارسنجی سمت سرور در هر شرایطی عمل می‌کند، مگر اینکه خودتان بخواهید آن را تغییر دهید. شاید با این تفسیر این سؤال به ذهن خطور کند که با این شرایط لزوم استفاده از اعتبارسنجی با جاوا اسکریپت چیست؟ اگرچه پیش از این گفتیم که ممکن است تمام مرورگرها از جاوا اسکریپت پشتیبانی نکنند (مثلاً جاوا اسکریپت توسّط کاربر غیرفعال شده باشد یا به فرض در مورد ارسال هرزنامه توسط ربات‌های خزنده و...) امّا در اکثر موارد این‌طور نیست، لذا برای افزایش قابلیت‌های تعاملی برنامهٔ خود و راهنمایی کاربران در هنگام پر کردن فرم‌های وب، همچنان می‌توان علاوه بر اعتبارسنجی سمت سرور، از جاوا اسکریپت نیز در کنار آن استفاده کرد، نتیجه اینکه هیچ‌گاه نباید تنها متّکی بر جاوا اسکریپت باشیم، بلکه در کنار برنامه‌نویسی امن در سمت سرور، می‌توانیم از امکانات جاوا اسکریپت نیز استفاده کنیم.

اعتبارسنجی فرم PHP

متغیر $_["PHP_SELF"]SERVER$ می‌تواند توسّط هکرها مورد استفاده قرار گیرد!
اگر PHP_SELF در صفحهٔ شما استفاده شود، هکر می‌تواند در نوار آدرس مرورگرش بعد از آدرس فایل یک اسلش (/) قرار دهد و سپس از دستورات XSS یا Scripting Cross Site برای تخریب سایت شما استفاده کند.
با استفاده از تابع() htmlspecialchars، می‌توان از طریق $_["SERVER["PHP_SELF با بیشتر انواع نفوذها مقابله نمود. کد فرم باید مانند نمونهٔ ذیل باشد:

```
<form method=”post”
action=”<?php echo
htmlspecialchars($_
SERVER[“PHP_SELF”]);?>”>
```

تابع() htmlspecialchars، کاراکترهای خاص را به HTML entity تبدیل می‌کند. حالا اگر هکر و خرابکار بخواهد از متغیر "PHP_SELF" سوءاستفاده کند، با نتیجهٔ زیر روبرو خواهد شد:

```
<form method="post"
action="test_form.php/&amp;quot;
&amp;gt;&amp;lt;script&amp;gt;alert('hacked'
)&amp;lt;/script&amp;gt;">
```

تلاش هکرها بی‌فایده است و هیچ آسیبی به سایت شما وارد نخواهد شد!
می‌توان دو ترفند دیگر نیز انجام داد:
۱.با استفاده از تابع trim() کاراکترهای غیرضروری (مثل: فاصله‌های اضافی، tab و خطوط خالی) را حذف کنیم.
۲.با استفاده از تابع() stripslashes، بک‌اسلش‌ها (\) را حذف کنیم.

اعتبارسنجی جاوا اسکریپت

این اعتبارسنجی کاملاً قابل سفارشی‌سازی است. اولین موردی که در کار با فرم‌های وب و بررسی اعتبار آنها به ذهن خطور می‌کند، اطمینان از خالی نبودن محتوای ارسالی است. بدین منظور ابتدا لازم است که یک تابع در جاوا اسکریپت داشته باشیم که در هنگام ارسال فرم، خالی نبودن مقادیر value فیلد را بررسی کند.

```
function validateForm(){

var field = document.
forms["form1"]["name1"].
value;

if (field == null || field == ""){

alert("فیلد نام نباید خالی باشد");
return false;

}}
```

در این تابع مقادیر فیلد فرضی name1 را از فرمی با نام form1 دریافت می‌کند. با یک دستور شرطی if بررسی می‌کند که فیلد name خالی نباشد. اگر فیلد خالی باشد، پس نتیجهٔ بررسی true می‌باشد و با یک دستور alert پیام موردنظر به کاربر نشان داده می‌شود.
یکی دیگر از موارد پرکاربرد اعتبارسنجی فرم‌ها مربوط به ایمیل است. کد زیر یک تابع است که در صورت اشتباه وارد کردن ایمیل به کاربر یک پیام هشدار می‌دهد.

```
function
emailValidate(formid,email) {

   var reg =
/^([A-Za-z0-9_\-\.])+\@
([A-Za-z0-9_\-\.])+\.([A-Za-z]
{2,4})$/;

   var address = document.
forms[formid].elements[email].
value;

   if(reg.test(address) == false) {
```

```
alert('آدرس ایمیل وارد شده نامعتبر است');
    return false;

{{
```

این تابع مبتنی بر دو عنصر کلیدی است:

۱-استفاده از عبارات باقاعده (Regular Expressions): با استفاده از عبارت باقاعده، الگوی موردنظرمان را تعریف می‌کنیم. در اینجا الگویی از ایمیل در حالت معمول تعریف شده است.

۲-متد Test: با استفاده از این متد بررسی می‌کنیم که آیا مقادیر فیلد ایمیل ما با الگوی موردنظر تطابق دارد؟ در صورتی که پاسخ منفی باشد، مقدار false برگردانده می‌شود، در نتیجه قسمت داخلی دستور شرطی if اجرا شده و پیغام هشدار نشان داده می‌شود.

اعتبارسنجی در HTML

ساده‌ترین روش برای اعتبارسنجی فرمها در html، استفاده از خاصیت type است.

مثلاً تصور کنیم ما یک فیلد متنی داریم که نیاز هست حتماً پر شود. برای اعمال چنین حالتی به سادگی می‌توان از خاصیت required استفاده کرد. با استفاده از این قابلیت مروگر، در صورتی که کاربر ورودی را پر نکند، به وی هشدار خواهد داد.

```
<input  type="text" required>
```

در صورتی که نوع ورودی number باشد، تنها اجازهٔ ورود اعداد را به کاربر می‌دهد. مروگر در این حالت یا از دریافت و قبول کردن کاراکترهای دیگر خوددرای می‌کند و یا آن‌که یک پیغام مبنی بر وارد کردن درست داده‌ها را به کاربر نشان می‌دهد.

```
<input type="number"
pattern="[-+]?[0-9]">
```

Pattern برای مطمئن شدن از محدود کردن ورودی به اعداد، علاوه بر خاصیت Type استفاده می‌شود. به صورت پیش فرض ورودی number تنها به اعداد اجازهٔ نوشته شدن می‌دهد. اگر بخواهیم از اعداد اعشار استفاده کنیم، باید از خاصیت Step استفاده کنیم.

اعتبارسنجی ویندوز

فرم اعتبارسنجی یک فرایند فوق‌العاده است، وقتی که شما در حال اجرای فرایند اعتبارسنجی خود هستید، اطلاعات شما به بانک اطلاعاتی ارسال شده و در صورت تأیید، نتیجه را در صفحهٔ رسمی می‌بینید. امّا وقتی که یک برنامهٔ کاربردی تحت وب طراحی کرده باشید که توسّط تعداد زیادی از افراد قابل استفاده است، برای فرایند اعتبارسنجی استفاده از اعتبارسنجی ویندوز، خیلی مقدمتر و سودمندتر است.

اعتبارسنجی مبتنی بر ویندوز، اداره کردن Windows Server و دستگاه سرویس‌گیرنده است.

برنامهٔ کاربردی ASP.NET وابسته به Internet Information Server (IIS) است. تمام درخواست‌های کاربران وب مستقیماً به IIS می‌رود و و این یک فرایند اعتبارسنجی در مدل‌های اعتبارسنجی مبتنی بر ویندوز را فراهم می‌کند. این نوع اعتبارسنجی در محیط اینترنت برای هر کاربری که درخواست Log In شدن به هر شبکه‌ای را می‌دهد، بسیار کاربردی است.

مزایای اعتبارسنجی ویندوز

- اعتبارسنجی ویندوز متکی بر اجازهٔ کاربر به استفاده از حساب کاربری ویندوز است؛
- ایجاد اصولی برای یک مدل احراز هویت یکنواخت برای انواع پیچیده از برنامهٔ کاربردی است؛
- اجرا کردن اعتبارسنجی ویندوز برای توسعه دهندگان بسیار آسان است؛ برای مثال دوستان من در مقطع کاردانی یاد گرفتند که می‌توان با چند دستور ساده در زبان‌هایی مانند سی‌شارپ که برای تولید برنامه‌های تحت ویندوز مناسب است، اعتبارسنجی فرم‌هایشان را انجام دهند.

معایب اعتبارسنجی ویندوز

- تنها با Platform مایکروسافت قابل اجرا است؛
- Platform بدون کنترل سفارشی یک فرآیند اعتبارسنجی را ایجاد می‌کند.

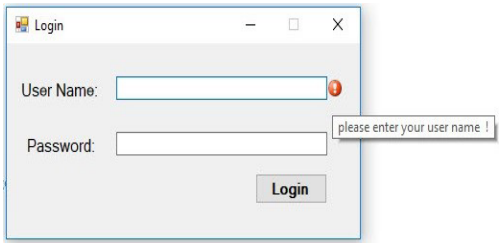
اعتبارسنجی با استفاده از زبان‌های برنامه‌نویسی

دربارهٔ اعتبارسنجی و یا Validation باید بیشتر در زبان‌های تحت وب مانند ASP.NET شنیده باشید و یا در وب‌سایت-هایی با آنها مواجه شده باشید. ما باید به عنوان یک برنامه‌نویس برای هرچه بهتر و کاربرپسند شدن پروژهٔ خود از اعتبارسنجی مطالب استفاده کنیم. در زبان تحت ویندوز Validation را با نام Error Provider شناسایی می‌کنند.

در زیر ما با استفاده از زبان برنامه‌نویسی c# قطعه کد مربوط به اعتبارسنجی را بررسی می‌کنیم.

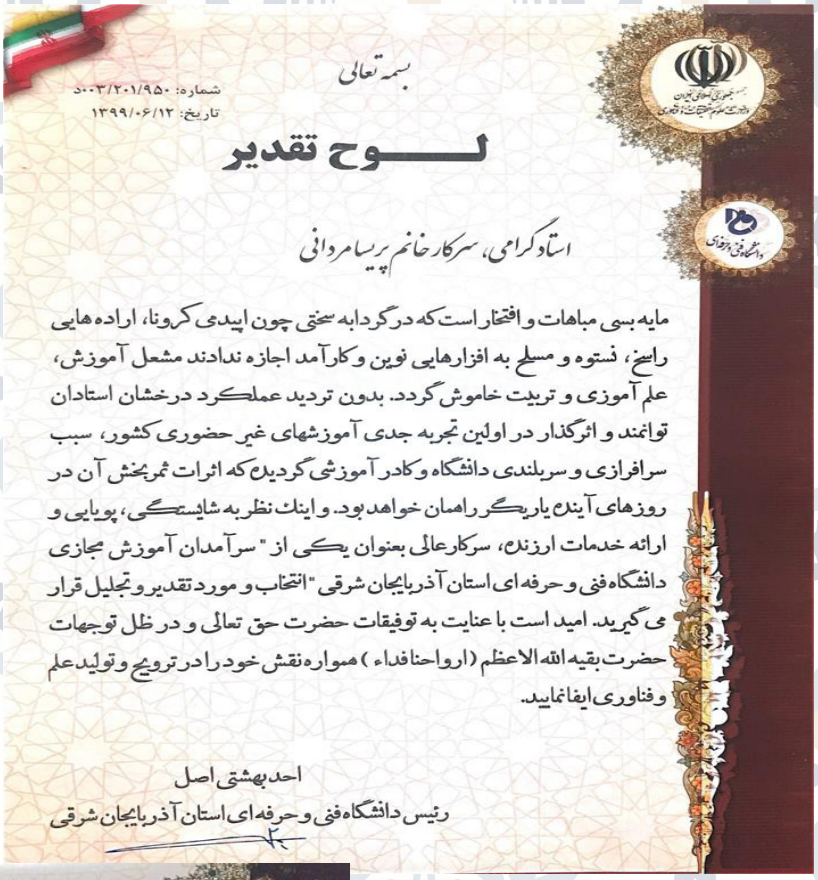
```
if (string.
IsNullOrEmpty(txtUsername.
Text))

        {

            e.Cancel =
true;

            txtUsername.Focus();

          errorProvider.
SetError(txtUsername, "please
enter your user name  !");

        }
```

در این قطعه کد ما مقدار خالی بود. textbox را با استفاده از Error Provider بررسی می‌کنیم. نتیجهٔ نهایی به صورت زیر خواهد بود.



منابع:
https://www.webhouse.ir
https://clicksite.org
https://barnamenevisan.org

انتخاب خانم مهندس مردانی و آقای مهندس ساکت به عنوان سرآمدان آموزش مجازی دانشگاه فنی‌وحرفه‌ای استان آذربایجان‌شرقی



بسمه تعالی

شماره: ۵۰۰۳/۲۰۱/۹۵۰
تاریخ: ۱۳۹۹/۰۶/۱۲

لـــــوح تقدیر

استاد گرامی، سرکار خانم پریسا مردانی

مایه بسی مباهات و افتخار است که در گردابه سختی چون اپیدمی کرونا، اراده هایی راسخ، نستوه و مسلح به افزارهایی نوین و کارآمد اجازه ندادند مشعل آموزش، علم آموزی و تربیت خاموش گردد. بدون تردید عملکرد درخشان استادان توانمند و اثرگذار در اولین تجربه جدی آموزشهای غیر حضوری کشور، سبب سرافرازی و سربلندی دانشگاه و کادر آموزشی گردید که اثرات ثمربخش آن در روزهای آینده یاریگر راهمان خواهد بود. و اینک نظر به شایستگی، پویایی و ارائه خدمات ارزنده، سرکار عالی بعنوان یکی از " سرآمدان آموزش مجازی دانشگاه فنی و حرفه ای استان آذربایجان شرقی " انتخاب و مورد تقدیر و تجلیل قرار می گیرید. امید است با عنایت به توفیقات حضرت حق تعالی و در ظل توجهات حضرت بقیه الله الاعظم (ارواحنافداء) همواره نقش خود را در ترویج و تولید علم و فناوری ایفا نمایید.

احد بهشتی اصل
رئیس دانشگاه فنی و حرفه ای استان آذربایجان شرقی

بسمه تعالی

شماره: ۵۰۰۳/۲۰۱/۹۵۰
تاریخ: ۱۳۹۹/۰۶/۱۲

لـــــوح تقدیر

استاد گرامی، جناب آقای توحید ساکت

مایه بسی مباهات و افتخار است که در گردابه سختی چون اپیدمی کرونا، اراده هایی راسخ، نستوه و مسلح به افزارهایی نوین و کارآمد اجازه ندادند مشعل آموزش، علم آموزی و تربیت خاموش گردد. بدون تردید عملکرد درخشان استادان توانمند و اثرگذار در اولین تجربه جدی آموزشهای غیر حضوری کشور، سبب سرافرازی و سربلندی دانشگاه و کادر آموزشی گردید که اثرات ثمربخش آن در روزهای آینده یاریگر راهمان خواهد بود. و اینک نظر به شایستگی، پویایی و ارائه خدمات ارزنده، جنابعالی بعنوان یکی از " سرآمدان آموزش مجازی دانشگاه فنی و حرفه ای استان آذربایجان شرقی " انتخاب و مورد تقدیر و تجلیل قرار می گیرید. امید است با عنایت به توفیقات حضرت حق تعالی و در ظل توجهات حضرت بقیه الله الاعظم (ارواحنافداء) همواره نقش خود را در ترویج و تولید علم و فناوری ایفا نمایید.

احد بهشتی اصل
رئیس دانشگاه فنی و حرفه ای استان آذربایجان شرقی

شبیه سازی حمله dos در شبکه های نرم افزار محور

نرگس فردوسی - دانشجوی کارشناسی کامپیوتر
زیر نظر مسعود صدقی‌وش

مقدمه

امروزه با پیشرفت سریع در زمینه فناوری اطلاعات، اخیرا معماری های شبکه‌ای کار آمدی در حال رشد می‌باشد، شبکه های نرم افزار محور SDN یک الگوی جدید از این معماری شبکه می‌باشد که این حوزه را دگرگون ساخته است. با توجه به ظهور شبکه‌های نرم‌افزار محور و با توجه به گسترش آن در دنیای امروزی همچنین به دلیل پرهزینه بودن و پیچیدگی بالای منابع در شبکه‌های سنتی، شبکه‌های نرم‌افزارمحور جایگزین سریعی برای شبکه‌های سنتی به شمار می‌روند. شبکه نرم‌افزار محور به مدیریت‌های متوسط و بزرگ به صورت مرکزی و بر اساس نرم‌افزار گفته می‌شود دقیقا درجایی که یک کنترلر متمرکز و منطقی تصمیمات را به سوئیچ ها ارسال می‌کند، شبکه نرم‌افزارمحور کنترل و سطوح داده را از یکدیگر تفکیک می‌کند. این تفکیک یک دید وسیع از شبکه را برای کنترلر فراهم می‌کند و آن را قادر می سازد تا تصمیماتی آگاهانه و بهتر در شبکه بگیرد. علاوه بر این، سوئیچ ها را می‌توان سبک‌تر و ارزان‌تر ساخت زیرا آنها دیگر نیاز به هوش محاسباتی برای انجام و پردازش کنترل سطوح نخواهند داشت.

حمله محروم سازی سرویس یک روش برای مسدود کردن خدمات به کاربرانی است که از قبل درنظرگرفته شده اند می‌باشد. شدت این حملات باتوجه به میزان ضرر و مدت زمان حمله متفاوت است حملات محروم سازی سرویس را می‌توان به حملات محروم سازی سرویس توزیع شده تعمیم داد که در مقیاس بزرگ بسیارمخرب می‌باشد.

تعریفی از حمله DOS و اهداف ان

اگر مهاجم برای حمله از یک میزبان استفاده کند به این نوع حمله DOS می‌گوئیم. در واقع هرحمله ای علیه دسترس پذیری به عنوان حمله منع سرویس درنظرگرفته می‌شود ازسوی دیگر اگرمهاجم از سیستم های زیادی به طور همزمان برای راه اندازی حملات علیه یک میزبان راه دور استفاده کند به عنوان حمله DDOS یاحملات توزیع شده تلقی می‌گردد. در روش DDOS تمام کامپیوترها همزمان با هم عمل می‌کنند به طوری که ممکن است در برخی موارد خسارات جبران ناپذیری به بار اورند. اهداف حمله DOS معمولا سایت‌ها یا خدمات میزبانی وب سرور با ویژگی‌های مناسب مانند بانک‌ها ،کارت‌های اعتباری می‌باشد سرورهای ریشه را هدف قرارمی‌دهند. یکی از روشهای معمول حمله شامل اشباع ماشینهای هدف با درخواست های ارتباط خارجی است. به طوریکه نمی‌تواند به ترافیک قانونی پاسخ دهد یا پاسخ ها با سرعت کم داده شوند و یا در دسترس نباشند چنین حملاتی منجر به سربار زیاد سرور می‌شوند. حمله dos کامپیوتر هدف را وادار به ریست شدن یا مصرف منابع اش می‌کند،

بنابرایـــن نمی‌توانـــد به ســـرویس های موردنظرش ســـرویس بدهد و همچنین سیاست های مورد قبول فراهم کنندگان سرویس‌های اینترنتی را نقض می‌کنند.

چگونه می‌توان پهنای باند را هنگام حمله های dos کنترل کرد؟

در معماری شبکه های نرم افزارمحور یکی از نقـــاط ضعف امنیتـــی اصلی در ماهیت خود این معماری نهفته اســـت. ترکیب کنترل کننده متمرکز و جداسازی لایه کنترل از لایه داده، خود یک چالش امنیتی عمده به حســـاب می اید که باید برای آن راه حلی یافت شود. یک مهاجم با ارسال سیلی از بسته ها که برای ارسال انها نیاز به تصمیم گیری کنترل کننده باشد می‌تواند کنترل کننـــده را برای کاربران عادی از دسترس خارج کند. حمله انکار سرویس مشابهی می‌تواند درلایه داده با پرکردن جدول جریان ســـوئیچ که حجم حافظه محـــدودی دارد انجام پذیرد برای مثـــال وقتـــی حمله صـــورت می‌گرفت الگوریتم های قبلی اگرچه می‌توانســـتند به وسیله ی سیستم های تشخیص نفوذ مانند اسنورت و با تلفیق شبکه های نرم افزار محـــور با حمله مقابله کنند ولی در مقابل به شدت پهنای باند شبکه را پایین می آوردند. بنابراین کارایی شبکه را تحت تاثیر قـــرار می‌دادند بطوریکـــه کاربران شبکه نمی‌توانستند از پهنای باند شبکه استفاده بهینه کنند.بیشترین پژوهش در این زمینه ازسال ۲۰۱۱ به بعد با ایده و روش‌های متفاوتی انجام گرفته است که هر کدام راه حـــل متفاوتی را ارائه داده و نتایجی نیز به دست آورده اند.

پژوهشگر	سال انتشار	ایده پژوهش	نتیجه پژوهش
Jose et al	2011	استفاده مهاجمان از ترافیکهای بزرگ برای حمله	استفاده از سویچ های جریان باز برای کنترل ترافیک
Ferguson et al	2012	مفهوم سلسله مراتبی وایجاد راهکار با استفاده از سیاست های امنیتی	ایجاد یک treepolice بر اساس ارتباط مرتبه ای میان سیاست های مختلف
Jain et al	2013	مسیریابی وبررسی ترافیک درمرکز داده های گوگل b4	Open flow (جریان باز) برای مدیریت سویچ ها و بهینه ساختن کاربرد پهنای باند
Wang et al	2014	متغیر بارگیری ترافیک وچگونگی کاربرد ان در شبکه های باز	استفاده از روشهای دسته بندی یادگیری ماشین برای بررسی پیشبینی اضافه بار احتمالی استفاده از net fuse
Sun et al	2014	رفتارشبکه ها در مدیریت ترافیک	مدیریت ترافیک بر اساس اطلاعات مشترک از شبکه جریان باز و میزبان های نهایی
Choi et al	2014	مدیریت جریان وچالش های کنترل با فرض مرکزیت و مقیاس پذیری انها	پیشنهاد جعبه میانی برای گرفتن مقدار پردازش روند بازبینی از کنترل کننده
Rasley et al	2014	مدیریت ترافیک	Plank بسته نرم افزاری مدیریت ترافیک، برای بالا رفتن داده های ترافیک
Wang et al	2014	جلوگیری از حمله های سیل اساdos	ارایه روش of_guard [۸]
Benjamin et al	2015	جلوگیری از حمله های سیل اسا	ارایه روش Irma [۲]
Wan et al	2015	جلوگیری از حمله های dos	ارایه روش flooguard

چارچوب کلی روش پیشنهادی

در این پژوهش با اســتفاده از معماری شــبکه های پس از انتشار ســه لایه با ایجاد یک مدیر کلی فعالیت‌های شــبکه را توانستیم تحت تاثیر قرار دهیم در این طرح پیشنهادی به غیر از سه لایه مطرح شده در شــبکه های عصبی، یک بخش مدیریت که در واقع ماشین مجازی اصلی با چندین ماشــین مجازی فرعی اضافه گردیــد بخش مدیریت تمــام اطلاعاتی که دیگر بخش‌ها ردوبدل می‌کنند تحت نظــر دارد و به صورت پویــا تصمیمات مهم را اتخاذ می‌کند این ماشین مجازی مقادیر مشــخص از منابع دسترسی پیدا کند که برای انجام کار تشــخیص نفوذ انتخاب خواهند شــد و دیگر ماشین‌های مجازی به لایه ورودی، پنهان و خروجی اختصاص داده می‌شوند بنابراین مجموع این ماشــین‌های مجازی و لایه های یک شبکه عصبی هوشمند(ANN) و سیستم تشخیص نفوذ را تشخیص می دهند که مــی توانند در هنــگام حمله تصمیمات مهم را اتخاذ کند. درساختارشبکه عصبی هوشــمند پیشــنهادی، لایه‌ی ورودی مســئول جمع آوری داده ها از شــبکه شامل تمامی درخواست ها یا جریان داده ها برای شناسایی فعالیت مخرب می‌باشد.

لایه ی پنهــان، داده‌های خام گرفته شــده را به لایه ورودی انتقال می‌دهد و لایه خروجی نیز نتایج نهایی را بر اساس آن چه که از لایه پنهان دریافت می‌کند منتقل می نماید همچنیــن ارزش‌های وزن برای لایه مخفــی را بروز می‌دهد و آنها را به لایه پنهان می‌فرســتد تا رفتار کلی شبکه را بهبود ببخشد. همچنین در این طرح معماری ارتقائ قابلیت اطمینان که یکــی از چالش های مهم سیســتم تشــخیص نفوذ است در نظر گرفته شده اســت هنگامی که یک گره در سیستم تشــخیص نفوذ می‌پیوندد، یک نخ ایجاد می‌کند و به شبکه متصل می‌شود. سپس سرور نخ را جهت ذخیره سازی آدرس و شماره پورت مشتری به صف می‌برد.

وقتی که اولین اتصال برقرار می‌شــود، همه مشتریان اطلاعات استفاده از منابع را، به منظور انتخاب مناسب ترین گره‌ها برای ساخت سیســتم تشخیص نفوذ به طور دوره ای به مدیر می‌فرستند.

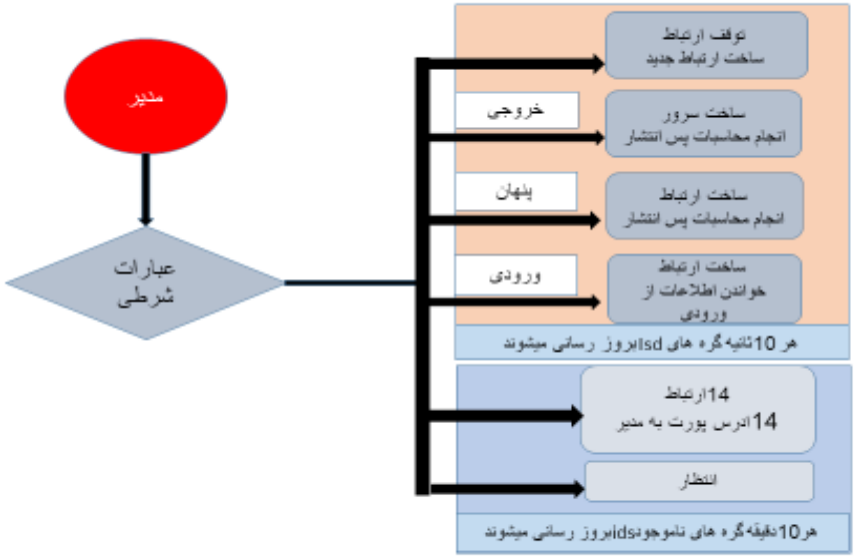
پس از ساخت سیستم تشخیص نفوذ تمام گره های سیســتم تشخیص نفوذ دیگــر، پیام را از مدیر دریافت می‌کنند و تابع مربوطه (ورودی - پنهان – خروجی یا انتظار) را بر اســاس زمان ورود، مدت زمان ماندن، مدت زمان غیر فعال بودن، مدت زمــان انتظار و زمــان خروج اجرا می‌کند.

علاوه بر این،گره های سیســتم های تشــخیص نفوذ هر۱۰ ثانیــه اطلاعات مدیریــت منابع مورد اســتفاده به مدیر جهت بروزرســانی ارسال خواهند کرد، و تمام گره های دیگر هر ۱۰ دقیقه این کار را انجام خواهند داد.

هنگامــی که برخــی از گــره ها در سیستم تشخیص نفوذ غیر قابل دسترس می‌شوند(مشغول یا خاموش شدن)، مدیر براساس این طراحی سیستم پیشنهادی در مدت ۱۰ ثانیه مطلع خواهند شد.

اگر گره نتواند به سیســتم تشــخیص نفــوذ برگردد مدیــر براســاس اخرین اطلاعات استفاده از منابع،گره های جدید را انتخاب می‌کند.

ســپس این پیام ها را بــرای متوقف کــردن اتصالات قدیمی جهت جلوگیری از حملات DOS ارسال می‌کند و خواهان ساختن موارد جدید می‌شود بنابراین کل



شکل (1)روند فرایندچندنخی

سیستم تشـــخیص نفوذ می‌تواند به کار ادامه دهد همچنیـــن هنگامی که برخی از گره های خارج از سیســـتم تشخیص نفوذ در دســـترس نباشند مدیر در طول ۱۰دقیقه از این تغییر مطلع خواهند شد.

بنابراین مدیر آنها را بـــه عنوان نامزد برای گره های سیســـتم تشخیص نفوذ انتخاب نمی‌کنـــد از انجایی که در روش پیشنهادی از الگوریتم شبکه های عصبی هوشـــمند استفاده شده اســـت و شبکه بـــا ایجاد ISD هـــای پویا قادر اســـت تا فعالیت‌های مخرب را شناســـایی کند لذا هنـــگام حمله در کمتریـــن زمان ممکن می‌تواند بـــه فعالیت‌های مخرب واکنش نشان دهد.

همچنین در این روش چون ارتباطات قطع شـــده به صـــورت دوره ای به مدیر گزارش می‌شود لذا نفوذکننده نمی‌تواند وارد شبکه شـــود و پهنای باند شبکه را تحت کنتـــرل خود قرار دهـــد با اعمال این روش توانســـتیم پهنای باند شبکه را در اختیار خود قرار دهیم و از دسترســـی حملات مصون داریم.

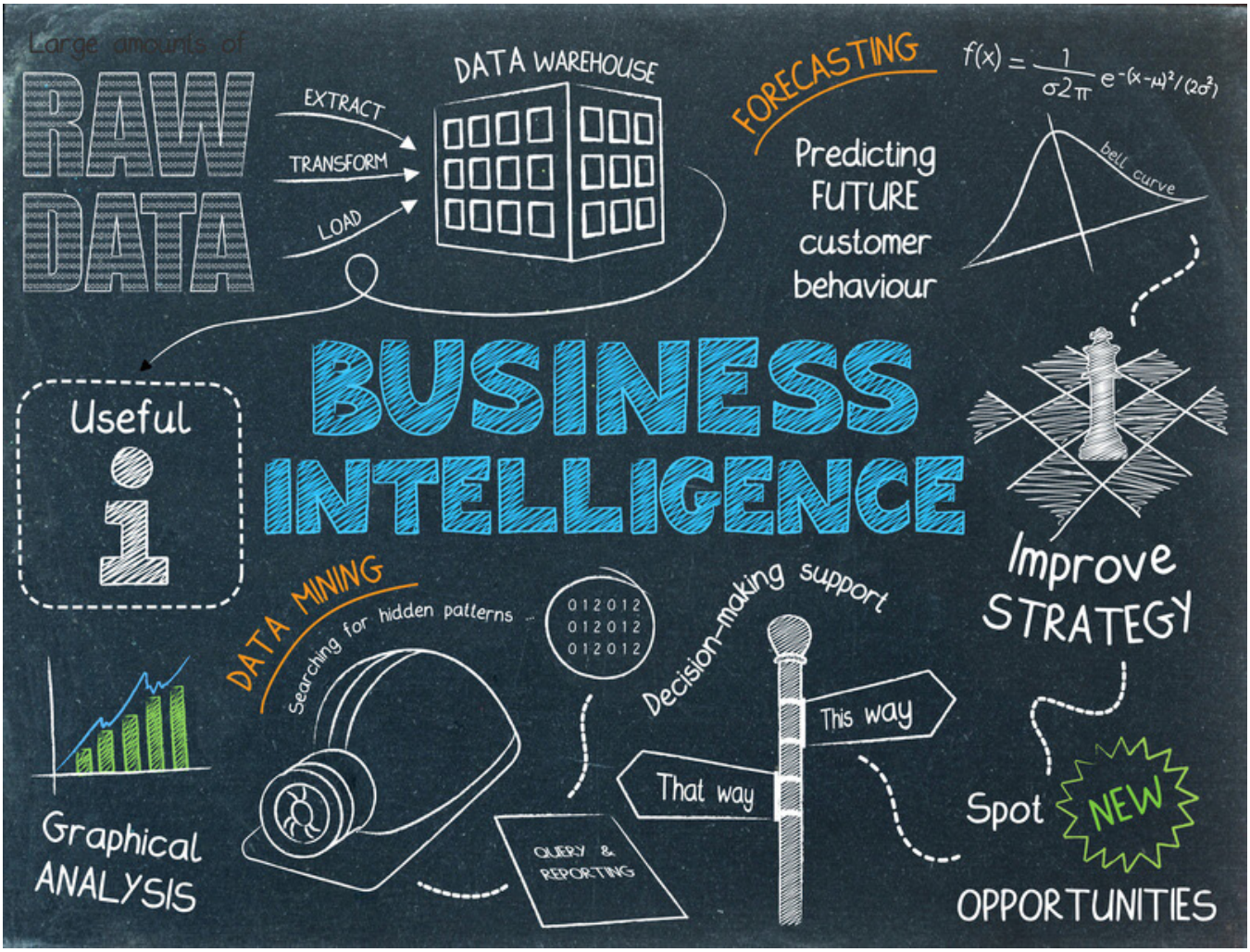
نتیجه‌گیری

شبکه های نرم افزار محور، نسل جدیدی از شبکه هاست که با استفاده از لایه های مجازی، ســـوییچ هـــای مجازی،کنترلر مرکزی،اســـتانداردهای ارتباطی و رابط های برنامه نویســـی کاربردی سطح بالا سعی می‌کنند برخی از کارهای کنترلی و مدیریتی ســـوییچ ها و روتر های شبکه را در لایه های بالاتر به صورت نرم افزاری انجام دهند. به زبانی دیگر شـــبکه های نرم افزار محور وابســـتگی به سخت افزار را کاهـــش داده و قابلیت‌های نرم افزاری و هوشمندی شـــبکه را افزایش می‌دهد. از این رو بررســـی راه هـــای جلوگیری از حمـــلات DOS دارای اهمیت فراوانی می‌باشد در این مدل پیشنهادی، همانطور که گفته شد در بخش مدیریت می‌توانیم کلیه فعالیت‌های هر ســـه لایه‌ی ورودی، پنهـــان و خروجی را تحت کنترل بگیرد. یکی از خصیصه های بخش مدیریت این اســـت که به صورت پویا، باتوجه به نوع حمله و منابع موجود می‌تواند سیســـتم تشخیص نفوذ مربوطه را بسازد. همچنین در صورتی کـــه یک گره نتوانـــد به کار خود ادامه دهد از آن مطلع خواهد شـــد و گره دیگری را برای سیســـتم تشخیص نفوذ انتخاب می‌کند. مدل پیشنهادی در زمان حمله می‌تواند عکس العمل خوبی را نشان داده و از پهنای باند و منابع شبکه محافظت کند.

منابع:

[1] Alsmadi, I.,& Xu, D.(2015). Security of Software Defined Networks: A Survey.Computers & Security, doi: 10.1016/j.cose.

[2] Wang,H., Xu, L.,& Gu, G.(2015).FloodGuard: A DoS Attack Prevention Extension in Software-Defined Network.IEEE Computer Society.



هوش تجاری چیست؟

ساحل نصر- دانشجوی کارشناسی کامپیوتر

هوش تجاری مفهوم بسیار وسیع و گسترده‌ایست بطوریکه امروزه اکثر مدیران سازمان‌ها برای گرفتن تصمیمات کاربردی برای بهبود شرایط موجود از آن استفاده می‌کنند. هوش تجاری با جمع‌آوری داده‌های خام و انجام تجزیه و تحلیل بر روی آنها برای اتخاذ تصمیمات نهایی به مدیران سازمان ها تحویل داده می‌شود.

هوش تجاری شامل فرایندها، ابزار و فناوری های مختلف می باشد که برای تبدیل داده خام به اطلاعات و اطلاعات به دانش مورد نیاز هستند، که با استفاده از همین دانش مدیران قادر به تصمیم گیری بهتر می شوند و در نتیجه عملکرد سازمان خود را بهبود می بخشند. مجموعهای از نظریات، روشها، فرایندها، معماریها و فناوریهایی است که برای تبدیل داده خام به اطلاعات مفید و معنادار استفاده می‌شود.

تصمیم‌گیری بر اساس هوش تجاری به سه بخش قابل تقسیم‌بندی است:

- جمع‌آوری داده و اطلاعات مورد نیاز
- تجزیه و تحلیل داده‌های جمع‌آوری شده و تصمیم‌گیری بر اساس آنها
- به کارگیری نتایج گرفته شده و نظارت بر آنها

معماری هوش تجاری چگونه است؟

هوش تجاری از نظر ساختار اجرا و معماری فرایند، دارای ۵ لایه اصلی است:

۱- منابع اطلاعاتی

در اولین مرحله برای پیاده‌سازی هوش تجاری در یک سازمان، داده‌های مهم را در قالب فرمت‌های به‌خصوص شناسایی و سازماندهی می‌کنیم، این داده‌ها می‌توانند از انواع منابع اطلاعاتی مانند دیتابیس‌ها و... تجمیع گردند.

۲- استخراج، تبدیل و بارگذاری

دراین مرحله، اطلاعات مناسب از منابعی که در مرحله‌ی قبل تشخیص داده شد استخراج شده، سپس به داده‌های قابل استفاده برای سیستم تبدیل می‌شود، در این مرحله داده‌های نامعتبر از مجموعه حذف خواهد شد و سپس در انبارهای داده گردآوری و بارگذاری می‌شوند.

۳- انبارهای داده

هدف از انجام این مرحله در حقیقت جمع‌آوری داده‌های مورد نیاز و ایجاد مجموعه‌ای یکپارچه از این اطلاعات می‌باشد، طراحی این مجموعه جز یکی از مهمترین مراحل فرایند پیاده‌سازی هوش تجاری است، انبار داده باید به‌گونه‌ای طراحی شود که انواع مختلف اطلاعات در آن قابل تجمیع باشند.

۴- مدلسازی داده‌ها

در این گام، حقایق مربوط به کسب‌وکار شامل فروش، پرداخت، زمان فروش، فروشنده و مشتری مشخص شده و در قالب گزارش‌هایی بررسی و روابط میان آنها مشخص می‌شود، پس از انجام این فرایند به مقادیر و اطلاعات محاسباتی دست می‌یابیم که می‌توان از آنها به عنوان شاخص‌های اندازه‌گیری اطلاعات استفاده کرد.

۵- ارائه‌ی اطلاعات

در آخرین لایه از فرایند هوش تجاری، اطلاعات به‌دست آمده را در قالب داشبوردهای مدیریتی و به شکل نمودارهای گرافیکی، گزارشات تصویری، متنی و... به کاربر نهایی (معمولا مدیران کسب‌وکار) نمایش داده می‌شود، این گزارش‌ها می‌توانند حاوی اطلاعاتی شامل نقاط ضعف و قوت سازمان، عوامل موفقیت یا شکست پروژه‌ها، تاثیر هزینه‌ها در فروش و... باشند که در نهایت می‌توانند استراتژیهای تجاری سازمان را دستخوش تغییر کنند.

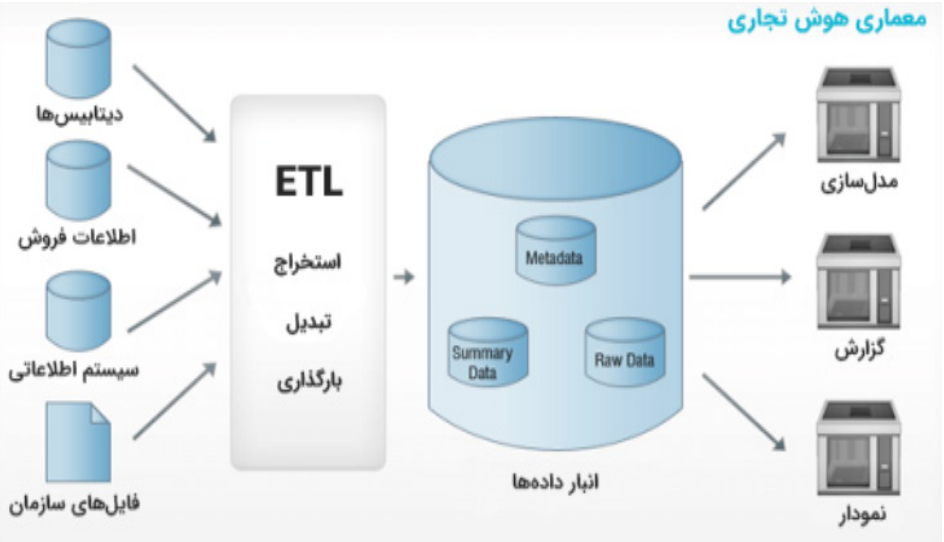
روشهای تحلیل داده بر اساس هوش تجاری

هوش تجاری شامل طیف گسترده ای از برنامه های تجزیه و تحلیل داده است .این ابزارها بر پایه تکنولوژی OLAP توسعه داده شده اند. در این فناوری می‌توان انواع داده ها را وارد سیستم کرد و مشخص کرد که داده ها بر چه اساسی طبقه بندی و چطور نمایش داده شوند.

برای مثال پس از وارد کردن اطلاعات یک فروشگاه زنجیره ای می شود مشخص کرد، داده ها بر اساس زمان، مکان، بیشترین میزان فروش، محصولات پرفروش، محصولات کم سود و .. طبقه بندی و آنالیز شوند.

بانک‌های اطلاعاتی به کار رفته در OLAP که Data warehouse یا انبار داده ها نامیده می شوند متشکل از مکعب های اطلاعاتی چند بعدی بوده که امکان آنالیز سریع اطلاعات پایگاه داده های مختلف را فراهم می‌آورند. بعنوان مثال یک پایگاه داده چند بعدی می تواند فروش کل سالیانه را با ماه فروش، تعداد مشتری و قیمت متقاطع سازد. حاصل این تقاطع این است که گزارشات بسیار متنوعی مثل مجموع فروش در ماه خاص یا بهترین قیمت و مشتری سال و ... از سیستم به راحتی قابل استخراج است.

معماری هوش تجاری



منابع

۱- رحمانی، زین العابدین و فخرآبادی، زهرا،۱۳۹۵نقش هوش تجاری (کسب و کار) بر رفتار شهروندی در سازمان ها،دومین کنفرانس ملی علوم مدیریت نوین و برنامه ریزی پایدار ایران،تهران

۲- کبیری دهکردی، مهناز و زمانی دهکردی، بهزاد و کیومرثی، فرشاد،۱۳۹۵مروری بر هوش تجاری در سازمانها،دومین همایش ملی علوم و فناوری های نوین ایران،تهران

این شماره:

محمد پورممی

فاطمه محمدی- دانشجوی کارشناسی کامپیوتر
مینا زاهدی- دانشجوی کارشناسی کامپیوتر

سلام و عرض ادب خدمت تمام خوانندگان عزیز فصلنامه تکنو اپ؛ امیدوارم در این حال و هوای کرونایی حال و احوالتان خوب باشد و زدن ماسک و رعایت پروتکل های بهداشتی را هم فراموش نکرده باشید!!!

با ورود دانشجویان دهه هشتادی به دانشگاه ها شاهد موفقیت ها و فعالیت های این نسل در زمینه های علمی و فرهنگی هستیم، سوژه ما برای مصاحبه این بار از بین همین دهه هشتادی هاست که قبل از ورود به هنرستان با اصول برنامه نویسی آشنا شده و درحال حاضر نیز مشغول آموزش دانسته های خود به افراد علاقه مند حوزه تکنولوژی و کامپیوتر میباشد،همراه ما باشید با آقای محمد پورممی

سلام اقای پورممی. از خودتان برایمان بگویید.

با سلام و عرض ادب خدمت شما و تمامی مخاطبین فصلنامه تکنو آپ، من محمد پورممی هستم دانشجوی ترم آخر مقطع کاردانی رشته نرم افزار دانشگاه فنی حرفه ای تبریز، متولد ۳ فروردین سال ۱۳۸۰ و اهل تبریزهستم.

بسیار بسیار علاقمند به تکنولوژی و یادگیری هرچیزی که مربوط به کامپیوتر و موبایل باشد مخصوصا برنامه نویسی ؛ شغل اصلیم هم برنامه نویسی وب و اندروید می‌باشد و تقریبا ۴ سال هست که در این زمینه به صورت حرفه ای فعالیت می‌کنم.

چه دلیل یا انگیزه ای باعث ورود شما به فنی و حرفه ای و بخصوص دنیای کامپیوتر شد؟

من علاقه ذاتی نسبت به خلق کردن دارم، حالا این خلق کردن می‌تواند توی شعر گفتن باشد یا نقاشی کشیدن یا هرچیز دیگری، وقتی هم برنامه نویسی می‌کنیم ، در واقع داریم یه سیستمی رو خلق می‌کنیم، من هم تقریبا یک سال قبل از انتخاب رشته با برنامه نویسی آشنا شدم و در نتیجه پیگیر شدن هنر برنامه نویسی، وارد رشته کامپیوتر شدم.

چه فعالیت ها و موفقیت هایی در این حوزه داشته‌اید؟

به غیر از فعالیت اصلی‌ام که برنامه نویسی وب و اندروید هست، بیش از یک سال است که یک صفحه اینستاگرام راه اندازی کردم و انجا سعی می‌کنم در حد توانم به بقیه دوستانی که دوست دارند وارد این حرفه بشوند کمک کنم و خوشبختانه تا الان نشده که سوالی را بی جواب بگذارم؛ در مورد موفقیت هم، بزرگترین موفقیتم را این میدانم که بتوانم تاثیر مثبتی در زندگی افراد و اطرافیانم بگذارم، امیدوارم توانسته باشم این کار را انجام بدهم.

بزرگترین آرزوی اقای پورممی چه چیزی هست؟

یکی از اهداف همیشگیم این هست که بتوانم افراد زیادی را یکجا جمع بکنم و با همدیگر بتوانیم تغییرات بزرگی را در جامعه در جهت مثبت ایجاد کنیم، و به این موضوع ایمان دارم و آینده خودم را به این صورت تصور می‌کنم.

طی فعالیت هایتان با چه مشکلاتی از اول تا به الان درگیر بودید؟

یکی از اصلی ترین مشکلاتی که متاسفانه اکثر جوان ها درگیرآن هستند، مشکلات مالی هست و من هم از این قضیه مستثنی نبودم، خیلی سخت هست که بخواهی با شرایط بد مالی کاری انجام بدهی، اما باید به خلاقیت هایمان تکیه کنیم، من خیلی چیزها نداشتم و توانایی خریدشان را هم

نداشـــتم، شـــاید باورتان نشـــود ولی خودم می‌ســـاختم آن لوازم را، یک مثال ساده هم اینکه سه پایه برای دوربین نمیتوانستم بخرم که بتوانم ویدئو های آموزشی را ضبط کنم، خودم با چهار پایه و مونوپد و چوب و چسب چیزی ســـر هم کردم، فقط بخاطر اینکه در حرکت باشـــم و بخاطر اینکه یک وسیله ای ندارم از مسیرم منصرف نشوم ، وقتی هدف و انگیزه داشته باشی، به هر روشی که شده باید کارت را راه بیندازی.

به نظر خودتان دلیلی که شـــما را از بقیه دانشجویان متمایز و موفق تر کرد چه چیزی می‌تواند باشد؟

قطعا دلایل زیادی دخیل هســـتند اما بنظرم اصلی ترین دلیل، اجتماعی بودنم هست، من با همه سریع رفیق می‌شـــوم، بدون در نظر گرفتن جنســـیت و نـــژاد و زبان و هرچیزی. سریع گرم می‌گیرم و خوشبختانه به همین دلیل دوستان زیادی دارم، درسته هر از گاهی این رفتار من باعث ســـوءتفاهم هم میشود. همین ارتباط باعـــث اتفاق های خیلی خوبه در زندگی من شده است و دومین دلیل هم می‌توانم به داشـــتن علاقه واقعی به این کار اشاره کنم، چون فقط علاقه و انگیزه می‌تواند باعث شود که شـــما با وجود تمامی سختی ها و کمبود ها، باز هم از مســـیرتان منصرف نشوید ، چون شما از خود مسیر لذت می‌برید.

توصیه شـــما برای هم نسل ها و هم رشته های شما چیست؟

نسل من یکی از نسل‌هایست که در بدترین وضعیت اقتصادی کشـــور بزرگ شـــدند و از لحاظ مالی بیشـــترین ضربـــه را خوردند، اما توصیه من به دوستانم این است که، به جای اینکه اجازه بدهند شـــرایط بر آنها غلبه کند ، آنها بر شـــرایط غلبه کنند، ببینید زندگی مثل یک قابلمه آب جوش هســـت، شما اگر یک تخم مرغ و یک ســـیب‌زمینی را بندازی داخل قابلمه، ســـیب زمینـــی در آب جوش نرم می‌شـــود ولی تخم مرغ ســـخت، زندگی و شـــرایط برای همه یکسان هست، همه ما در یک جامعه زندگـــی می‌کنیم، پس بهتر هست بجای بهانه کردن شانس و پارتی، یک خورده به خودمان تکان بدهیم و سعی کنیم خودمان را از این شرایط خارج کنیم.

در مورد کلمات زیر، اولین جمله ای که به ذهنتان می‌رســـد را بفرمایید.

برنامه نویسی: یک شغل آینده دار با درآمد بالا کـــه افـــراد زیـــادی دوســـت دارند به آن برســـند اما اکثرا یا نصفه ول می‌کننـــد یا حوصله ادامه دادن ندارند، چون برخی مواقع ممکن هست بسیار کلافه کننده باشد.

دارک وب: در مـــوردش اطلاعـــات زیـــادی ندارم ولی خب می‌دانم که جای خوبی برای فضولی نیســـت، ممکن هست عواقب روحی بدی داشته باشد.

هک: یک شـــغل هیجان انگیز ولی متاسفانه در ایران آنقدر که باید بها داده نمی‌شـــود، هکرها می‌توانند خیلی کارها در جهت مثبت انجام بدهند.

فرانت اند: فرانت اند دوســـت همیشگی بک اند هست، اگه واقعا باهم دیگر رفیق باشند.

یوتیوب: پلتفرم بسیار بسیار ارزشمندی است که متاسفانه داخل ایران به سختی می‌توانیم ازش اســـتفاده کنیم، یوتیوب یک گنجینه واقعی است.

اچ تی ام ال، سی اس اس: زیربنای هر سایت

بیل گیتس: صاحب یکی از بزرگترین شرکت های نرم افزاری دنیا، می‌تواند الگوی خیلی ها باشد.

هنرســـتان: ســـکوی پرتاب، قطعا هنرستان می‌تواند بهترین سکوی پرتاب و بهترین راه برای ورود به بازار کار باشد.

هر چیزی که حـــس می‌کنید باید می‌پرسیدیم و در بین سوالاتمان نبود.

من می‌خواســـتم در مورد هنرستان و رشته فنـــی صحبت کنـــم، خیلی هـــا فکر میکنند که هرکسی رشته فنی بخواند چه میدانم درسش ضعیف هست یا از روی ناچـــاری رفته فنی خوانده‌است، حتی چندیـــن بـــار به خود من با طعنه گفتند، بخاطر فرار از ســـربازی رفتی دانشـــگاه فنـــی؟ در حالی کـــه اصلا اینطور نیســـت، مـــن بـــه جرئت می‌توانـــم بگویـــم هنرجوهـــا و دانشـــجویان رشته فنی، در بازار کار بسیار بسیار مقدم تر از دانشجویان رشته های دیگر هستند که برنامه نویسی می‌کنند، البته این قضیه شامل همه نمی‌شـــود، ولی به صورت کلی دانشـــجویان فنی در عمـــل بهتر عمل می‌کننـــد، و حتی چندین بار دانشـــجویان از رشـــته های دیگر آمدنـــد پیش من برای مشاوره، اعتراف کردند که ای کاش می‌رفتند رشته فنی و عملی یاد می‌گرفتند، خلاصه که گوش به حرف‌هایـــی که مردم عوام می‌زنند ندهید.

سخن پایانی ...

در آخر تشکر ویژه می‌کنم از بخش اجتماعی فصلنامه تکنوآپ کـــه من را دعوت کردند و مطمئنم که هرکســـی برای خواسته هایش تلاش کافی بکند قطعا به بهترین ها دســـت خواهد یافت.

فقط
علاقه و انگیزه می تواند
باعث شود که شما با وجود تمامی
سختی ها و کمبود ها، باز هم از
مسیر تان منصرف نشوید