مدلسازی رویکرد هوشمند ارزیابی ریسک برای محیط رایانش ابری با استفاده از هوش مصنوعی و الگوریتم های نظارت شده یادگیری ماشین

نویسندگان:امیرحسین کریمی

دانشجو دانشگاه افسری امام علی(ع)تهران

چکیده

ستون اصلی بازار رقابتی و آتی امروز قطعا تبدیل شدن به رایانش ابری است و بنابراین شرکت ها از قابلیت های خدمات رایانش ابری استفاده می کنند. برای بهبود ابتکارات امنیتی توسط رایانش ابری سرویس یا CRP، انواع جدید ابزارها و پروتکل ها همیشه مورد تقاضا هستند. به منظور ایجاد روش جامع ارزیابی ریسک، مرور ادبیات گسترده ای برای شناسایی عوامل خطر که ممکن است انجام شود بر پذیرش رایانش ابری تأثیر می گذارد. در این زمینه عوامل خطر مختلفی شناسایی شدند. پس از انتخاب ویژگی و شناسایی عوامل خطر، مورد استفاده برای انتخاب موثرترین ویژگی ها با استفاده از الگوریتم های رگرسیون خطی. سپس از تکنیک‌های AI-ML مانند درخت تصمیم (DTC)، طبقه‌بندی‌کننده فیلتر تصادفی، ستاره k با روش RMSE استفاده می‌شود. تجزیه و تحلیل تهدیدات در محیط CC نتایج تجربی تقسیم مجموعه داده را به (۹۵٪ -۵٪) نشان داد. بهترین نتیجه را از هر پارتیشن بندی باقی مانده ارائه می دهد و علاوه بر این الگوریتم DTC ارائه شده را ارائه می دهد بهترین نتایج از کل مجموعه داده های مورد استفاده در تنظیمات آزمایشی

کلید واژه ها: هوش مصنوعی رایانش ابری (CC) امنیت ابری فراگیری ماشین ارزیابی ریسک

۱. مقدمه

ابر [۱] یکی از پرکاربردترین و پویاترین اختراعات است که تمرکز فناوران را در صحنه جهانی جلب کرد. اگرچه رایانش ابری با پاداش های بزرگی مانند خدمات اندازه گیری شده، کشش سریع، مقیاس‌پذیری و مهم‌ترین آن هزینه کم برای شرکت‌ها است با نسبت خوبی از خطرات امنیتی تعبیه شده است که توسط هیچ شرکت دیگری وجود ندارد که بتوان آن را نادیده گرفت. خطر امنیتی که از طیف وسیعی از آسیب پذیری های ذاتی هر یک سرچشمه می گیرد نوع سیستم رایانش ابری و در غیاب امنیت قابل اعتماد دستورالعمل ها، بی میلی ظاهری از سوی سازمان ها وجود دارد برای اتخاذ یک محیط قدرتمند به نام رایانش ابری می باشد [۲].

بدون زحمت در مورد تعمیرات فیزیکی و فنی یا چالش های مدیریت منابع اصلی، رایانش ابری کاربرانی که قادر به کنترل و دسترسی به منابع خود به صورت آنلاین با کمک اینترنت در هر زمان بدون توجه به مکان هستند [۳]. علاوه بر این، منابع آن مقیاس پذیر و پویا نیز می باشد. این یک پلتفرم محاسباتی مستقل است که کاملاً با محاسبات ابزار و شبکه متفاوت است. بهترین مثال رایانش ابری را می توان در Google Apps مشاهده کرد که در دسترسی به خدمات از طریق مرورگر کمک می کند و می تواند به راحتی بر روی تعداد زیادی از رایانه ها از طریق پیوندهای اینترنتی نصب شود [۴]. با استفاده از اینترنت، منابع به راحتی از محیط ابری از هر مکان و در هر زمان در سراسر جهان قابل دسترسی هستند. در مقایسه با سایر مدل های محاسباتی، از نظر هزینه کمتر است. به عنوان ارائه دهنده خدمات پاسخگو برای دسترسی و در دسترس بودن خدمات مختلف، هزینه نگهداری آن ناچیز است و مشتریان با مدیریت آزاد می مانند و مسائل نگهداری منابع در انتهاست. به خاطر این ویژگی‌ها، رایانش ابری بر اساس تقاضا یا محاسبات ابزار نامیده می‌شود. یکی از ویژگی های مهم رایانش ابری مقیاس پذیری آن است و از طریق مجازی سازی

سرورهای آنها به دست می آید [۵،۶]. به نرم افزار، محاسبات، خدمات ذخیره سازی و دسترسی به داده ها می دهد که نیازی به دانش کاربر نهایی پیکربندی سیستم ندارد و خدمات یا موقعیت فیزیکی را ارائه می دهد.

فناوری رایانش ابری بر روی سه SPI (نرم افزار) مختلف کار می کند زیرساخت پلت فرم) مدل ها و چهار استقرار (عمومی، خصوصی، مدل‌های ترکیبی و جامعه [۷]. بر اساس استفاده یا نیاز مصرف کننده می تواند از سرویس(های) ابر استفاده کرده و ابر را مستقر کند. در حال حاضر، دارای سه نوع مدل خدمات است که SPI (نرم افزار) نیز نامیده می شود زیرساخت پلت فرم) مدل هایی که در زیر آورده شده است [۸]:

Ø SaaS(نرم افزار به عنوان یک سرویس) -:[9]

این یک طرح توزیع و استقرار نرم افزار است که در آن برنامه ها در قالب خدمات به مشتریان تحویل داده می شوند. برای دسترسی و با استفاده از سرویس یا اپلیکیشنی که در فضای ابری تعبیه شده است، مشتریان به راحتی این امکانات را دریافت می کنند. چنین برنامه ای می تواند اجرا شود وب سرورهای ارائه دهنده خدمات یا ماشین های محاسباتی مشتری SaaS .خدماتی را برای مدیریت پچ به طور کارآمد ارائه می دهد و همکاری را نیز ارتقا می دهد. کمترین توسعه پذیری و بیشترین میزان مسئولیت ایمن سازی توسط ارائه دهنده ابر گرفته شده است. اساساً از برنامه های ارائه دهنده از طریق شبکه استفاده می کند که "Salesforce.com" یک مثال است، در صورت لزوم اطلاعات برای تعامل بین مصرف کننده و خدمات میزبانی به عنوان بخشی از سرویس در فضای ابری و ارائه خدمات پایه کسب و کار و برنامه ها که شامل پردازش کلمه و ایمیل توسط Google است ارائه میشود [11]

Ø PaaS(پلتفرم خدمات) -:[11]

مشتری با توانمندسازی آنها در سازماندهی برنامه و نرم افزار و برنامه های کاربردی خود در حوزه ابری، به پلتفرم دسترسی پیدا می کند. فناوری اطلاعات در جایی در وسط قرار دارد، با قابلیت توسعه و امنیت ویژگی هایی که باید توسط مشتری استفاده شود. مسئولیت اصلی PaaSدر حال استقرار برنامه های مرتبط با مشتری در یک ابر است.

Ø IaaS(زیرساخت به عنوان یک سرویس) -:[12]

این مدل ذخیره سازی، پردازش و دیگر منابع مهم محاسباتی برای مشتری است. این کلاینت‌ها چارچوب اصلی ابر را مدیریت یا کنترل نمی‌کنند، اما دارای قابلیت‌های دسترسی در ذخیره‌سازی اولیه، سیستم عامل، مهارت‌های محاسباتی هستند .خدمات استاندارد در شبکه داده شده و برنامه های کاربردی مستقر شده است. آی تی به توسعه پذیری بیشتر و کمترین مسئولیت امنیتی که توسط ارائه دهنده ابر بر عهده می گیرد، نیاز دارد. ظرفیت شبکه (سرورها، سوئیچ ها، روترها و سایر سیستم ها) ذخیره سازی، پردازش و سایر منابع محاسباتی اساسی تحت این مدل قرار می گیرند.

رایانش ابری از نظر ویژگی ها بسیار غنی است اما آینده های اصلی Cloud محاسبات به شرح زیر است:[13]

Ø استفاده از خدمات مبتنی بر اینترنت برای پشتیبانی از فرآیند کسب و کار: -

پلتفرم رایانش ابری به شبکه‌های خاصی محدود نمی‌شود، اما می‌توان از طریق شبکه عظیمی از آنها که اینترنت است، به آن دسترسی داشت. [۱۳].

Ø خدمات IT اجاره ای مبتنی بر ابزار: -

رایانش ابری شامل اجاره منابع محاسباتی مانند پهنای باند شبکه، نرم‌افزار و سخت‌افزار، بر اساس تقاضا یا بر اساس نیاز، مانند محاسبات ابزاری که پیش‌روی رایانش ابری بود. بدون نگرانی در مورد هزینه نصب و نگهداری رایانش ابری [13].

این ترکیبی از فن‌آوری‌ها و روش‌های رایج است که در پارادایم زیرساختی جدید تعبیه شده است که انعطاف‌پذیری، مقیاس‌پذیری، زمان راه‌اندازی سریع‌تر، کاهش هزینه‌های مدیریت، در دسترس بودن به موقع منابع و چابکی کسب‌وکار را فراهم می‌کند.

۲. کارهای مرتبط

رایانش ابر یک توسعه طبیعی برای مراکز محاسباتی و اطلاعات/داده‌هایی است که با فناوری‌های مجازی‌سازی فعال می‌شوند .متعادل سازی حجم کار و مدیریت سیستم های خودکار [۱۴]. با همه این تحولات فناوری‌ها، پیچیدگی‌هایی به وجود آورد که به عدم تمایل به پذیرش ابر توسط بازار کمک می‌کند. اصل موضوع، تهدیدات امنیتی برای انتقال

داده ها و برنامه ها در آن است در ابر به دلایل واضح علاوه بر این، تهدیدات امنیتی نیز وجود دارد دسته بندی های مختلف مانند تهدیدات امنیتی داده ها، تهدیدات امنیتی شبکه، تهدیدات امنیتی سرور، تهدیدات امنیتی برنامه، احراز هویت و تهدیدات امنیتی مجوز، تهدیدات امنیتی وب، تهدیدات امنیتی مجازی سازی. هر یک از خطرات امنیتی از مسائل یا مسائل خاص خود تشکیل می شود نگرانی ها. یکی از مشکلات برجسته در امنیت شبکه و امنیت داده ها، حملات سایبری است. بنابراین، کل این بررسی ادبیات عمدتا است نگران تهدیدات یا مسائل امنیتی مختلف در محیط ابری است.

در [۱۵]، نویسندگان مروری بر مطالعه ای ارائه می دهند که به بررسی CC پرداخته است مشکلات امنیتی، چالش ها و راه حل هایی که شامل یک یا چند مورد می شود تکنیک های یادگیری ماشینی این شامل نگاهی به چندین دستگاه است. روش های یادگیری مانند نظارت، بدون نظارت، نیمه نظارت، و یادگیری تقویتی، که برای رفع نگرانی های امنیتی ابر استفاده می شود. سپس، احتمالات تحقیقاتی آینده را برای مدل‌های CC شناسایی می‌کند تا امنیت آنها را تضمین کند.

با توجه به ویژگی‌های نظری، مزایا و جنبه‌های منفی آن‌ها، عملکرد هر رویکرد را مقایسه می‌کند. علاوه بر این، آن را با هدف ترویج استفاده از بهترین شیوه ها برای ارائه تضمین امنیت و حفاظت در حوزه رایانش ابری، Cloudامنیت اتحادها (CSA) یک سازمان غیرانتفاعی است CSA .همچنین دانشی را در مورد نحوه استفاده از Cloud Computingبرای کمک به محافظت کامل از سایر اشکال محاسبات ارائه می دهد. از این رو در حال شناسایی است به عنوان هفت خطر اصلی برای پلتفرم ابری از طریق مقاله «تهدیدهای برتر به Cloud Computing V1.0"که به شرح زیر است:[16،17]

Ø کاربرد شیطانی و سوء استفاده از رایانش ابری

Ø رابط های برنامه نویسی برنامه به طور ناامن

Ø برنامه های مخرب در داخل ماشین ها

- آسیب پذیری های مرتبط با فناوری اشتراکی
- از دست دادن/نشت اطلاعات
- خدمات و حساب
- ربودن ترافیک

رایانش ابری مستعد تهدیدات امنیتی چندگانه به اشکال مختلف است تهدیدات سطح شبکه برای تهدیدات سطح برنامه [۱۸-۲۰]. دلیل اینکه انجام بررسی ادبیات این است که بفهمیم رایانش ابری دقیقاً به چه معناست، کار کردن رایانش ابری، و چه مشکلاتی دارد در رایانش ابری همچنین بر چگونگی کاهش خطرات متمرکز شد و شرکت ها/مصرف کنندگان را تشویق به استفاده از رایانش ابری کنید محیط.

خطرات، ضعف ها و کاهش ریسک و همچنین هنجارها و قوانین، در [۲۱] برجسته شده است. این سه فناوری سپس با استانداردهای بین المللی (OWASP, NIST, ISO, و GDPR) نشان می‌دهند که اکثر استانداردها و مقررات هوش مصنوعی و IoT هنوز در حال توسعه هستند، در حالی که رایانش ابری از پایه کافی برای پشتیبانی از استانداردها برخوردار است. برای مقابله با DDoS نویسنده یک الگوریتم سیستم تشخیص DDoS بر اساس C.4.5 ایجاد کرد [۲۲]. این روش، هنگامی که با رویکردهای تشخیص امضا ترکیب می‌شود، درخت تصمیمی را ارائه می‌کند که می‌تواند حملات امضایی برای حملات سیل DDoS را به طور خودکار و مؤثر شناسایی کند. انتخاب کرد رویکردهای مختلف یادگیری ماشین و مقایسه نتایج برای اعتبارسنجی سیستم. نویسندگان در [۲۳] سیستم پیشنهادی خود را نشان می دهند نه تنها طیف وسیعی از حملات سایبری را تشخیص می دهد، بلکه آنها را نیز شناسایی می کند با دقت بسیار بالا (تا ۹۷.۱۱٪). همچنین مقایسه هایی را با روش های فعلی مبتنی بر یادگیری ماشین به منظور نشان دادن کارایی راه حل پیشنهادی آن پردازش و تجزیه و تحلیل عظیم داده های به دست آمده از روش ها و حسگرهای S۳، همانطور که توسط نویسنده توضیح داده شده است در [۲۴]، دیدگاه های جالبی برای توسعه یک فناوری یکپارچه ارائه می دهد سیستم برای حفاری.

کاربرد الگوریتم های یادگیری ماشین برای ارزیابی ریسک می باشد بر اساس [۲۵]، همانطور که با روند افزایشی در انتشارات سالانه مشاهده می شود، به وضوح یک موضوع مطالعه در حال توسعه است. رویکردهای یادگیری ماشین ممکن است بهبود ارزیابی ریسک سنتی با ارائه بینش‌های مبتنی بر داده داده های بیشتری در مورد سیستم های مختلف اجتماعی و فنی جمع آوری شده است. نویسنده از [26] تکنیک ریاضی برای خودکارسازی تشخیص ناهنجاری با ادغام اصول طراحی موتور شناختی، محاسبات لبه ارائه می‌کند .هوش مصنوعی و یادگیری ماشینی با تعبیه مصنوعی هوش و یادگیری ماشینی در لبه شبکه های اینترنت اشیا، این موتور یک تغییر گام در ارائه ایمن و کاربردی در زمان واقعی ایجاد می کند .هوش برای تجزیه و تحلیل خطرات سایبری پیش‌بینی‌کننده است

از روزهای اولیه طراحی کامپیوتر، نفوذ مبتنی بر شبکه سیستم های تشخیص (NIDS) که از معیارهای آماری یا رایانه استفاده می کنند آستانه ها به تحقیقات امنیتی مرتبط شده اند [۲۷]. با این حال، دارای نرخ بالای کاذب منفی (عدم تشخیص) و کاذب مثبت هستند، آنها برای تجزیه و تحلیل خطرات سایبری معاصر یعنی سیستم های شبکه ای و بسیار پیچیده ICT (هشدارهای نادرست) بی فایده هستند. در در مورد اینترنت اشیا، تشخیص تهدید توزیع شده در سطح مه نشان داده شده است مقیاس پذیرتر از ابر متمرکز [۲۸] است. اگر بردارهای حمله شناخته شده است، شکلی از حمله با استفاده از واحدهای حافظه کوتاه مدت دوسویه (LSTM) معرفی شده به شبکه عصبی بازگشتی (RNN)می تواند دستیابی به دقت ۹۹.۹۹۹٪ [۲۹] داشته باشد. به طور مشابه، در مقایسه با سایر الگوریتم‌ها، یک چارچوب طبقه‌بندی شبکه سیامی (SNCF) ممکن است عدم تعادل پیش‌بینی ریسک را کاهش داده و یافته‌های قابل اعتمادتری ارائه دهد[30] .

امنیت شبکه ابری طبقه بندی انواع مختلف را نشان می دهد حملات ابری که در گذشته اخیر رخ داده‌اند و همچنین مواردی را فهرست می‌کند راه حل های موفقیت آمیز برای کاهش خطرات [۳۱،۳۲]. مرور ادبیات، انواع مختلفی از تهدیدات و حملات را نشان می دهد و شبکه های ابری شامل Denial of Service (Distributed DoS،

HDoS، XDoS می باشد حمله، Man-in-the-Middle، حمله جعل IP، حمله Sniffer، حمله مجدد، حمله دیکشنری، حمله تزریقی، Hypervisor، Wrapping حمله و غیره [۳۳]. موارد برجسته Do's با دسته ها هستند حملات DDoS و Man-in-the-Middle. تحت امنیت شبکه ابری تهدیدات، دو دسته از حملات را تحلیل کرده است که در شبکه های ابری برجسته تر هستند. این دو دسته شامل حملات DoS و حمله Man-in-the-Middle هستند (DDoS، XDoS، HDoS). حملات DoS حملات بسیار قوی هستند که خدمات را برای مدت طولانی قطع می کنند. در عوض اگر حمله ای به طور مخرب در ارتباطات دسترسی پیدا کند پیوند دهید تا ارتباطات را کنترل و نظارت کند و پیام ها را دستکاری کند زیرا که برای نیت های بدخواهانه، حمله Man-in-the-middle صورت می گیرد. با کمک روشهای احراز هویت و شناسایی توسط اعتبارسنجی هویت کاربران می تواند از این گونه آسیب ها جلوگیری کند. تعداد کمی حملات شبکه ای در زیر شرح داده شده است:

i Man-in-the-Middle Attack

ii حمله انکار سرویس (DoS).

iii حمله DoS توزیع شده (DDoS

IV انکار

v امتیازات ارتفاع

حمله کرم ها و ویروس ها

vii حمله جعل.

viii آدرس های IP استفاده مجدد.

ix مسمومیت با کوکی.

xترمز.CAPTCHA

xi هک گوگل

xii Dictionary Attack.

xiii حملات تزریق بدافزار.

xiv حمله اسنیفر.

xv دستکاری.

xvi استراق سمع/ افشای اطلاعات.

xvii حمله مجدد

xviii حمله بسته بندی.

جدای از این مشکلات، قابل توجه است که صنایع برای اتخاذ رایانش ابری بی میل هستند و نویسندگان مختلف دیدگاه های متفاوت برای عدم تمایل دارند بنابراین به دلیل عدم تمایل شرکت ها و مصرف کنندگان به پذیرش خدمات ابری نیاز به بررسی دلایل وجود دارد.

Harshit Srivastavaو همکاران در[34] ، Secure Cloud's Control Frameworkمعتقدند که فناوری بزرگ بعدی رایانش ابری است .با کاربرد آن برای اندازه های مختلف سازمان، اما مسائل امنیتی و حفظ حریم خصوصی باعث نگرانی جدی برای پذیرش شده است که نیاز به توجه در این مقاله نویسندگان از بسیاری از نتایج نظرسنجی استفاده کرده اند تا به این نتیجه برسند که امنیت و حریم خصوصی امنیت فیزیکی، محیطی و مجازی سازی مسئولیت فروشنده است. این مقاله نشان می دهد که سازمان‌ها می‌توانند بر روی سه لایه اصلی مانند لایه فیزیکی، منطقی و روش‌شناسی برای مقابله با تهدیدات به ترتیب امنیت شبکه و امنیت داخلی در مرکز داده اعمال کنترل کنند . نویسندگان یک نهاد حاکم با چارچوب کنترل خودکار پیشنهاد کرده اند که هدف محاسبه شاخص تهدید برای حل چالش های امنیتی با ایجاد ارتباط در CSP ها بر اساس حملات موجود است.

در [۳۵]، نویسنده پروتکل‌های این فناوری نوظهور و جدید رایانش ابری را توضیح می‌دهد که خدمات و منابع مشترک را در کاهش قیمت نرم افزار و سخت افزار به همراه امنیت کمی مرتبط چالش ها در حین استفاده از خدمات ابری علاوه بر این، نویسنده در مورد مشخصه اشغال چندگانه تمرکز می کند در حالی که مشکلات امنیت اطلاعات در فضای

ابری که توسط CSA در معرض دید قرار گرفته است نیز صحبت می شود. رایانش ابری مسئله امنیت را می توان با طراحی یا تغییر قوی کاهش داد که معماری آن توسط نویسندگان به نتیجه رسید.

با توجه به [۳۶]، نویسنده فرض می کند که برای تأمین منابع و داده های کاربران، مهم ترین هدف باید حفظ سیا باشد (محرمانه بودن، یکپارچگی و در دسترس بودن) به منظور ادامه سرویس ابری برای کسب و کار تحت چالش های نوظهور امنیتی که این فناوری را تهدید می کند. نویسندگان از بسیاری از نتایج نظرسنجی استفاده کرده اند همانطور که در سال ۲۰۱۳ حمله DoS پنجمین تهدید در بین افراد بدنام اعلام شد ممکن است منجر به آسیب سخت افزار یا داده ها و در نتیجه از دست دادن پول در صورت ربوده شدن سرویس توسط CSA (Cloud اتحاد امنیتی). این مقاله همچنین تعداد کمی از حملات DoS و DDoS را توصیف می کند و اثرات آن بر ابر با قطعنامه های فعلی مطابق دارد. با این حال، این مقاله عمدتاً بر دو دسته از حملات DoS یعنی H-DoS و X-DoS و Cloud Protectorو Cloud Trace Back (CTB) را برای حذف این موارد پیشنهاد می کند انواع حملات و Cloud Defender System (CSQD)برای کاهش XML آسیب پذیری در وب است.

در [۳۷]، نویسنده رایانش ابری را به عنوان یک تغییر فنی برای ارائه خدمات از راه دور توسط شخص ثالثی به نام ارائه دهندگان خدمات مورد بحث قرار داد .نویسندگان در درجه اول به تهدیدهای خودی با دو دیدگاه نگاه کرده اند با دید ارائه دهنده خدمات ابری و بعداً با برون سپاری ابر دیدگاه و بر این اساس اقدامات متقابلی را پیشنهاد کرده اند. در برابر برون سپاری ابر اقدامات متقابل برای دیدگاه کاربر مبتنی بر میزبان است IDS/IPS، حسابرسی گزارش و با طرف ارائه دهنده، احراز هویت چند عاملی، تشخیص ناهنجاری و تفکیک وظایف است. محققان بیشتر بر روی ۳ نوع مختلف از حملات در دسته فعلی مانند تغییر تشکیل دهنده فایل کاربران بدون اطلاع آنها، به دست آوردن خصوصی کلیدهای کاربران فایل های رمزگذاری شده، آلودگی با الگوهای وب و تکنیک های کاهش آنها تمرکز دارند. نویسندگان با بیان اینکه سازمان ها باید از آسیب‌پذیری‌هایی که در اثر استفاده از سرویس‌های ابری در معرض دید قرار می‌گیرند، آنگاه مراقب در دسترس بودن خدمات ابری برای کارمندان سازمان ها باشید.

در مقاله [۳۸]، نویسنده بیان می کند که امنیت ابری در حال تکامل است زیر دامنه امنیت اطلاعات، امنیت شبکه و امنیت کامپیوتر. ملاحظات امنیتی حیرت انگیز متخصصان امنیت اطلاعات باید هنگام ارزیابی خطرات رایانش ابری در نظر گرفته شود. مسائل اساسی امنیت برنامه و داده ها و ابر است کاربر و ارائه دهنده هر دو مسئول این هستند. با این حال، ارائه دهندگان باید اطمینان حاصل کنند که زیرساخت آنها امن است و برنامه های مشتری و نویسندگان بحث کردند، داده ها محافظت می شوند و کاربر باید اقداماتی را برای استفاده از رمزهای عبور قوی و اقدامات احراز هویت اتخاذ کند. محققین تاکید بر مسائل حریم خصوصی و امنیت ابری، کنترل‌های امنیت ابری، الگوریتم های آن مانند AES, MD-5, RSAبا معایب و به این نتیجه رسیدند که رمزگشایی و رمزگذاری نوآورانه در بهبود امنیت در سراسر شبکه باید به کار گرفته شود.

در مقاله [۳۹]، Pallavi Marathe و همکاران. استدلال کردند که، ابر محاسبات از طریق شخص ثالث برون سپاری می شود، بنابراین ذاتاً خطر امنیتی اضافه شده که حفظ امنیت، در دسترس بودن، محرمانه بودن داده ها را دشوارتر می کند و همچنین مانعی برای پذیرش است. رایانش ابری مسائل اوراق بهادار ابری به طور کلی دسته بندی می شوند در دو کلاس مانند مشکلات مربوط به امنیت که توسط ارائه دهندگان خدمات با چالش های ابری و امنیتی که در پایان احساس می شود تجربه می کنند کاربران در این مورد، مشتری اطمینان حاصل می کند که ارائه دهنده به درستی اقدام کرده است اقدامات امنیتی برای محافظت از داده های آنها و ارائه دهنده باید از آن اطمینان حاصل کنند زیرساخت آنها امن است و داده ها و برنامه های مشتریان امن است حفاظت شده. خدمات و فضای ذخیره سازی رایانش ابری به طور گسترده ارائه می شود توسط گوگل و آمازون و VMware نرم افزار را برای ایجاد فراهم می کنند یک ابر خصوصی در کنار مزایای رایانش ابری، خطرات امنیتی ذاتی نیز وجود دارد. با انتقال/حرکت داده های بیشتری از مرکز ذخیره سازی سرور به مکان دیگری در ابر، یعنی احتمال به خطر افتادن داده های خصوصی نیز افزایش می یابد. در این مقاله نویسندگان عمدتاً بر روی تهدیدات اطلاعات از طریق محرمانه بودن، یکپارچگی، در دسترس بودن متمرکز

شده اند و استفاده از برخی ابزارها را پیشنهاد می کنند. موجود در بازار برای کاهش خطرات این تهدیدات مانند Viivo،

SkyCrypt، CipherCloud، Bitglass، Skyhigh در مورد عملکرد، مزایا، معایب آنها توضیح می دهند. آنها به این نتیجه رسیدند که ابزار Skyhigh و Bitglass در رمزگذاری اطلاعات و کشف ابر بهترین هستند استفاده نویسندگان همچنین پیشنهاد می‌کنند که اگر شرکت‌ها قادر به حفظ کنترل و هماهنگی سیاست کلیدهای رمزگذاری باشند، می‌توانند توافق با الزامات نظارتی خارجی و داخلی را تضمین کنند.

در [۴۰]، نویسنده اسمیتا پارته و همکاران. در مورد چگونگی ابر بحث کرده اند محاسبات مزایای فن آوری و مالی جذابی را ارائه می دهد و امکانات ساخت، مدیریت استقرار و طراحی برنامه های کاربردی مستقل آنها از راه دور بدون نیاز به نرم افزار و سخت افزار اضافی. آنها همچنین تأکید می کنند که ملاحظات امنیتی به دلیل اطلاعات محرمانه در فضای ابری، ویژگی‌های اصلی و حیاتی در رایانش ابری باقی می‌مانند. نویسندگان بر حفظ حریم خصوصی، اعتماد تمرکز دارند چالش های امنیتی (کمبود کنترل کاربر، حافظه تایید نشده عمل، انفجار داده ها، تامین پویا، دسترسی، داده های مرزی جریان، چند اجاره، حسابرسی، در دسترس بودن و غیره) مسائل، طبقه بندی امنیت جنبه ها، نگرانی های امنیتی (مدیریت دسترسی، رمزگذاری، مدیریت کلید، و سایر مدیریت خطر)، قطعنامه های موجود مانند فایروال، IDS/IPS، آنتی ویروس ها و غیره که دارندگان سهام، فروشندگان، شرکت ها، سازمان ها باید قبل از پذیرش به نگرانی های امنیتی مربوط به رایانش ابری توجه جدی داشته باشند .سیستم های ابری.

در [۴۱]، نویسندگان پدیده رشد رایانش ابری را همراه با چالش‌های آن مورد بحث قرار می‌دهند و مسائل نیز به سرعت در حال رشد هستند. این این مقاله عمدتاً نمای کلی، معماری، تهدیدات و اقدامات متقابل موجود تهدیدات رایانش ابری را پوشش می‌دهد. انواع حملات امنیتی و تهدیدات در بسیاری از لایه ها سطوح فیزیکیIaaS-، application-virtualPaaS، SaaS، (و همچنین نفوذ آنها مانند اینسایدر، سیل، کاربر به روت، پورت اسکن، مجازی سازی، کانال درب پشتی(DDoS) ، تخصیص فضای ذخیره سازی، مجوز و احراز هویت و اصلاح داده ها توسط نویسندگان.

عوامل خطر زیر برای ارزیابی شناسایی می شوند:

i احراز هویت و کنترل دسترسی (AC&A)

ii بررسی کافی ناکافی (IDD)

iii از دست دادن داده (DL)

برنامه ریزی کاربردی ناامن (IAP)

برنامه ریزی کاربردی ناامن (IAP)

vi تداوم کسب و کار و در دسترس بودن خدمات (SA & BC)

vii محیط مشترک (ShE)

viii انطباق با مقررات (RC)

ix نقض داده ها (DB)

x مکان داده و پشتیبانی تحقیقاتی (IS&DL)

xi مدیریت بخش سوم (TPM)

xii تفکیک داده ها (DS)

xiiiبازیابی(R)

xiv یکپارچگی داده (DI)

آسیب پذیری های مجازی سازی (VV) xv

xvi Resource Exhaustion (RE)

xvii قرارداد سطح خدمات (SLA)

xviii قابلیت همکاری و حمل و نقل (P&I)

۳. روش

این مرحله سطوح ریسک برآورد شده را با معیار پذیرش ریسک، که آستانه ای است که توسط مدیران کسب و کار تعیین می شود، مقایسه می کند.

هدف این کار ارائه ابزاری روش شناختی برای ارزیابی ریسک در محیط رایانش ابری که هم قابل اعتماد و هم موثر است. رویکرد مدل‌سازی ارزیابی ریسک هوشمند پیشنهادی با استفاده از مدل ML در سه فاز اجرا می‌شود شکل ۱.

اهداف تحقیق دقیق زیر به منظور تعیین شد رسیدن به این هدف:

۱- ارزیابی و شناسایی مجموعه اطلاعات در مورد مسائل ریسک

مربوط به رایانش ابری

۲- برای اجرای شبیه سازی مجموعه داده با استفاده از ریسک از قبل تعیین شده

متغیرها

۳-استفاده از تکنیک های یادگیری ماشین برای ایجاد یک مدل ارزیابی ریسک امکان پذیر برای محیط های رایانش ابری. نویسندگان در [41]برخی از مسائل ذکر شده باید در هنگام انتخاب مورد توجه قرار گیرد مناسب ترین تکنیک ارزیابی:

- در دسترس بودن منابع برای تجزیه و تحلیل.
- پیچیدگی و اندازه فرآیندی که تجزیه و تحلیل می شود.
- مرحله ای که در آن ارزیابی خطر در فرآیند بررسی خواهد شد چرخه زندگی.
- در دسترس بودن اطلاعات.

مدل پیش‌بینی زیر برای ساخت مدل برای ارزیابی عملکرد از طریق تکنیک‌های هوش مصنوعی و الگوریتم‌های رگرسیون خطی (یادگیری ماشینی) همانطور که در شکل ۲ نشان داده شده است استفاده می‌شود:

مرحله ۱: ارزیابی ادبیات رایانش ابری انجام شد، و عوامل خطر مرتبط کشف شد. مشکلاتی که کشف شد همان عامل خطر تعریف شده توسط بسیاری از مطالعات بود، اما آنها آن را با نام های مختلف درج کرده بودند. مطالعات دیگر

متغیرهای ریسک را تعریف کردند، اگرچه ممکن است آنها را با اصطلاح دیگری ادغام و طبقه بندی کنید. در نتیجه ۱۸ عامل خطر برای این اختلالات کشف شده است. هدف پروژه شناسایی حیاتی ترین متغیرهای ریسک که می توانند بر ابر تأثیر بگذارند پذیرش محاسبات، و همچنین ارزیابی اینکه کدام عناصر دارای a تأثیر قابل توجهی بر اهداف سازمان دارد، به طوری که آنها را می توان گنجاند و به عوامل خطر شناسایی شده اضافه کرد .همه ۱۸ عامل خطر به عنوان متغیرهای ورودی به منظور ایجاد استفاده می شود یک مجموعه داده با تنها یک خروجی، که ریسک تخمینی است. هر یک سپس متغیر به چهار دسته تقسیم می شود: کم، متوسط، زیاد، و فوق العاده بالا سپس از یکی از داده های اندازه گیری استفاده می کند روش هایی که به عنوان مقیاس فاصله ای برای تخصیص مقادیر عددی به هر یک شناخته می شوند متغیر؛ هر متغیر یک مقدار محدوده عددی دارد.

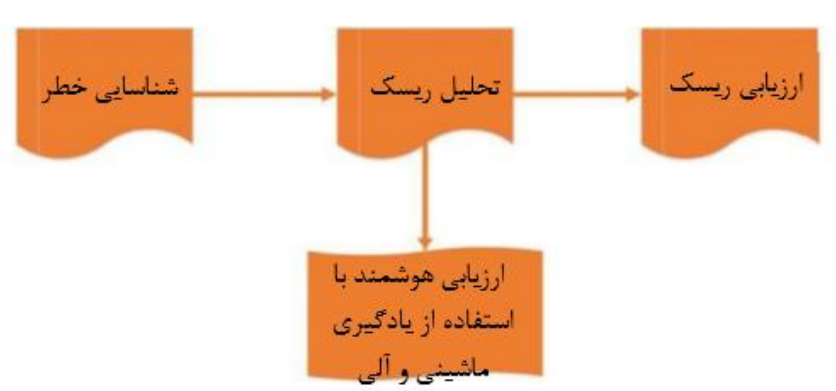
مرحله ۲: پس از آماده سازی مجموعه داده ها، لازم است که به حداقل برسد ابعاد داده، که به الگوریتم تجزیه و تحلیل داده اجازه می دهد تا اجرا سریعتر و کارآمدتر با استفاده از روش های انتخاب ویژگی است که در این مطالعه این کار با به کمک ابزار WEKA / orange که یک پیاده سازی تکنیک انتخاب ویژگی پیشنهادی است. بهترین اول، جستجوی تصادفی و رتبه بندی همیشه از روش های انتخاب ویژگی استفاده می شد.

مرحله ۳: پس از آماده‌سازی مجموعه داده، لازم است ابعاد داده‌ها به حداقل برسد، که به الگوریتم تجزیه و تحلیل داده‌ها اجازه می‌دهد تا سریع‌تر و کارآمدتر اجرا شود. روش های مورد سوال این الگوریتم ها به خوبی شناخته شده اند و زمینه تجزیه و تحلیل داده ها را نشان داده و در عمل موثر واقع شده است. این الگوریتم ها با سفارشی سازی مناسب از ابزار WEKA / orange استفاده می شوند. بر اساس تکنیک استاندارد بالا به پایین، درختان تصمیم گیری بسیار تصادفی یا درخت اضافی مجموعه ای از درختان تصمیم یا رگرسیون هرس نشده را می سازد. داده ها به طور کامل یا جزئی به طور تصادفی تقسیم می شوند.

درخت اضافی با القای درخت تصمیم موجود متفاوت است که تکنیک ها را به دو صورت انجام می دهد: گره ها را با انتخاب نقاط برش جدا می کند کاملاً تصادفی است و درختان را با استفاده از کل یادگیری رشد می دهد نمونه. متریک

فاصله آنتروپی در K*، یک روش یادگیری مبتنی بر نمونه، برای کمی کردن فاصله بین دو نمونه استفاده می‌شود. متریک فاصله آنتروپی دارای مزایای مختلفی است، از جمله روشی یکنواخت برای پرداختن به نمادهای با ارزش واقعی، و ویژگی های با ارزش از دست رفته. معمولاً برای اجرای یک طبقه‌بندی دلخواه روی داده‌هایی که از طریق یک دسته‌بندی دلخواه ارسال شده‌اند استفاده می‌شود فیلتر در مورد طبقه بندی فیلتر تصادفی. ساختار فیلتر، مانند ساختار طبقه‌بندی کننده، صرفاً به آن وابسته است داده های آموزشی و نمونه های آزمایشی توسط فیلتر مدیریت می شود بدون هیچ تغییری در ساختار آنها.

مرحله ۴: مجموعه گروهی از ماشین های یادگیری است که قضاوت آنها برای بهبود عملکرد کلی سیستم ترکیب می شود .پس از اعمال روش های یادگیری ماشینی، دو مجموعه داده را با هم ترکیب می کند آنها را برای ساخت مدل مجموعه. در آزمایشات، مدل گروه با استفاده از تکنیک رأی ساخته شده است. الگوریتم رأی نوعی از الگوریتم پیش بینی که بسیاری از پیش بینی ها را ترکیب می کند. برای رگرسیون، چندین ترکیب از تخمین های احتمال ممکن است .هر پیش‌بینی در روند رای‌گیری یک رای می‌گیرد و اکثریت برنده می‌شوند. به عنوان یک قانون ترکیبی، الگوریتم رأی با استفاده از رویکرد میانگین احتمال پیاده‌سازی می‌شود. دستگاه تکنیک های یادگیری مورد استفاده برای ارزیابی ریسک ابری به شرح زیر است:



شکل ۱. رویکرد مدلسازی ارزیابی ریسک هوشمند.

شکل 2. روش مورد استفاده برای ساخت مدل پیش بینی پیشنهادی.

) درختان تصمیم

برای طبقه‌بندی‌کننده نظارت‌شده، تکنیک‌های مجموعه‌ای مبتنی بر درخت است .تصمیم-درختان به فرآیند تصادفی سازی، قوانین تقسیم بستگی دارد به طور دلخواه در هر عنصر درخت فشار داده می شوند و به انتخاب شده بستگی دارد یکی از این رهنمودهایی که باید با آن گره مرتبط شود، بهترین عمل است در ارزیابی محاسباتی امتیازدهی چنین روش هایی به بهبود کمک می کند سرعت تمرین، همبستگی خسته کننده بین درختان تصمیم القایی، و کاهش عوارض با روش های القایی.

) طبقه بندی فیلتر تصادفی

برای اجرای یک طبقه بندی کننده تصادفی بر روی اطلاعاتی که دارد استفاده می شود از طریق یک فیلتر دلخواه منتقل شده است. مشابه طبقه‌بندی‌کننده، ساختار فیلتر منحصراً به نمونه‌های آزمایشی و اطلاعات آموزشی وابسته است که بدون تغییر ساختار اصلی آنها توسط فیلتر اجرا می شود

K نزدیکترین همسایگان (k-NN یا K*)

این الگوریتم، معروف به k-NN، یادگیری وابسته به نمونه است که کل نمونه آموزشی نگهداری می شود و هیچ مدلی ایجاد نمی شود تا زمانی که یک نمونه جدید مورد نیاز است که گروه بندی شود، و آنها از تعداد کمی از توابع فاصله خاص دامنه برای بازیابی یکسان ترین استفاده می کنند

نمونه ای از مجموعه ای از نمونه های آموزشی. ادغام روش‌های یادگیری ماشین بالا همراه با سیستم ارزیابی ریسک تطبیقی یکنواخت با استفاده از تکنیک هوش مصنوعی انجام می‌شود. نتیجه این هوش مصنوعی سیستم پیشنهادی را با قابلیت‌های تطبیقی با کمک پیش‌بینی و کاهش تهدید در حال تکامل هستند. برخی از شاخص های عملکرد مرسوم در این تحقیق برای ارزیابی اثربخشی رویکردهای حاصل استفاده شده است. ابتدا از دو معیار آماری برای حل این مشکل استفاده کرد ضریب همبستگی (R) و دوم ریشه میانگین مربعات خطا است

(RSME) [۴۶،۴۷،۴۸،۴۹] همانطور که در معادلات نشان داده شده است. (۱) و (۲):

$$R = \sqrt{1 - \frac{\sum_1^n (Pi - Ai)^2}{\sum_1^n Ai^2}} \qquad (1)$$

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N} (Pi - Ai)^2} \qquad (2)$$

مقادیر خروجی واقعی (مطلوب) و برازش (پیش بینی شده) نشان داده شده است به ترتیب توسط Pi و .Ai در نتیجه، مقدار یک را انتظار دارد یا نزدیک به یک از معیارهای ضریب همبستگی (CC) که است ارزیابی با استفاده از معادله

(۱) و مقادیر کم از مربع میانگین ریشه معیارهای خطا (RMSE) به عنوان نتیجه نهایی که با استفاده از معادله ارزیابی می شود.(2) .

۴. نتیجه و بحث

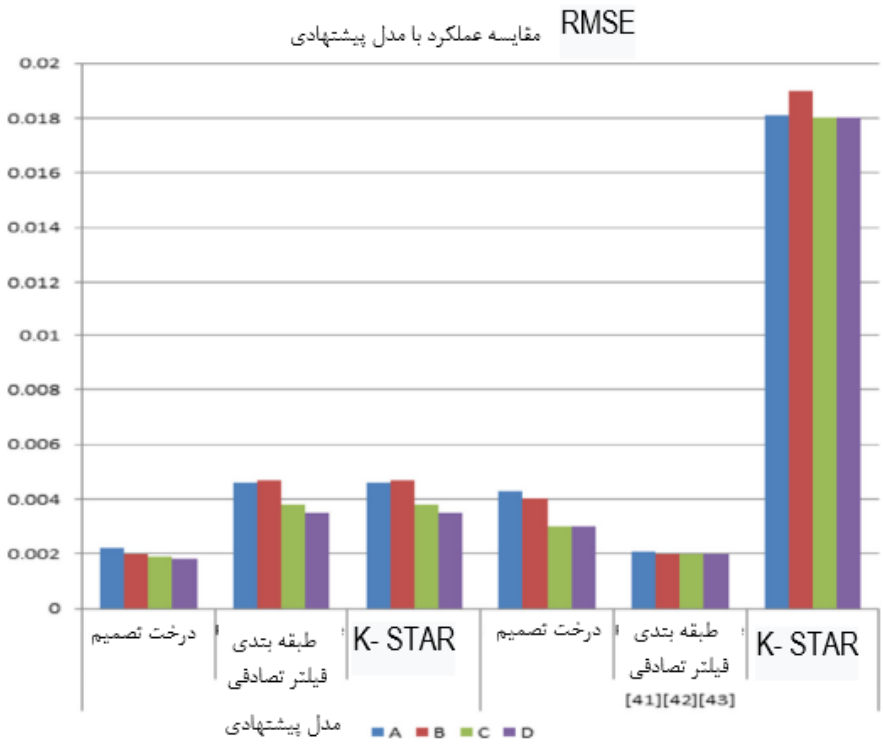
برای نهایی کردن عوامل خطر یک بررسی انجام شد. در این مورد سوال می کند

داوطلبان برای طبقه بندی عوامل خطر در سه لایه مجزا بر اساس احتمال وقوع و تأثیر آنها بر CC. موارد زیر هستند نتایج این کلاس‌ها: اصطلاحات «مهم نیست»، «مهم» و «خنثی» به جای یکدیگر استفاده می‌شوند. از کشورهای مختلف ۳۵ بین المللی کارشناسان در این نظرسنجی پاسخ دادند و هر کدام آن را تایید کردند عواملی که قبلا تجویز شده بودند قابل توجه هستند، به این معنی که آنها یک اهرم زیادی در دنیای رایانش ابری. بعدا عدد داد طیف وسیعی از مقادیر برای هر عامل خطر، و در نهایت، پروتکل ها و قوانین خبره را ایجاد کرد و از این رو از برخی تکنیک های آماری برای تولید اطلاعات بسته به آن قوانین استفاده کرد. ۱۸ ویژگی ورودی شامل شد

توسط مجموعه داده و شامل حدود ۱۹۴۰ نمونه است. برچسب گذاری ۱۸ ویژگی با محدوده مربوط به آنها برای مقادیر عددی، عوامل خطر هستند در جدول ۱ ارائه شده است. از طریق تقسیم درصد برای ارزیابی اعمال شد

و الگوریتم تست از طریق تقسیم درصد، مجموعه داده به صورت دلخواه است تقسیم اطلاعات تست و آموزش که به شرح زیر است:

- 50–50% (A)
- 65–35% (B)
- 85–15% (C)



شکل ۳. مقایسه عملکرد RMSE برای همه آزمون ها مجموعه داده ها با مدل پیشتهادی

جدول ۱ مقادیر محدوده مرتبط با ریسک مربوطه عوامل

عامل خطر	مقدار محدوده
RC, I & P, IAS, DS	0-1
TPM, RE, DB, DI	0-2
DT,DL, DL & IS, SLA, A & AC	0-3
IDD, BC & SA, R, ShE, VV	1-3

جدول ۲ مقایسه عملکرد RMSE مدل پیشنهادی با مدل های دیگر با استفاده از هر چهار کلاس های مجموعه داده

الگوریتم		A	B	C	D
پیشنهاد شده مدل	درخت تصمیم	**0.0022**	**0.002**	**0.0019**	**0.0018**
	فیلتر تصادفی	0.0046	0.0047	0.0038	0.0035
	طبقه بندی				
	k-star	0.0046	0.0047	0.0038	0.0035
[50]	درخت تصمیم	0.0043	0.004	0.003	0.003
[51]	فیلتر تصادفی	0.0021	**0.002**	0.002	0.002
[52]	طبقه بندی				
	k-star	0.0181	0.019	0.018	**0.018**
[53]	K-mean	0.022			
[54]	SVM	0.1152			

• 95–5% (D)

آزمایش‌ها در WEKA اجرا شدند که مجموعه‌ای از ابزارهای پیش پردازش داده ها و الگوریتم های یادگیری ماشین در یک دامنه GUI برای ارزیابی الگوریتم و کاوش اطلاعات همانطور که در نشان داده شده است

میز ۱:

با هر الگوریتم، جدول ۲ بهترین نتایج آزمون (RMSE) را خلاصه می کند .از همه درصد داده ها و مقایسه عملکرد RMSEمدل پیشنهادی با مدل دیگر:[50-54]

بهترین عملکرد از نظر پارامتر RSME برجسته شده است در هر ستون از جدول ۲. در k-mean [44،45] برای ارزیابی استفاده می شود عملکرد سیستم در حالی که SVM برای ارزیابی عملکرد سیستم استفاده می شود. مقایسه عملکرد RMSE بین مدل پیشنهادی با [۴۱-۴۳] در شکل ۳ برای درصد کل مجموعه داده نشان داده شده است و آن درصد داده های آموزشی اضافی را در حدود نشان می دهد .(۵٪ تست و ۹۵٪ آموزش) بهترین نتایج را ایجاد می کند که به معنای یادگیری بهتر است. از نتایج، مشخص است که عملکرد RSME مدل پیش بینی پیشنهادی در مورد درخت تصمیم و k* بهتر است الگوریتمی که در صورت طبقه‌بندی فیلتر تصادفی قبلی بود بهتر ابتدا روش ها و رویکردهای یادگیری توضیح داده شد و سپس انتخاب ویژگی ها انجام شد. به دنبال آن، چندین رویکرد یادگیری مانند درختان تصمیم، ستاره k و غیره در نظر گرفته شدند. در نهایت، معیارهای اندازه‌گیری عملکرد ارائه شده‌اند که برای ارزیابی مدل‌های پیش‌بینی استفاده می‌شوند.

۵. نتیجه گیری

با افزایش استفاده از داده ها به مرور زمان، سیستم های سیستم های کلان داده به یکی از محرک های مهم نوآوری تبدیل شدند که مسیری را ارائه می دهند .در مدیریت اطلاعات دامنه ابری به طور گسترده کلان داده ها را با ارائه دامنه های اصلاح شده به سیستم های کلان داده ها تنظیم می کند. در حالی که کلان داده ها در رایانش ابری سیستم های قوی و قدرتمندی هستند که هر دو این امکان را فراهم می کنند، تحقیقات بیشتر برای توسعه و افزایش و شرکت وجود دارد و گمانه‌زنی‌های کمی در رابطه با ارزیابی ریسک بعد از بحث و بررسی واقعی وجود دارد. کار سخت اضافی برای طراحی و توسعه مکانیزم ارزیابی ریسک استفاده شده است که به امنیت در حوزه رایانش ابری برای کلان داده ها می پردازد. اما به سرعت برای حل امنیت ارزیابی ریسک اجرا شود که مسائل هدف اصلی این سختی تجربی دستیابی به کاهش است؛ بهترین دقت در مجموعه داده های آزمایش و یافتن بهترین ها طرح های موجود برای این مجموعه داده استفاده می شود. بررسی می شود که رفتار الگوریتم های مختلف یادگیری ماشینی برای نشان دادن عامل خطر مربوط به رایانش ابری است. تاثیر زیر مجموعه های تست و آموزش از اطلاعات در این مقاله با تقسیم دلخواه زیر مجموعه داده ها در چهار کلاس مختلف توضیح داده شده است. نتیجه تجربی آن شکاف را به تصویر می کشد که مجموعه داده تا (۹۵٪ - ۵٪) بهترین بازده را از کل باقیمانده ارائه می دهد و پارتیشن بندی و همچنین الگوریتم Decision Tree Classifierرا نشان می دهد. *k نتایج بهتری را بین تمام مجموعه‌های داده در حوزه رایانش ابری ارائه می‌دهد، در حالی که طبقه‌بندی‌کننده فیلتر تصادفی ساز کمی نسبت به قبلی داشت.

مطالعات آینده: از آنجا که امنیت اولویت اصلی در محیط رایانش ابری است، چارچوب امنیتی هم به مشتریان ابر و هم به ارائه دهندگان خدمات ابری در مورد مرزهای فردی و مسئولیت های مشترک در هر سطح ارائه می شود. بازیگران ابر می‌توانند پارامترهای امنیتی و انطباق را با شبیه‌سازی چارچوب امنیتی رایانش ابری در محیط‌های ابری داخلی یا خارجی خود ارزیابی کنند. در نتیجه، به عنوان یک پروژه آتی، مایل به انجام تحقیق در مورد آن است تا تجزیه و تحلیل

مقایسه ای عملکرد ارزیابی امنیت هوشمند مدل ها یا چارچوب ها از طریق شبیه سازی و ادغام امنیت استانداردها و دستورالعمل ها برای مدل های خدمات و تحویل انجام شود به آن که کمک خواهد کرد.

در معیارهای چارچوب تحقیقات تکمیلی در حال انجام است موضوع ادغام قراردادهای سطح سرویس ابری (SLA) با چارچوب های امنیتی تطبیقی و هوشمند، که به بسیاری از CSP ها کمک می کند سطح خدمات مورد نیاز مشتریان خود را تضمین می کند. در آینده، نیاز صنعتی به ارزیابی ریسک بلادرنگ نیز ممکن است به این پذیرش دامن بزند که از تکنیک های یادگیری ماشینی حرکت رو به جلو، رویه هایی برای تأیید اعتبار توسط نهادهای نظارتی مختلف ایمنی استفاده از یادگیری ماشین در ارزیابی ریسک نیز باید مورد توجه قرار گیرد.

References

[1] H. Guo, L. Wang, F. Chen, D. Liang, Scientific big data and digital earth, Chin. Sci. Bull. 59 (35) (2014) 5066–5073.
[2] M.G. Porcedda, Patching the patchwork: appraising the EU regulatory framework on cyber security breaches, Comput. Law Secur. Rev. 34 (5) (2018) 1077–1098.
[3] P. Subramani, P. BD, Prediction of muscular paralysis disease based on hybrid feature extraction with machine learning technique for COVID-19 and post-COVID-19 patients, Pers. Ubiquit. Comput. (2021) 1–14.
[4] Rajkumar Buyya, Rajiv Ranjan, Rodrigo N. Calheiros, Modeling and simulation of scalable Cloud computing environments and the CloudSim toolkit: Challenges and opportunities, in: 2009 international conference on high performance computing & simulation, IEEE, 2009, pp. 1–11.
[5] D.N. Tran, T.N. Nguyen, P.C.P. Khanh, D.T. Trana, An iot-based design using accelerometers in animal behavior recognition systems, IEEE Sensors J. (2021).
[6] Michael Miller, Cloud computing: Web-based applications that change the way you work and collaborate online, Que publishing, 2008.
[7] K. Yu, L. Lin, M. Alazab, L. Tan, B. Gu, Deep learning-based traffic safety solution for a mixture of autonomous and manual vehicles in a 5G-enabled intelligent transportation system, IEEE Trans. Intell. Transp. Syst. 22 (7) (2020) 4337–4347.
[8] Laxmana Rao Battula, Network security function virtualization (nsfv) towards cloud computing with nfv over openflow infrastructure: Challenges and novel approaches, in: 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE, 2014, pp. 1622–1628.
[9] B.D. Parameshachari, Big data analytics on weather data: predictive analysis using multi node cluster architecture, Int. J. Comput. Appl. (2022) 0975–8887.
[10] Abhishek Sharma, Umesh Kumar Singh Dr., Cloud Computing Security Framework Based on Shared responsibility Model, “Cyber-Physical, IoT, and Autonomous Systems in Industry 4.0” (December) (2021) 39–56 ISBN: 9780367705152 3. In this issue, doi:10.1201/9781003146711-3.
[11] N.T. Le, J.W. Wang, D.H. Le, C.C. Wang, T.N. Nguyen, Fingerprint enhancement based on tensor of wavelet subbands for classification, IEEE Access 8 (2020) 6602–6615.
[12] Anurag Jain, Rajneesh Kumar, A taxonomy of cloud computing, Int. J. Scient. Res. Publ. 4 (7) (2014) 1–5.

[13] Z. Guo, Y. Shen, A.K. Bashir, M. Imran, N. Kumar, D. Zhang, K. Yu, Robust spammer detection using collaborative neural network in Internet-of-Things applications, IEEE Internet Things J. 8 (12) (2020) 9549–9558.
[14] Laura. Savu, Cloud computing: Deployment models, delivery models, risks and research challenges, in: 2011 International Conference on Computer and Management (CAMAN), IEEE, 2011, pp. 1–4.
[15] B. Rachana, T. Priyanka, K.N. Sahana, T.R. Supritha, B.D. Parameshachari, R. Sunitha, Detection of polycystic ovarian syndrome using follicle recognition technique, Global Trans. Proc. 2 (2) (2021) 304–308.
[16] Archana Mantri, Suman Nandi, Gaurav Kumar, Sandeep Kumar, High performance architecture and grid computing, International Conference, HPAGC, 2011.
[17] D.L. Vu, T.K. Nguyen, T.V. Nguyen, T.N. Nguyen, F. Massacci, P.H. Phung, HIT4Mal: Hybrid image transformation for malware classification, Trans. Emerg. Telecommun. Technol. 31 (11) (2020) e3789.
[18] edited by Mainak Adhikari, Aditi Das, Akash Mukherjee, Utility Computing and Its Utilization, in: Ganesh Chandra Deka, G.M. Siddesh, K.G. Srinivasa, L.M. Patnaik (Eds.), In Emerging Research Surrounding Power Consumption and Performance Issues in Utility Computing, IGI Global, Hershey, PA, 2016, pp. 1–21, doi:10.4018/978-1-4666-8853-7.ch001.
[19] L. Tan, K. Yu, F. Ming, X. Chen, G. Srivastava, Secure and resilient artificial intelligence of things: a HoneyNet approach for threat detection and situational awareness, IEEE Consumer Electronics Magazine, 2021.
[20] Daniel Beimborn, Thomas Miletzki, Stefan Wenzel, Platform as a service (PaaS), Bus. Inf. Syst. Eng. 3 (6) (2011) 381–384.
[21] Wesam Dawoud, Ibrahim Takouna, Christoph Meinel, Infrastructure as a service security: Challenges and solutions, in: 2010 the 7th International Conference on Informatics and Systems (INFOS), IEEE, 2010, pp. 1–8.
[22] Jong-Hei. Ra, Qualitative study on service features for cloud computing, J. Digit. Contents Soc. 12 (3) (2011) 319–327.
[23] Subashini Subashini, Veeraruna Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (1) (2011) 1–11.
[24] Umer A. Butt, Muhammad Mehmood, Syed B.H. Shah, Rashid Amin, M.W. Shaukat, Syed M. Raza, Doug Y. Suh, Md.J. Piran, A review of machine learning algorithms for cloud computing security, Electronics 9 (9) (2020) 1379 9091379, doi:10.3390/electronics.
[25] Raj Samani, Jim Reavis, Brian Honan, CSA guide to cloud computing: Implementing cloud privacy and security, Syngress, 2014.
[26] Abhishek Sharma, & Dr, Umesh Kumar Singh, Deployment model of e-educational cloud for departmental academics automation using open source, HTL J. 27 (5) (2021) 36 ISSN 1006-6748, doi:10.37896/HTL27.5/3535.
[27] Dan Hubbard, Michael Sutton, Top threats to cloud computing v1. 0, Cloud Secur. Alliance (2010) 1–14.
[28] Abhishek Sharma, Umesh Kumar Singh, et al., An Investigation of Security Risk & Taxonomy of Cloud Computing Environment, IEEE 2ndInternational conference on Smart Electronics and Communication (ICOSEC 2021), 2022 ISBN: 978-1-6654-3368-6.
[29] Abhishek Sharma, Umesh Kumar Singh, et al., A Comparative analysis of security issues & vulnerabilities of leading Cloud Service Providers and in-house University Cloud platform for hosting E-Educational applications, IEEE Mysore Sub Section International Conference (MysuruCon), 2021 ISBN: 978-0-7381-4662-1.
[30] R.A. Attar, J. Al-Nemri, A. Homsi, A. Qusef, Risk Assessment for Emerging Domains (IoT, Cloud Computing, and AI), in: 2021 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), 2021, pp. 120–127, doi:10.1109/JEEIT53412.2021.9634156.
[31] M. Zekri, S.E. Kafhali, N. Aboutabit, Y. Saadi, DDoS attack detection using machine learning techniques in cloud computing environments, in: 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), 2017, pp. 1–7, doi:10.1109/CloudTech.2017.8284731.

[32] K.K. Nguyen, D.T. Hoang, D. Niyato, P. Wang, D. Nguyen, E. Dutkiewicz, Cyberattack detection in mobile cloud computing: A deep learning approach, in: 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018, pp. 1– 6, doi:10.1109/WCNC.2018.8376973.
[33] Song-Shun Lin, Shui-Long Shen, Annan Zhou, Ye-Shuang Xu, Risk assessment and management of excavation system based on fuzzy set theory and machine learning methods, Autom. Constr. 122 (2021) 103490 ISSN 0926-5805, doi:10.1016/j.autcon.2020.103490.
[34] Jeevith Hegde, Børge Rokseth, Applications of machine learning methods for engineering risk assessment – A review, Saf. Sci. 122 (2020) 104492 ISSN 0925-7535, doi:10.1016/j.ssci.2019.09.015.
[35] P. Radanliev, D. De Roure, K. Page, et al., Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments – cyber risk in the colonisation of Mars, Saf. Extreme Environ. 2 (2020) 219–230, doi:10.1007/s42797-021-00025-1.
[36] R Vinayakumar, M Alazab, KP Soman, P Poornachandran, A Al-Nemrat, S Venkatraman, Deep learning approach for intelligent intrusion detection system, IEEE Access 7 (2019) 41525–41550, doi:10.1109/ACCESS.2019.2895334.
[37] AA Diro, N Chilamkurti, Distributed attack detection scheme using deep learning approach for Internet of Things, Futur. Gener. Comput. Syst. 82 (2018) 761–768, doi:10.1016/j.future.2017.08.043.
[38] D Berman, A Buczak, J Chavis, C Corbett, A survey of deep learning methods for cyber security, Information 10 (4) (2019) 122, doi:10.3390/info10040122.
[39] D. Sun, Z. Wu, Y. Wang, Q. Lv, B. Hu, Risk prediction for imbalanced data in cyber security: a Siamese network-based deep learning classification framework, in: Proceedings of the international joint conference on neural networks, 2019-July, 1–8, 2019, doi:10.1109/IJCNN.2019.8852030.
[40] Rohit Bhadauria, NabenduChaki RituparnaChaki, Sugata Sanyal, A survey on security issues in cloud computing, arXiv preprint arXiv:1109.5388 (2011) 1–15.
[41] Mohammad Masdari, Marzie Jalali, A survey and taxonomy of DoS attacks in cloud computing, Secur. Commun. Netw. 9 (16) (2016) 3724–3751.
[42] Harshit Srivastava, SathishAlampalayam Kumar, Control framework for secure cloud computing, J. Inf. Secur. 6 (01) (2014) 12.
[43] Amit Wadhwa Varsha, Swati Gupta, Study of security issues in cloud computing, Int. J. Comput. Sci. Mob. Comput. 4 (6) (2015) 230–234 ISSN 2320-088X, IJCSMCpg..
[44] Khalid H. Alotaibi, Threat in Cloud-denial of service (DoS) and distributed denial of service (DDoS) attack, and security measures, J. Emerg. Trends Comput. Inf. Sci. 6 (5) (2015) 241–244.
[45] Atulay Mahajan, Sangeeta Sharma, The malicious insiders threat in the cloud, Int. J. Eng. Res. Gen. Sci. 3 (2) (2015) 245–256.
[46] K. Vijayakumar, Security issues and algorithms in cloud computing, Global J. Adv. Res. 2 (3) (2022) 569–574.
[47] Pallavi Marathe, Cloud Computing Security threats and tools, 4, 2015 ISSN-2319—8354(E).
[48] Smita Parte, Noumita Dehariya, Cloud computing: issues regarding security, applications and mobile cloud computing, Int. J. Advanc. Res. Comp. Sci. Softw. Eng 5 (3) (2015) 403–406.
[49] ShaikKhaja Mohiddin, Suresh BabuYalavarthi, Research challenges in the emerging trends of cloud computing, Int. J. Adv. Comput. Sci. Technol. (IJACST) 4 (1) (2015) 4.
[50] Nada Ahmed Mohammednour Eisa, PhD diss, Sudan University of Science and Technology, 2016.
[51] M. Hall, et al., The WEKA data mining software: an update, ACM SIGKDD Explor. Newslett. 11 (1) (2009) 10–18.
[52] I.H. Witten, et al., Weka: Practical machine learning tools and techniques with Java implementations, 1999.

[53] Zhe Mi, Tiangang Wang, Zan Sun, Rajeev Kumar, Vibration signal diagnosis and analysis of rotating machine by utilizing cloud computing, Nonlinear Eng. 10 (1) (2021) 404–413, doi:10.1515/nleng-2021-0032.
[54] Priyanka Nehra, A. Nagaraju, Host utilization prediction using hybrid kernel based support vector regression in cloud data centers, J. King Saud Univ. - Comput. Inf. Sci. (2021) 1319–1578, doi:10.1016/j.jksuci.2021.04.011.