به نام خدا

ارائه یک متدولوژی هوش مصنوعی به منظور کشف ناهنجاری در شبکه رایانش ابری با استفاده انتخاب ویژگی و دسته بندی

مولف :

عظیمه باباگل زاده

انتشارات ارسطو

(سازمان چاپ و نشر ایران – ۱۴۰۳)

سرشناسه : باباگل زاده، عظیمه، ۱۳۶۷
عنوان و نام پدیدآور : ارائه یک متدولوژی هوش مصنوعی به منظور کشف ناهنجاری در شبکه رایانش ابری با استفاده انتخاب ویژگی و دسته بندی/ مولف عظیمه باباگل زاده.
مشخصات نشر : انتشارات ارسطو (سازمان چاپ و نشر ایران)،۱۴۰۳.
مشخصات ظاهری : ۴۹ ص.
شابک : ۲-۰۷۵-۴۰۸-۶۲۲-۹۷۸
وضعیت فهرست نویسی : فیپا
موضوع : هوش مصنوعی - شبکه رایانش ابری
رده بندی کنگره : PN۲۱۸۷
رده بندی دیویی : ۸۰۹/۲۳۰
شماره کتابشناسی ملی : ۹۴۹۳۸۳۵
اطلاعات رکورد کتابشناسی : فیپا

نام کتاب : ارائه یک متدولوژی هوش مصنوعی به منظور کشف ناهنجاری در شبکه رایانش ابری با استفاده انتخاب ویژگی و دسته بندی
مولف : عظیمه باباگل زاده
ناشر : انتشارات ارسطو (سازمان چاپ و نشر ایران)
صفحه آرایی، تنظیم و طرح جلد: پروانه مهاجر
تیراژ : ۱۰۰۰ جلد
نوبت چاپ : اول - ۱۴۰۳
چاپ : زبرجد
قیمت : ۴۹۰۰۰ تومان
فروش نسخه الکترونیکی - کتاب‌رسان :
https://chaponashr.ir/ketabresan
شابک : ۲-۰۷۵-۴۰۸-۶۲۲-۹۷۸
تلفن مرکز پخش : ۰۹۱۲۰۲۳۹۲۵۵
www. chaponashr. ir

فهرست مطالب

فصل اول

کلیات

مقدمه

از ابتدای پیدایش ایدۀ رایانش ابری، کاهش پایش کاربر روی داد ەهای خود و امکان دسترسی دیگران به آنها به عنوان اولین دغدغه در حوزۀ امنیت مطرح بوده است .با نگرش همه جانبه به حوزه امنیت، بدیهی است که این موضوع به یک چالش اساسی تبدیل شود . از طرفی پژوهشگران و محققان درصدد ارائه راهکار علمی برای رفع این دغدغه بود ه اند، همچنین شرکتهای تجاری بزرگ برای موفقیت در بازار ارائه سرویس‌های رایانش ابری و جلب اعتماد مشتریان خود، به دنبال ارائه راهکارهای عملی بوده اند.

سازمانها از رایانش ابری در بسیاری از مدل‌های سرویس دهی استفاده می‌کنند. مسائل و نگرانی‌های امنیتی در ارتباط با رایانش ابری وجود دارد اما تمام این نگرانی‌ها به دو دسته کلی تقسیم می‌شوند: اول، مسائل امنیتی مربوط به فراهم کنندگان رایانش ابری و دوم، مسائل امنیتی مربوط به مشتریان. در اغلب موارد، فراهم کننده باید از ایمن بودن زیرساختش مطمئن باشد و از داده‌های مشتریانش و برنامه‌های کاربردی محافظت کند در حالیکه، مشتری باید از عملکرد فراهم کننده خدمات رایانش ابری در راستای ایجاد معیارهای امنیتی مناسب برای محافظت از داده‌هایش مطمئن شود. کابرد گسترده مجازی

سازی در پیاده سازی زیرساخت رایانش ابری نگرانی‌های امنیتی یکسانی برای مشتریان و خدمات عمومی رایانش ابری ایجاد کرده است. مجازی سازی، جایگزین ارتباط بین سیستم عامل و سخت افزار در محاسبات، ذخیره سازی‌ها و حتی شبکه می‌شود. این امر باعث معرفی لایه جدیدی به نام لایه مجازی میشود که خودش نیاز به تنظیم، مدیریت و امنیت صحیح دارد. از این رو در این فصل به ارائه کلیات تحقیق می‌پردازیم تا بتوانیم راهکاری ارائه دهیم که بتواند امنیت ذخیره سازی داده‌های کاربران را افزایش دهد.

رایانش ابری استفاده از سیستم‌های خارج از سایت[1] برای کمک به رایانه‌ها برای ذخیره، مدیریت، پردازش و/یا ارتباط اطلاعات است. این سیستم‌های خارج از سایت به‌جای رایانه یا سایر فضای ذخیره‌سازی محلی، روی ابر (یا اینترنت) میزبانی می‌شوند. آنها می‌توانند هر چیزی را از سرورهای ایمیل گرفته تا برنامه‌های نرم افزاری، ذخیره سازی داده‌ها یا حتی افزایش قدرت پردازش کامپیوتر را در بر گیرند[۱].

"ابر" اصطلاحی است که به سادگی به معنای "اینترنت" است. محاسبات شامل زیرساخت‌ها و سیستم‌هایی است که به رایانه اجازه می‌دهد تا اطلاعات را اجرا و بسازد، استقرار دهد یا با آن تعامل داشته باشد. در رایانش ابری، این بدان معناست که به جای میزبانی زیرساخت‌ها، سیستم‌ها یا برنامه‌های کاربردی بر روی‌هارد دیسک یا یک سرور در محل، آن را روی سرورهای مجازی/آنلاین میزبانی می‌کند که از طریق شبکه‌های امن به رایانه شما متصل می‌شوند[۲].

رایانش ابری یک زیرساخت مهم برای بسیاری از شرکت‌ها است. پس از ۱۰ سال توسعه، رایانش ابری به موفقیت بزرگی دست یافته است و اقتصاد، جامعه، علم و صنایع را به شدت متحول کرده است. به ویژه، با توسعه فناوری کلان داده، تقریباً تمام خدمات آنلاین و خدمات داده بر روی رایانش ابری ساخته شده اند، مانند خدمات بانکداری آنلاین ارائه شده توسط بانک‌ها، خدمات الکترونیکی ارائه شده توسط اخبار. رسانه‌ها، سیستم‌های اطلاعات ابری دولتی ارائه شده توسط ادارات دولتی، خدمات تلفن همراه ارائه شده توسط شرکت‌های ارتباطی. علاوه بر این، ده‌ها هزار استارت آپ به ارائه خدمات رایانش ابری

[1] Off-site

متکی هستند. بنابراین، اطمینان از قابلیت اطمینان ابر بسیار مهم و ضروری است. با این حال، واقعیت این است که سیستم‌های ابری فعلی به اندازه کافی قابل اعتماد نیستند.
در واقع، با توسعه و بلوغ مستمر رایانش ابری، تعداد زیادی از سیستم‌های تجاری سنتی بر روی پلت فرم ابری مستقر شده اند[۳]. رایانش ابری منابع سخت افزاری موجود را از طریق فناوری مجازی سازی یکپارچه می‌کند تا یک منبع اشتراکی ایجاد کند که برنامه‌ها را قادر می‌سازد تا منابع محاسباتی، ذخیره سازی و شبکه را بر اساس تقاضا به دست آورند و به طور موثر مقیاس پذیری و استفاده از منابع زیرساخت‌های فناوری اطلاعات سنتی را افزایش داده و هزینه عملیات سنتی را به میزان قابل توجهی کاهش دهد. سیستم‌های تجاری با این حال، با افزایش تعداد برنامه‌های کاربردی در حال اجرا بر روی ابر، مقیاس مرکز داده ابری در حال گسترش است، سیستم رایانش ابری فعلی بسیار پیچیده شده است، که عمدتاً در موارد زیر منعکس می‌شود[۴]: ۱) مقیاس بزرگ. یک مرکز داده معمولی شامل بیش از ۱۰۰۰۰۰ سرور و ۱۰۰۰۰ سوئیچ است، تعداد گره‌های بیشتر معمولاً به معنای احتمال بیشتر خرابی است. ۲) ساختار برنامه پیچیده. جستجوی وب، تجارت الکترونیک و سایر برنامه‌های ابری معمولی رفتار تعاملی پیچیده ای دارند. برای اجرای سریعتر درخواست‌ها نیاز به رقابت برای منابع وجود دارد.
رقابت منابع با یکدیگر تداخل خواهد داشت و بر عملکرد برنامه تأثیر می‌گذارد. پیچیدگی این سیستم‌های رایانش ابری، پیچیدگی ساختار تعامل برنامه‌ها و الگوی اشتراک ذاتی پلتفرم‌های ابری، سیستم‌های ابری را نسبت به پلت‌فرم‌های سنتی مستعد ناهنجاری‌های عملکردی می‌کند. می‌توان گفت که ناهنجاری یک حالت عادی در رایانش ابری است[۵].
برای تجزیه و تحلیل بیشتر، رقابت منابع، تنگناهای منابع، پیکربندی نادرست، نقص نرم افزار، خرابی سخت افزار و حملات خارجی می‌تواند باعث ناهنجاری یا خرابی سیستم ابری شود. ناهنجاری عملکرد به هرگونه کاهش ناگهانی عملکرد که از رفتار عادی سیستم منحرف می‌شود، اشاره دارد. برخلاف قطعی‌هایی که باعث توقف فوری سیستم می‌شوند، ناهنجاری‌های عملکرد معمولاً منجر به کاهش کارایی سیستم می‌شوند. دلایلی مانند پیکربندی نادرست، نقص نرم افزار، خرابی سخت افزار، اغلب می‌تواند باعث ناهنجاری

عملکرد شود. برای سیستم‌های رایانش ابری، تشخیص قطعی یا سایر ناهنجاری‌های عملکردی کافی نیست، زیرا این ناهنجاری‌ها اغلب باعث وقفه در سرویس می‌شوند و می‌توانند به سادگی با راه‌اندازی مجدد یا جایگزینی سخت‌افزار برطرف شوند. در حالی که ناهنجاری‌های عملکرد ناشی از اشتراک منابع و تداخل، ارزش بیشتری برای توجه دارند، ، زیرا ناهنجاری‌های عملکرد را می‌توان قبل از قطع سرویس حذف کرد تا از ادامه خدمات اطمینان حاصل شود.[۶]

اگر ناهنجاری‌های عملکرد سیستم رایانش ابری به موقع رسیدگی نشود، ممکن است عواقب بسیار جدی ایجاد کند که نه تنها بر عملکرد عادی سیستم تجاری تأثیر می‌گذارد، بلکه مانع استقرار خدمات خود در سیستم‌های ابری نیز می‌شود. به خصوص برای آن دسته از برنامه‌های ابری حساس به تأخیر، از بین بردن ناهنجاری‌های عملکرد به موقع بسیار مهم است. به عنوان مثال، آمازون کاهش ۱٪ در فروش به ازای هر ۱۰۰ میلی ثانیه تاخیر، گوگل ۲۰٪ کاهش در ترافیک به ازای هر ۰,۵ ثانیه تاخیر در صفحه جستجو، و معامله گران سهام دریافتند که در صورت تجارت الکترونیکی آنها، ۴۰۰ میلیون دلار ضرر خواهد داشت. پلتفرم ۵ میلی ثانیه از رقبا عقب افتاد. تحقیقات دیگر نیز نشان می‌دهد که میانگین حداکثر زمان خرابی مرکز داده ابری حدود ۱۰۰ ساعت است که تجربه کاربران سرویس ابری را به طور جدی تحت تاثیر قرار می‌دهد. در محیط ابری، از آنجایی که تعداد زیادی از سیستم‌های تجاری در مرکز داده ابری مستقر شده‌اند، خرابی مرکز داده ابری بر تعداد زیادی از کاربران تأثیر می‌گذارد، مانند خرابی آمازون S3 که قبلاً ذکر شد، که منجر به ضررهای اقتصادی جدی می‌شود[۷].

بنابراین، تشخیص به موقع و دقیق ناهنجاری‌های رایانش ابری بسیار مهم است. تشخیص ناهنجاری ابزاری موثر برای کمک به مدیران پلتفرم ابری برای نظارت و تجزیه و تحلیل رفتارهای ابری و بهبود قابلیت اطمینان ابر است. این به شناسایی رفتار غیرعادی سیستم کمک می‌کند تا مدیران پلتفرم ابری بتوانند قبل از خرابی سیستم یا خرابی سرویس، عملیات پیشگیرانه را انجام دهند. با این حال، به دلیل ویژگی‌هایی مانند مقیاس بزرگ، پیچیده و اشتراک منابع، تشخیص دقیق ناهنجاری‌ها در رایانش ابری بسیار دشوار است.

اگر نتوان ناهنجاری‌ها را به طور دقیق تشخیص داد، بازیابی بیشتر غیرممکن خواهد بود. با توجه به اهمیت این مشکل، ارائه دهندگان خدمات رایانش ابری فعلی معمولاً خدمات نظارت آنلاین را ارائه می‌دهند[۸].

فصل دوم

مبانی نظری

مقدمه

این فصل مهمترین اصطلاحات رایج در پژوهش را ارائه کرده و همینطور معماری‌ها در محیط رایانش ابری و انواع ابر و خدماتی که در محیط رایانش ابری مطرح میکند و مباحث مربوط به امنیت در رایانش ابری و تشخیص نفوذ نیز مورد بررسی قرار میگیرد. در انتها الگوریتم‌های بکار رفته در پژوهش ارائه و تشریح شده است.

رایانش ابری

رایانش ابری یک اصطلاح کلی برای هر چیزی است که شامل ارائه خدمات میزبانی شده از طریق اینترنت می شود.[۹].

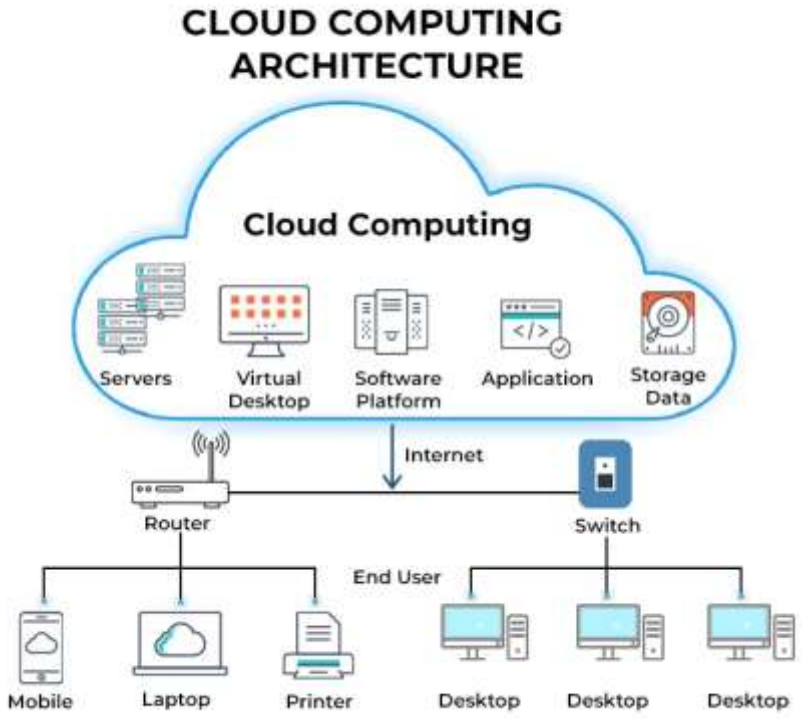
یک ابر می‌تواند خصوصی یا عمومی باشد. یک ابر عمومی خدمات را به هر کسی در اینترنت می‌فروشد. یک ابر خصوصی یک شبکه اختصاصی یا یک مرکز داده است که خدمات میزبانی شده را برای تعداد محدودی از افراد با تنظیمات دسترسی و مجوزهای خاص ارائه می‌کند. خصوصی یا عمومی، هدف رایانش ابری ارائه دسترسی آسان و مقیاس پذیر به منابع محاسباتی و خدمات فناوری اطلاعات است[۱۰].

زیرساخت ابری شامل اجزای سخت افزاری و نرم افزاری مورد نیاز برای اجرای صحیح یک مدل رایانش ابری است. رایانش ابری را می‌توان به عنوان رایانش کاربردی یا رایانش بر اساس تقاضا نیز در نظر گرفت.

رایانش ابری با امکان دسترسی به داده‌ها و برنامه‌های کاربردی ابری از طریق اینترنت از سرورهای فیزیکی، پایگاه‌های اطلاعاتی و رایانه‌ها به دستگاه‌های سرویس گیرنده کار می‌کند.

یک اتصال شبکه اینترنتی، بخش پیشخوان[1] را که شامل دسترسی به دستگاه مشتری، مرورگر، شبکه و برنامه‌های نرم‌افزار ابری است، با بخش پسخوان[2] که از پایگاه‌های داده، سرورها و رایانه‌ها تشکیل می‌شود، پیوند می‌دهد. قسمت پسخوان به عنوان یک مخزن عمل می‌کند و داده‌هایی را ذخیره می‌کند که توسط قسمت پیشخوان قابل دسترسی است. در شکل ۱-۱ ساختار کلی رایانش ابری نشان داده شده است[۱۱].

[1] Front end
[2] Back end



شکل ۲-۱: ساختار کلی رایانش ابری

ارتباطات بین قسمت‌های پیشخوان و پسخوان توسط یک سرور مرکزی مدیریت می‌شود. سرور مرکزی برای تسهیل تبادل داده‌ها به پروتکل‌ها متکی است. سرور مرکزی از نرم افزار و میان افزار برای مدیریت اتصال بین دستگاه‌های مختلف کلاینت و سرورهای ابری استفاده می‌کند. به طور معمول، یک سرور اختصاصی برای هر برنامه یا حجم کاری جداگانه وجود دارد.

انواع سرویس‌های رایانش ابری

رایانش ابری را می‌توان به سه دسته کلی ارائه خدمات یا اشکال رایانش ابری تقسیم کرد[۱۳]:

سرویس IaaS: ارائه دهندگان IaaS، مانند خدمات وب آمازون (AWS)، یک نمونه سرور مجازی و فضای ذخیره سازی و همچنین رابطهای برنامه نویسی برنامه (API) را ارائه می‌دهند که به کاربران اجازه می‌دهد بارهای کاری را به یک ماشین مجازی (VM) منتقل کنند. کاربران ظرفیت ذخیره سازی اختصاص داده شده دارند و می‌توانند به صورت دلخواه VM و فضای ذخیره سازی را راه اندازی، توقف، دسترسی و پیکربندی کنند. ارائه دهندگان IaaS نمونه‌های کوچک، متوسط، بزرگ، فوق العاده بزرگ و بهینه سازی شده با حافظه یا محاسبات را علاوه بر امکان سفارشی سازی نمونه‌ها، برای نیازهای حجم کاری مختلف، ارائه می‌دهند. مدل ابری IaaS نزدیکترین به یک مرکز داده از راه دور برای کاربران تجاری است.

سرویس PaaS: در مدل PaaS، ارائه دهندگان ابری ابزارهای توسعه را در زیرساخت‌های خود میزبانی می‌کنند. کاربران با استفاده از APIها، پورتال‌های وب یا نرم افزار دروازه به این ابزارها از طریق اینترنت دسترسی دارند. PaaS برای توسعه عمومی نرم افزار استفاده می‌شود و بسیاری از ارائه دهندگان PaaS نرم افزار را پس از توسعه میزبانی می‌کنند. محصولات رایج PaaS شامل پلتفرم لایتنینگ Salesforce، AWS Elastic Beanstalk و Google App Engine هستند.

سرویس SaaS: SaaS یک مدل توزیع است که برنامه‌های نرم افزاری را از طریق اینترنت ارائه می‌دهد. این برنامه‌ها را اغلب وب سرویس می‌نامند. کاربران می‌توانند از هر مکانی با استفاده از رایانه یا دستگاه تلفن همراهی که به اینترنت دسترسی دارد به برنامه‌ها و خدمات SaaS دسترسی داشته باشند. در مدل SaaS، کاربران به نرم افزارهای کاربردی و پایگاه‌های داده دسترسی پیدا می‌کنند. یکی از نمونه‌های رایج برنامه SaaS مایکروسافت ۳۶۵ برای بهره وری و خدمات ایمیل است[۱۳] شکل ۲-۱ انواع سرویس‌های رایانش ابری و کاربرد آن‌ها را نشان می دهد.

شکل ۲-۲: انواع سرویس‌های رایانش ابری و کاربرد آن‌ها

مدل‌های استقرار رایانش ابری

رایانش ابری از سه مدل استقرار برای ابرها استفاده می‌کند[۱۴] که شکل ۲-۳: انواع استقرار ابرها را نشان می‌دهد.

شکل ۲-۳: انواع استقرار ابرها