دوفصلنامه محاسبات و سامانه های توزیع شده
سال ششم، شماره ۱، شماره پیاپی ۱۱، صفحه ۱۳۷ تا ۱۵۳، سال ۱۴۰۲

امنیت رایانش ابری:
مروری بر مفاهیم پایه‌ای، چالش‌های امنیتی ، مسائل ، الزامات، استانداردهای امنیتی و انواع حملات در رایانش ابری

حمید زنگی آبادی زاده[۱]، مهدی قاسمی[۲]، فرشید وظیفه دوست[۳]، سمیه کدخدا ده‌خانی[۴] و مائده رحمانی[۵]

[۱]دانشجوی مقطع کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز ،دانشگاه پیام نور مرکز بین الملل کیش
Hamid.zangiabadi@gmail.com

[۲] دانشجوی مقطع کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز ،دانشگاه پیام نور مرکز بین الملل کیش
Mahdikmg1@gmail.com

[۳] فارغ التحصیل مقطع کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز از دانشگاه پیام نور مرکز بین الملل قشم
Vazifehdoostfarshid@gmail.com

سمیه کدخدا ده خانی

[۴]فارغ التحصیل مقطع کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز از دانشگاه پیام نور مرکز بین الملل قشم
Emailsk65@gmail.com

[۵]دانشجوی مقطع کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار ،دانشگاه پیام نور مرکز بین الملل کیش
Maede9708@gmail.com

چکیده

رایانش ابری یک الگوی محاسباتی است که می‌تواند منابع مجازی پویا و مقیاس‌پذیر را از طریق سرویس اینترنت در اختیار کاربران درخواستی قرار دهد و همچنین توسعه یافته محاسبات توزیع‌شده، محاسبات موازی و محاسبات شبکه‌ای است. یکی از پرچالش ترین ویژگی‌های رایانش ابری امنیت است و داده‌ها در دستگاه‌های ذخیره‌سازی ذخیره می‌شوند که توسط هیچ شخص دیگری قابل هک یا استفاده نیستند. این فناوری دارای سرویس ذخیره‌سازی سریع و قابل اعتماد است، البته به شرطی که همه تدابیر امنیتی از ابتدا درست برای آن فراهم شود. در واقع امنیت در این محیط بسیار حیاتی است علاوه بر این، به دلیل سطح شفافیت نامشخص امنیت ابری توسط بسیاری از ارائه دهندگان خدمات ابری، امنیت یک نگرانی قابل توجه برای سازمان‌ها است. سازمان‌هایی که به فکر انتقال خدمات فناوری اطلاعات خود به فضای ابری هستند، نسبت به چندین ناحیه در ابر اطمینان ندارند و انتظار نمی‌رود برخی از این مناطق توسط ارائه‌دهنده روشن شوند. در این مقاله به امنیت رایانش ابری، مسائل / الزامات امنیت ابری، چالش‌های امنیتی رایانش ابری، انواع امنیت رایانش ابری، استانداردهای امنیت رایانش ابری و انواع شبکه و حملات در امنیت رایانش ابری، می‌پردازیم.

کلمات کلیدی: رایانش ابری، امنیت ، محاسبات ابری و حملات.

تاریخچه مقاله:
تاریخ ارسال: ۱۴۰۲/۰۱/۱۵
تاریخ اصلاحات: ۱۴۰۲/۰۵/۳۱
تاریخ پذیرش: ۱۴۰۲/۰۶/۲۲
تاریخ انتشار: ۱۴۰۲/۰۶/۳۰
ایمیل نویسنده مسئول: Hamid.zangiabadi@gmail.com

۱ – مقدمه

ابر رایانه‌هایی که همه کارهای محاسباتی را انجام می دهند، امروزه‌توسط شبکه‌های رایانه‌های کوچک جایگزین شده-اند و هدف از تولید یک شبکه، اشتراک تجهیزات مانند چاپگرها، اسکنرها، پردازنده‌ها و منابع اطلاعاتی است. یکی از مهمترین منابع برای به اشتراک گذاری، پردازنده‌ها هستند که هدف از به اشتراک گذاری پردازنده افزایش توان عملیاتی، محاسبات سریعتر و حل مشکلات پیچیده می‌باشد. به دلیل امکان استفاده از پردازنده مشترک و اهمیت آن، اخیراً بحث‌های جدیدی در فضای محاسبات رایانه‌ای ظاهر شده‌است که "محاسبات توزیع-شده" نامیده می‌شود[۱]. محاسبات ابری جدیدترین فناوری اعلام شده است که در دنیای شبکه راه اندازی شده است و انواع مختلفی از فناوری‌های محاسباتی به شکل محاسبات توزیع شده،، محاسبات خوشه‌ای، محاسبات شبکه‌ای و محاسبات ابر است[۲]. رایانش ابری که به عنوان محاسبات بر اساس تقاضا نیز شناخته می‌شود، نوعی محاسبات مبتنی بر اینترنت است که

منابع پردازش مشترک و داده‌ها را در اختیار رایانه‌ها و سایر دستگاه‌ها بر حسب تقاضا قرار می‌دهد [۳]. تمرکز روی امنیت فضای ابری و حملات تهدید کننده آن، همچنین استفاده از یک سیستم تشخیص نفوذ کارآمد و نحوه جلوگیری از این حملات از مباحث مطرح شده دنیای تکنولوژی امروزی است. با توجه به افزایش حوادث سایبری، طراحی و پیاده سازی سیستم‌های تشخیص نفوذ موثر برای حفاظت از سیستم‌های اطلاعاتی امنیتی نیز امری ضروری می‌باشد[۴].

محققان در امنیت رایانش ابری عمدتاً به مدیریت دسترسی، کنترل‌های احراز هویت در برابر پس‌زمینه هزینه‌ها از نظر مصرف انرژی و ارتباطات در مقابل کارایی توجه دارند، آنها پروتکل‌ها، الگوریتم‌ها و تکنیک‌هایی را توسعه داده‌اند تا این نیازها را متعادل کنند. اغلب این کنترل‌ها معمولاً بسیار پرهزینه، اما کارآمد یا ارزان هستند، اما ممکن است تهدیدات را کاهش ندهند. برخی از رویکردهای امنیتی در ادبیات برای مقابله با نقص‌های امنیتی فعلی فاقد انعطاف‌پذیری در کاهش تهدیدات متعدد بدون تضاد با اهداف امنیت ابری هستند[۵]. مسائل امنیتی پیرامون رایانش ابری، یک فناوری به سرعت در حال توسعه که اکنون برای محاسبات شخصی و تجاری ضروری است. رایانش ابری با وجود مزایای فراوانی مانند مقیاس پذیری، مقرون به صرفه بودن و انعطاف پذیری، خطرات امنیتی جدی را به همراه دارد که نیازمند توجه دقیق است[۶].

رایانش ابری خطرات امنیتی جدی را به همراه دارد. امنیت داده‌ها یا اطمینان از محرمانه بودن، یکپارچگی و در دسترس بودن اطلاعات، نگرانی اصلی است. علاوه بر این، امنیت شبکه برای جلوگیری از حملات سایبری به زیرساخت ابر ضروری است، مسائل امنیتی با وجود قابلیت دسترسی و انعطاف پذیری رایانش ابری مطرح می‌شود. نقض داده‌ها، نشت و دسترسی غیرمجاز به دلیل سهولت دسترسی به منابع از هر مکان، خطرات جدی در چندین لایه ابری ایجاد می‌کند. رایانش ابری با استفاده از انواع روش‌های رمزگذاری داده‌ها، کنترل‌های دقیق دسترسی و مدیریت کلید، امنیت بسیار خوبی را ارائه می‌دهد[۷].

این مقاله دارای دو بخش است که بخش اول به مرور و بررسی مفاهیم پایه ای و چالش های رایانش ابری پرداخته می‌شود و بخش اصلی این مقاله مربوط به امنیت رایانش ابری که شامل مسائل / الزامات امنیت ابری، چالش‌های امنیتی رایانش ابری، انواع امنیت رایانش ابری، استانداردهای امنیت رایانش ابری و انواع شبکه و حملات در امنیت رایانش ابری، و مقایسه **مقایسه مشکلات امنیتی (تهدیدات امنیتی و اقدامات متقابل)** می‌باشد.

۲ – رایانش ابری

توسعه رایانش ابری به طور قابل توجهی نحوه عملکرد بخش فناوری اطلاعات امروز را تغییر داده است. رایانش ابری امکان بررسی خدمات فناوری اطلاعات بهتر با هزینه کمتر و سرمایه‌گذاری کمتر را فراهم می‌کند. محبوبیت نرم‌افزار به عنوان یک سرویس به دلیل تأثیر محاسبات ابری بر نحوه توسعه و تهیه سخت‌افزار فناوری اطلاعات افزایش یافته است. این یک فناوری مبتنی بر اینترنت است که به کاربران امکان می‌دهد هر زمان که بخواهند به داده‌های ذخیره شده در سرور به عنوان یک سرویس دسترسی داشته باشند. مشتریان فقط برای سرویسی که استفاده می‌کنند هزینه می‌پردازند زیرا این یک سرویس پرداختی است. رایانش ابری به عنوان یک مدل محاسباتی است که در آن قابلیت‌های انبوه مقیاس‌پذیر مبتنی بر فناوری اطلاعات به عنوان خدماتی به مشتریان متعدد ارائه می‌شود. استفاده از فناوری رایانه مبتنی بر اینترنت برای انواع خدمات (به عنوان ظرفیت ذخیره‌سازی، قدرت پردازش، برنامه های کاربردی تجاری یا اجزاء) است. این مجموعه‌ای از خدمات فعال شبکه است که خدمات مقیاس‌پذیر، تضمین شده، معمولا سفارشی شده و نسبتاً مقرون به صرفه را به روشی آسان برای استفاده ارائه می دهد. رایانش ابری به عنوان یک رویکرد محاسباتی تعریف می‌شود که در آن قابلیت‌های بسیار مقیاس-پذیر مرتبط با فناوری اطلاعات به عنوان یک سرویس از طریق اینترنت به مصرف کنندگان خارجی مختلف ارائه می شود. این یک الگوی خدمات فناوری اطلاعات است که در آن سخت‌افزار و نرم‌افزار بر حسب تقاضا در سراسر شبکه بدون استفاده از دستگاه یا مکان در اختیار مصرف‌کنندگان قرار می‌گیرد. مؤسسه ملی استانداردها و فناوری، رایانش ابری را به عنوان مدلی برای اجازه دادن همه جا، راحت، یک مجموعه مشترک از منابع محاسباتی سفارشی شده و خدماتی که می‌تواند به سرعت با حداقل کار اداری یا تماس خدماتی عرضه و به کار گرفته شود، تعریف می کند[۸].

رایانش ابری را به دلیل گسترده بودن در کاربرد، نمی‌توان تعریف کلی ارائه داد، بنابراین، تعاریف آن به این

بستگی دارد که برای چه کاربردی استفاده می‌شود. رایانش ابری را می‌توان با نگاه به دو دیدگاه مانند دیدگاه کاربر و سازمان تعریف کرد. بنابراین، از دیدگاه کاربر، رایانش ابری برای دستیابی به خدمات مبتنی بر محاسبات بدون نیاز به شناخت عمیق فناوری اساسی مورد استفاده، بسیار مهم است و برای سازمان خدماتی را برای مصرف کنندگان و نیازهای تجاری با مقیاس نامحدود و بدون محدودیت، کیفیت خدمات متمایز برای تقویت نوآوری و تصمیم گیری سریع ارائه می‌دهد. مفهوم رایانش ابری به سیستمی اشاره دارد که در آن منابع یک مرکز داده با استفاده از فناوری مجازی‌سازی شده به اشتراک گذاشته می‌شود که همچنین می‌تواند خدمات منعطف، درخواستی و فوری را به مشتریان ارائه دهد و به مشتری اجازه دهد با استفاده از روش پرداخت به ازای استفاده پرداخت کند [۹].

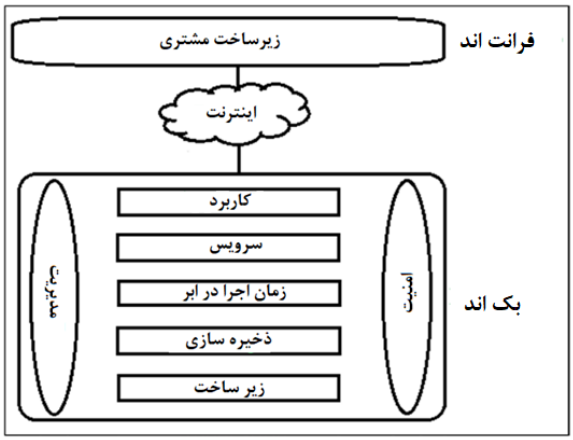
در واقع رایانش ابری به عنوان دسته‌ای از خدمات محاسباتی بر اساس تقاضا که توسط ارائه دهندگان تجاری مانند مایکروسافت و آمازون ارائه می شود، توصیف می‌شود. هدف این اصطلاح ارائه محاسبات، ذخیره‌سازی و نرم‌افزار به عنوان یک سرویس است. هدف رایانش ابری دستیابی به دسترسی مقیاس-پذیر به منابع محاسباتی و خدمات فناوری اطلاعات است. علاوه بر این، رایانش ابری می‌تواند برای ذخیره مقادیر زیادی داده در موضوعات مختلف مانند موسیقی، کتاب های الکترونیکی، پادکست‌ها، برنامه‌ها، ویدئوها و فایل‌ها استفاده شود[۱۰].

۳- تاریخچه و معماری رایانش ابری

رایانش ابری توسط جان مک کارتی در سال ۱۹۶۰ توسعه یافت. طبق گفته پارکهیل نام رایانش ابری در صنعت مخابرات به عنوان یک شبکه خصوصی مجازی معرفی شد. با استفاده از خطوط داده نقطه نقطه، پهنای باند هدر رفت و با استفاده از از شبکه خصوصی مجازی متعادل و سرورها و زیرساخت شبکه گنجانده شد. سپس رایانش ابری به طور گسترده توسط شرکت کنندگان در صنعت مورد استفاده قرار گرفت. آمازون خدمات وب آمازون را معرفی کرد و این کمک بزرگی به کسب و کار آنها کرد. علاوه بر این، گوگل و IBM هر دو تحقیقات رایانش ابری را راه اندازی کرده‌اند. اکالیپتوس اولین پلت فرم منبع باز برای استقرار ابر خصوصی بود[۸]. مطابق شکل ۱، معماری ابر به دو بخش روایت شده است[۱۱]:

فرانت‌اند[1](بخش جلویی): سمت مشتری یک سیستم محاسبات ابری به عنوان قسمت جلویی معماری ابری نامیده می‌شود. یعنی شامل تمام رابطهای کاربری و برنامه‌هایی است که مشتری برای دسترسی به منابع/سرویس‌های رایانش ابری استفاده می‌کند[۱۱]. در واقع مشتری با بخش جلویی تعامل دارد. این شامل رابطهای سمت مشتری و برنامه‌های کاربردی برای تعامل با خدمات رایانش ابری است. سرورهای وب (مانند کروم، فایرفاکس و اینترنت اکسپلورر)، کلاینت‌های باریک و چاق، تبلت‌ها و دستگاه‌های تلفن همراه، همگی بخش جلویی را تشکیل می‌دهند[۱۲].

بک‌اند[2](بخش پشتی): ابری که توسط ارائه‌دهنده خدمات استفاده می‌شود به عنوان Back End نامیده می‌شود. این شامل منابع، کنترل منابع و ارائه روش‌های امنیتی است. همچنین شامل فضای ذخیره‌سازی عظیم، برنامه‌های کاربردی مجازی، رایانه‌های مجازی، تکنیک‌های مدیریت ترافیک، مدل‌های استقرار و غیره است[۱۱]. در واقع ارائه دهنده خدمات از بخش پشتی استفاده می‌کند و بر تمام منابع مورد نیاز برای ارائه سرویس رایانش ابری نظارت دارد. این شامل مقدار زیادی از ذخیره‌سازی داده‌ها، و همچنین اقدامات امنیتی، ماشین‌های مجازی، مدل های استقرار، سرورها و مکانیسم های مدیریت ترافیک و موارد دیگر است[۱۲].



شکل۱:معماری عمومی رایانش ابری[۱۱].

اجزای معماری محاسبات ابری نیز به شرح زیر است[۱۱]:

- زیرساخت مشتری: زیرساخت مشتری جزء قسمت جلویی است .این یک رابط کاربری گرافیکی برای تعامل با ابر ارائه می دهد .

[1] Frontend

[2] Backend

- برنامه: برنامه می تواند هر نرم افزار یا پلتفرمی باشد که مشتری می خواهد از آن استفاده کند .
- سرویس: یک سرویس ابری بر اساس نیازهای مشتری به کدام نوع سرویس دسترسی دارید .
- ابر زمان اجرا[3]: محیط اجرا و زمان اجرا برای ماشین های مجازی توسط ابر زمان اجرا ارائه شده است .
- ذخیره‌سازی: یکی از مهم ترین جنبه های محاسبات ابری، ذخیره سازی است .این مقدار زیادی فضای ذخیره سازی ابری را برای ذخیره و مدیریت داده ها ارائه می دهد .
- زیرساخت: زیرساخت خدمات را در سطوح میزبان، برنامه و شبکه ارائه می‌دهد. سرورها، ذخیره‌سازی، دستگاه های شبکه، نرم‌افزار مجازی‌سازی و سایر منابع ذخیره‌سازی نمونه‌هایی از زیرساخت‌های ابری هستند.
- مدیریت: مدیریت برای مدیریت و هماهنگی اجزای پشتیبان مانند برنامه، سرویس، ابر زمان اجرا، ذخیره سازی، زیرساخت و سایر مسائل امنیتی استفاده می‌شود.
- امنیت: امنیت یک جزء پشتیبان داخلی رایانش ابری است. در قسمت پشتی، مکانیزم امنیتی را پیاده سازی می‌کند

اینترنت: اینترنت کانالی است که قسمت جلویی و انتهایی را به هم متصل می‌کند.

۴- خدمات رایانش ابری

محاسبات ابری شامل ارائه خدمات منتشر شده از طریق وب است که در معماری لایه‌های آن، ارائه دهندگان خدمات ابری به چهار دسته تقسیم می‌شوند:

زیرساخت به‌عنوان یک سرویس: زیرساخت به‌عنوان یک سرویس می‌تواند یک مدل ارائه باشد که طی آن یک شرکت فرآیندهای تعمیر و نگهداری معمولی با ابزار دقیق، متشکل از انبار، سخت‌افزار، سرورها و قطعات شبکه را برون‌سپاری می‌کند. بستر ابر مالک اصلی و مسئول نگهداری، راه‌اندازی و نگهداری داده است. خریدار معمولاً بر اساس هر بار استفاده پرداخت می‌کند. فضای زیرساخت به‌عنوان یک سرویس عموماً دارایی‌های اضافی مانند انتخاب تصویر درایو هارد دیسک ماشین مجازی، ذخیره بلوک داده‌های خام، همراه با ذخیره‌سازی فایل یا شاید سازمانی، متعادل‌کننده‌های بار، شبکه‌های فضای مجازی، فایروال‌ها، آدرس‌های IP و بسته نرم‌افزاری را ذخیره می‌کند. برای اتصال گسترده، مشتریان از وب یا ابرهای حامل (شبکه های مجازی غیرعمومی اختصاصی) استفاده خواهند کرد.

شکل۲: نمایی از خدمات رایانش ابری[۳].

پلتفرم به عنوان سرویس: در مدل‌های پلتفرم به عنوان سرویس، ارائه‌دهندگان ابری یک پلتفرم محاسباتی، معمولاً شامل چارچوب کاری، محیط اجرای گویش برنامه‌نویسی، پایگاه داده و وب سرور را منتقل می‌کنند.یعنی پلتفرم نرم‌افزاری همراه با زیرساخت‌های سخت‌افزاری مورد نیاز برای اجرای آن به صورت ابری در اختیار کسب و کارها و برنامه‌نویسان قرار میگیرد تا بتوانند در کمترین زمان ممکن از ظرفیت‌های رایانش ابری برای دستیابی به اهداف خود استفاده کنند

نرم‌افزار به‌عنوان سرویس: در مدل کسب‌وکار با استفاده از نرم‌افزار به‌عنوان سرویس، تامین کنندگان ابر با پایه و مراحلی که برنامه‌ها را اجرا می کنند سروکار دارند. نرم‌افزار به‌عنوان سرویس در حال حاضر و بارها به عنوان "برنامه نویسی بر حسب بهره" گفته می‌شود و به طور کلی با پرداخت هر فرض استفاده ارزش‌گذاری می‌شود. ارسال کنندگان نرم‌افزار به‌عنوان سرویس همه در همه برنامه های ارزشمند با استفاده از هزینه عضویت، در مدل نرم‌افزار به‌عنوان سرویس، ارائه دهندگان ابر نرم افزارهای کاربردی را در فضای ابری نصب و راه اندازی می‌کنند و کاربران ابری از کلاینت‌های ابری به نرم‌افزار دسترسی دارند. کاربران ابری زیرساخت و پلتفرم ابری را که برنامه در آن اجرا می شود مدیریت نمی‌کنند و این امر نیاز به نصب و اجرای

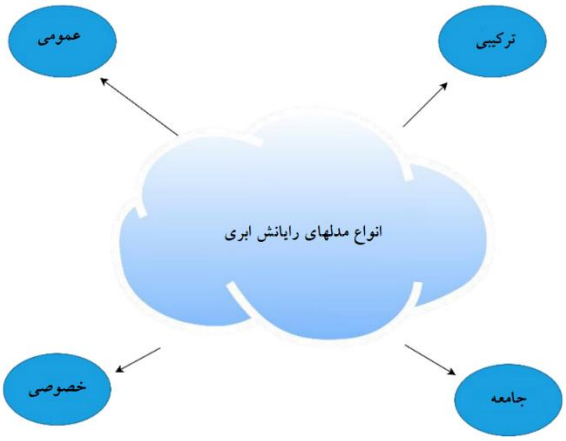
[3] Runtime cloud

برنامه بر روی رایانه شخصی کاربر ابری دارد که حفظ و پشتیبانی را آسان‌تر می‌کند. تنها نقطه ضعف نرم‌افزار به‌عنوان سرویس این است که اطلاعات مشتریان معمولاً روی سرور تأمین‌کننده ابر قرار می‌گیرد. در نتیجه، ممکن است دسترسی غیرمجاز به داده ها وجود داشته باشد .از این رو، مشتریان به تدریج از چارچوب‌های مدیریت کلیدی خارجی مشتاق برای کمک به امنیت اطلاعات خود استفاده می‌کنند[۳].

ذخیره‌سازی داده به عنوان سرویس: ذخیره سازی داده به عنوان سرویس[4] فضای ذخیره‌سازی مجازی که در صورت تقاضا در دسترس قرار می‌گیرد، اکنون یک سرویس ابری مجزا به نام سرویس ذخیره‌سازی داده است. سرویس ذخیره-سازی اطلاعات عالی به عنوان یک نوع زیرساخت و به عنوان یک سرویس منحصر به فرد است. این به دلیل این واقعیت است که هزینه‌های اولیه گران برای سیستم‌های پایگاه داده سازمانی در محل، گاهی اوقات با سرورهای اختصاصی، مجوزهای نرم افزار، خدمات پس از تحویل و نگهداری داخلی IT مرتبط است. مشتریان می‌توانند از ذخیره‌سازی داده به عنوان سرویس برای پرداخت هزینه خدماتی که استفاده می‌کنند به جای دریافت مجوز سایت برای کل پایگاه داده استفاده کنند. در کنار رابط-های ذخیره‌سازی سنتی‌تر مانند سیستم‌های فایل و سیستم‌های مدیریت پایگاه داده رابطه‌ای، که اغلب بسیار بزرگ، بسیار کند و بسیار گران هستند، برخی از ارائه دهندگان خدمات ذخیره-سازی داده نیز انتزاعی‌هایی به سبک جدول ارائه می‌دهند که حجم قابل توجهی از داده‌ها را در یک مقیاس زمانی بسیار فشرده ذخیره و بازیابی می‌کند[۸].

۵- انواع مدل‌های رایانش ابری

نسخه استقرار ابری به‌عنوان یک محیط محاسباتی دیجیتال عمل می‌کند و می‌توانید نسخه استقرار را بر اساس میزان اطلاعاتی که ذخیره می‌کنید، حق ورود به زیرساخت را انتخاب کنید. چهار نوع مختلف از مدل‌های استقرار محاسبات ابری وجود دارد: ابر عمومی، ابر خصوصی، ابر جامعه و ابر ترکیبی بر اساس موقعیت جغرافیایی خود طبقه‌بندی می‌شوند[۱۳].



شکل ۳: انواع مدلهای رایانش ابری[۱۳].

ابر عمومی: این نوع ابر برای عموم بسیار آزاد است. این مدل‌های ابر عمومی برای کسب‌وکارهایی با نیازهای فزاینده و نگرانی‌های امنیتی کمتر ایده‌آل هستند. ابرهای عمومی از طریق ارائه دهندگان اصلی حامل ابر تحت مالکیت و کنترل هستند[۱۳]. متشکل از شخص ثالثی است که منابع فیزیکی را به طور کامل در اختیار دارد و خدمات ابری مختلف را از طریق اینترنت به کاربران ارائه می‌دهد. کاربرانی که توسط ارائه‌دهنده ابر پشتیبانی می‌شوند، از افراد گرفته تا مؤسسات شرکتی را شامل می‌شوند[۱۴].

ابر خصوصی: ابرهای خصوصی توسط مشاغلی استفاده می‌شود که به دنبال کارایی هزینه و کنترل بهتر بر داده ها و منابع خود هستند. امکانات بیشتری برای کمک به رفع نیازهای سازمانی خاص از نظر سفارشی‌سازی ارائه می‌دهد (یک مدل استقرار رایانش ابری است که در آن تمام منابع سخت‌افزاری و نرم‌افزاری فقط به یک مشتری یا سازمان اختصاص داده می‌شود.) [۱۳]. ابر خصوصی به طور انحصاری برای یک موسسه خاص ارائه می‌شود. این مدل می‌تواند به نظارت بر عملکرد یک سیستم، دستورالعمل های امنیتی و داده‌ها کمک کند. یک مؤسسه همچنین می‌تواند خدمات ابری خاص خود را منتشر کند و یک مؤسسه شخص ثالث می‌تواند به تنهایی مدل را مدیریت کند[۱۴].

ابر اجتماعی: مجموعه‌ای از کسب‌وکارهای مختلف می‌توانند به سیستم‌ها، خدمات دسترسی داشته باشند و از طریق یک ابر جامعه، که نوعی معماری ابری است دسترسی داشته باشند، مدیریت کنید و اجرا کنید[۱۳]. ابر جامعه ارائه

[4] Data storage as service

خدمات ابری مختلف را بر اساس گروه خاصی از مؤسسات با مأموریت، شرایط انطباق، سیاست‌ها و خواسته‌های امنیتی یکسان نشان می‌دهد. یک ابر جامعه یک تعمیم ابر خصوصی را نشان می‌دهد و بنابراین، نهادهای بیشتری را در هر تحقق شامل می‌شود[۱٤].

ابر ترکیبی: ادغام و ترکیب مدل‌های ابری مختلف (به عنوان مثال: مدل‌های ابر عمومی، عمومی و خصوصی) یک مدل ابر ترکیبی را نشان می‌دهد. آنها در سال‌های اخیر در درجه اول به دلیل محبوبیت و استفاده گسترده از خدمات ابری بسیار محبوب شده‌اند، که اکنون با پویایی پیچیده زیرساخت های شرکتی و بازارهای تجاری جدید مواجه است. با وجود گروه بندی این مدل های مختلف با یکدیگر، آنها متمایز باقی می‌مانند و در استانداردهای انحصاری گنجانده شده‌اند و استانداردها و فناوری متمایز با توجه به عملکرد داده‌ها و کاربردهای مختلف دارند. ابر هیبریدی مزایا و معایب ابرهای اجتماعی، عمومی و خصوصی را به ارث می‌برد. در نتیجه، یک رویکرد بهینه را نشان می‌دهد که تعادل ظریفی بین قیمت و کنترل ایجاد می‌کند، که ملاحظات قوی برای دوام اقتصادی و همچنین رضایت کاربر از خدمات و برنامه های ابری است[۱٤].

امنیت در یک ابر عمومی پایین، در یک ابر خصوصی بالا و در یک ابر ترکیبی متوسط است. ابرهای عمومی به عنوان امنیت کمتری در نظر گرفته می شوند زیرا محافظت از داده‌ها در برابر حملات خصمانه چالش برانگیزتر است. ابرهای خصوصی آنهایی هستند که مالک یا شخص ثالث آنها را مدیریت می کند. سطوح امنیتی را می‌توان به این روش تغییر داد تا مطابق با نیازهای کسب و کار باشد. ابر اجتماعی مجموعه‌ای از مدل‌های مختلف است. متأسفانه، تمام نقص‌های امنیتی در سایر مدل‌های ابری به این مدل منتقل می شود[۷].

۶- چالش‌های سرویس‌های رایانش ابری

استفاده از محاسبات ابری، که تحویل بر اساس تقاضای منابع محاسباتی و ذخیره‌سازی داده‌ها است، دارای مزایا و معایبی است .اگرچه رایانش ابری به سرعت در حال گسترش است و به دلیل امکانات گسترده و پهنای ابری، یکی از بهترین شاهکارهای مهندسی نسل ما باقی مانده است، ارائه دهندگان خدمات ابری اکنون خدمات برتر ارائه می‌کنند که پذیرش آن در حال افزایش است. از آنجایی که رایانش ابری هزینه ها را کاهش می‌دهد، توسعه ابر برای سازمان‌های بزرگ دولتی و خصوصی و کسب و کارهای کوچک مفید است .پیش بینی می شود که بیش از ۹۴ درصد از کسب و کارها سرمایه‌گذاری ابری خود را بیش از ۴۵ درصد افزایش دهند. در نتیجه، اکنون فرصت های شغلی پرسودتری به خصوص برای توسعه دهندگان ابری در دسترس است. ممکن است تصور شود که ابر برای شرکت‌ها، دانش‌آموزان، توسعه‌دهندگان یا هر انجمن دیگری که به آن وابسته است، یکی از جنبه‌های کلیدی زندگی امروز است، اما با توجه به این اتکا، توجه به مشکلات مربوط به رایانش ابری نیز بسیار مهم است. با توجه به این موضوع، برخی از رایج‌ترین مسائل صنعت رایانش ابری مورد بحث قرار خواهد گرفت. برای اطلاعات بیشتر به هر یک از آنها به صورت جداگانه در زیر اشاره می‌شود[۱۳]:

امنیت داده‌ها و حریم خصوصی: امنیت داده‌ها هنگام استفاده از محاسبات ابری از اهمیت بالایی برخوردار است. داده هایی که برای کاربران یا کسب و کارها مهم و خصوصی هستند در فضای ابری ذخیره می‌شوند. علیرغم اینکه یک ارائه دهنده خدمات ابری به یکپارچگی داده‌ها اهمیت می‌دهد، مسئول شناسایی کاربر و مجوز نیز می‌باشد و اعتماد کاربران به برنامه‌ها، به دلیل نقض داده‌ها، حملات بدافزار و سایر تهدیدات امنیتی مانند سرقت هویت در فضای ابری کاهش می‌یابد، که این موضوع منجر به از دست دادن بالقوه موقعیت مناسب می‌شود. علاوه بر این، ارسال و دریافت سریع حجم زیادی از داده‌های مورد نیاز برای رایانش ابری، آن را در معرض نشت داده‌ها قرار می‌دهد.

مدیریت هزینه: همه ارائه‌دهندگان خدمات ابری رویکرد «پرداخت در حین کار» را ارائه می‌کنند که هزینه کلی منابع مصرف‌شده را کاهش می‌دهد، اما چند موقعیت وجود دارد که همراهی با استفاده از رایانش ابری هزینه‌های قابل‌توجهی را متحمل می‌شود. هزینه های پنهان زمانی افزایش می‌یابد که منابع بهینه نشده باشند (مانند زمانی که سرورها با حداکثر ظرفیت خود استفاده نشوند). اگر برنامه پیش‌بینی‌نشده در موارد استفاده یا عملکرد برنامه کاربردی پایین‌تر وجود داشته باشد، هزینه کلی افزایش می‌یابد. همچنین یکی دیگر از دلایل اصلی افزایش هزینه، استفاده ناکافی از منابع است، به طور مثال وقتی یک سرویس یا نمونه ابری در آخر هفته یا زمانی که ترافیک کمی وجود دارد فعال می‌شود و غیرفعال نمی‌گردد.

محیط چند ابری: امروزه کسب‌وکارها علاوه بر استفاده از یک ابر واحد، به بسیاری از ارائه‌دهندگان خدمات ابری وابسته هستند زیرا گزینه‌های بیشتری دارند. ۸۴ درصد از این شرکت‌ها از چندین ابر استفاده می‌کنند و بسیاری از آنها از معماری های ابری ترکیبی استفاده می‌کنند. به گفته تیم زیرساخت، مدیریت این امر اغلب دشوارتر می‌شود. این فرآیند اغلب برای تیم فناوری اطلاعات به دلیل تفاوت‌های بین ارائه‌دهندگان مختلف ابری بسیار دشوار می‌شود.

چالش‌های عملکرد: هنگام ارزیابی راه‌حل‌های مبتنی بر ابر، عملکرد عامل مهمی است که باید در نظر گرفته شود. اگر ابر عملکرد ضعیفی داشته باشد، کاربران ممکن است از آن استفاده نکنند و کسب و کارها ممکن است در نتیجه آسیب ببینند. کمی تأخیر در هنگام باز کردن یک برنامه یا وب سایت می‌تواند منجر به کاهش شدید کاربران شود. از آنجایی که سرور نمی‌تواند ترافیک ورودی را به طور موثر برای بهترین تجربه کاربری تقسیم کند، تعادل بار ناکارآمد ممکن است ریشه این تاخیر باشد .تحمل خطا، که به توانایی ادامه عملیات حتی زمانی که یک یا چند جزء از کار می افتد اشاره دارد، چنین مشکلاتی را ایجاد می‌کند.

قابلیت همکاری و انعطاف‌پذیری: از آنجا که برنامه-های کاربردی ساخته شده برای یک ابر و پشته برنامه‌های کاربردی آن باید برای ابر جدید توسعه داده شوند، تغییر از یک ارائه دهنده سرویس ابری به دیگری می‌تواند عملیات زمان بری باشد. مهاجرت از یک ابر به ابر دیگر دشوار است، بنابراین سازگار نیست. زیرا گاهی ممکن است به هر دلیلی برنامه‌ها بین دو یا چند اکوسیستم ابری جابه‌جا شوند که این کار برای سرویس‌های ابری، به یک چالش و محدودیت باشد.

فقدان دانش و تخصص: پیچیدگی ابر و نیاز شدید به تحقیق، کار با آن را اغلب به یک کار بسیار دشوار تبدیل کرده است که نیاز به تخصص و دانش قابل توجهی دارد. با وجود اینکه این کسب و کار متخصصان زیادی دارد، با این وجود آنها نیاز به بهبود مستمر توانایی های خود دارند. وقتی صحبت از رایانش ابری به میان می‌آید، به دلیل عدم تعادل عرضه و تقاضا، دستمزدها فوق‌العاده بالاست. علیرغم تعداد زیادی نقش که هنوز تکمیل نشده اند، مهندسان ابر ماهر، توسعه دهندگان و متخصصان زیادی وجود ندارند. برای اینکه این افراد بتوانند به طور فعال سیستم‌های مبتنی بر ابر را با کمترین مسائل و حداکثر قابلیت اطمینان درک، مدیریت و توسعه دهند، ارتقاء مهارت لازم است.

۷- مسائل / الزامات امنیت ابری

اعتماد به ارائه‌دهنده خدمات ابری و سرویس های آن‌ها یکی از قوی‌ترین نیروهای محرک در پس تصمیم کاربر برای انتقال به یک سیستم ابری یا ادامه دادن به سیستم قدیمی است. اعتماد مبتنی بر این ارزیابی است که آیا یک ارائه‌دهنده تمام خطرات را پوشش داده است، از جمله حوزه‌های امنیت داده، امنیت ماشین مجازی و همچنین سایر مسائل دولتی و انطباق. سه عاملی که در اینجا برای ارزیابی امنیت سیستم ابری در نظر گرفته شده اند عبارتند از: محرمانه بودن، یکپارچگی و در دسترس بودن. از آنجایی که سه‌گانه محرمانه بودن، یکپارچگی و در دسترس بودن ، سه مسئله پرکاربرد برای تعیین نگرانی‌های امنیتی یک سیستم اطلاعاتی سنتی است، تمرکز اصلی این بخش تعمیم الزامات امنیتی در یک سیستم ابری موجود تحت این مسائل است. طبقه‌بندی بیشتر و طبقه‌بندی دقیق مسائل امنیتی در اینجا ارائه شده است که درک، نقشه برداری و ارزیابی حملات خاص ابر و راه حل های پیشنهادی را آسان می‌کند[۱۵].

محرمانه بودن: محرمانگی به محافظت از برخی دارایی-های شرکت در برابر افشای اطلاعات به کاربران غیرمجاز اشاره دارد. در یک سیستم ابری، چنین کاربرانی ممکن است مشتریانی باشند که ممکن است بخواهند به داده های افراد دیگری که در جدولی مشابه با داده‌های نفوذگر توسط سیاست امنیت محتوا ذخیره می‌شود، دسترسی غیرمجاز داشته باشند. همچنین ممکن است خود سیاست امنیت محتوا شامل برخی از اعضای نادرست یا کنجکاو باشد که می‌توانند داده های خصوصی و ارزشمند مشتری را مشاهده کنند یا حتی در آن دستکاری کنند. به غیر از داده‌های مشتری، شبکه ماشین مجازی جز الزامات محرمانه اجتناب ناپذیری دارند[۱۵].

یکپارچگی: یکپارچگی به ویژگی امنیتی یک دارایی اطلاق می‌شود که تضمین می‌کند توسط برخی از پرسنل شخص ثالث که مجاز به انجام چنین فعالیتی نیستند، قابل دسترسی نیست. بنابراین صحت و درستی یک دارایی نسبت به مالک آن توسط این دارایی تضمین می‌شود. معمولاً اعتقاد بر این است که عملیات افزودن، حذف یا ویرایش یکپارچگی هر دارایی را تغییر می‌دهد. از آنجایی که کاربران از طریق

مرورگرهای وب به سرویس‌های مبتنی بر ابر دسترسی پیدا می‌کنند، بنابراین همه حملات مبتنی بر وب در یک محیط ابری که می‌تواند محتویات فایل‌های کاربر، پایگاه‌های داده، ابرداده‌های ماشین مجازی یا حتی فایل‌های WSDL[5] را تغییر دهد، بسیار رایج است[۱۵].

در دسترس بودن: در دسترس بودن یکی از مهمترین جنبه‌های امنیتی است که باید توسط CSP حفظ شود. شرکت‌های تجاری مختلف که از خدمات مبتنی بر ابر برای ارائه خدمات به مشتریان خود استفاده می‌کنند، باید از در دسترس بودن این خدمات اطمینان حاصل کنند، زیرا کوچک‌ترین خرابی می‌تواند منجر به زیان پولی بزرگی شود که غیرقابل جبران است. یک قرارداد معمولی در سطح خدمات بیان می‌کند که ارائه‌دهنده چه چیزی را از نظر در دسترس بودن و پاسخ به تقاضا ارائه کرده است. به عنوان مثال، سطح خدمات ممکن است مشخص کند که منابع در ۹۹.۹۹۹٪ مواقع در دسترس خواهند بود و اگر بیش از ۸۰٪ از هر منبعی استفاده شود، منابع بیشتری به صورت پویا ارائه می‌شود[۱۵].

۸- چالش‌های امنیتی رایانش ابری

امنیت چالش بزرگی است که محاسبات ابری به دلیل معماری باز و توزیع شده آن با آن مواجه است. از این رو، آسیب-پذیر و مستعد نفوذهایی است که محرمانه بودن، در دسترس بودن و یکپارچگی منابع ابری و خدمات ارائه شده را تحت تأثیر قرار می‌دهد. سیستم تشخیص نفوذ به متداول‌ترین مؤلفه مورد استفاده در امنیت سیستم رایانه‌ای و شیوه‌های انطباق تبدیل شده است که از محیط ابری در برابر انواع مختلف تهدیدات و حملات محافظت می‌کند[۱۶]. چون امنیت یک نگرانی ضروری برای داشتن ماهیت باز و توزیع شده ابر است، توسعه سیستم تشخیص نفوذ کارآمد یک کار ضروری است. نفوذ می‌تواند حمله‌ای باشد که از اطلاعات خصوصی یا حساس کاربران سوء استفاده کند یا می‌تواند منابعی مانند پردازنده، پهنای باند و فضای ذخیره‌سازی را مصرف کند. روش‌های سنتی برای تامین امنیت مانند فایروال ها کافی نیستند. اما نیاز به یک سیستم مناسب است که بتواند امنیت کاربران را تامین کند [۱۷]. بدون شک چالش برانگیزترین جنبه برای رایانش ابری، امنیت است. علیرغم بکارگیری تدابیر امنیتی مختلف برای ایمن سازی رایانش ابری، هنوز چالش‌های زیادی برای مقابله با CSP وجود دارد که به شرح زیر[۱۸]:

تهدیدات از داخل و خارج: تهدیدات مخرب خارج از شرکت برای CSPها خطرناک هستند زیرا حملات غیرقابل پیش بینی هستند و می‌توانند باعث آسیب شدید به CSPها و کلاینتهای رایانش ابری می‌شود. با این حال، تهدیدهای داخلی خطرناک ترین در نظر گرفته می‌شوند، زیرا دشمنان از درون شرکتی که سرویس رایانش ابری را ارائه می‌دهد، ظاهر می‌شوند.

برتری بین رایانش ابر عمومی و رایانش ابر داخلی (خصوصی): بهترین محافظت برای کاهش چشمگیر حملات، استفاده از رایانش ابر در محل است که پیچیدگی کمتری نسبت به رایانش ابر عمومی دارد. در عین حال، آنها پرهزینه هستند و انگیزه اصلی پشت رایانش ابر را نادیده می‌گیرند.

چند مستاجر: در عموم صاحبان CSP، یک Hypervisorواحد شامل ماشین‌های مجازی متعددی است که به چندین کلاینت رایانش ابری تعلق دارند. این‌ها ماشین مجازی میزبان نامیده می‌شوند و می‌توانند رقیب یکدیگر باشند یا به دنبال آن مشکلاتی برای حمله به ماشین مجازی دیگر ایجاد شوند.

دسترسی از وب: رایانش ابر در برابر دامنه وسیعی از حملات لایه برنامه، مانند حملات تزریقی زبان پرس و جو ساخت یافته و حملات سیلHTTP ، ناتوان است. باید دانش قابل توجهی در مورد تلاش‌های ایمنی برای توسعه دهندگان نرم‌افزار وجود داشته باشد. چرخه عمر پیشرفت نرم‌افزار باید تکنیک کنترل امنیتی را در بهبود SaaS بگنجاند.

Hypervisor تضمینی: هایپروایزر یا مدیر ماشین مجازی بر سیستم عامل‌های مختلف در حال اجرا بر روی یک سرور که توسط کلاینت‌های رایانش ابری مشارکت دارد، نظارت و مدیریت می‌کند. ماموریت اصلی مدیر ماشین مجازی تخصیص منابع به سیستم عامل یا ماشین مجازی متصل به یک کلاینت رایانش ابری است. مدیر ماشین مجازی باید از مرزهای ماشین مجازی محافظت کند. هرگونه مشکل امنیتی یا حمله به مدیر ماشین مجازی، امنیت ماشین مجازی میزبانی شده روی سرورهای فیزیکی را به خطر می‌اندازد .

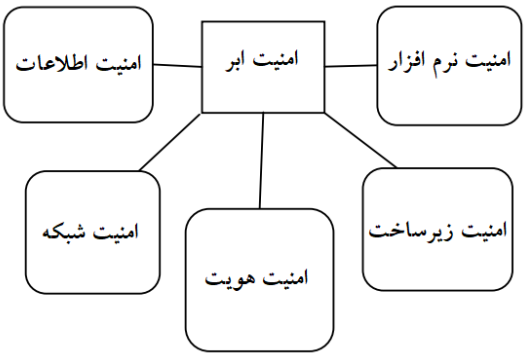
پویایی و پروتکل‌های محدوده شبکه: خدمات ارائه شده توسط رایانش ابری متنوع، پیچیده و کشسان هستند که

[5] Web Services Description Language

به طور بالقوه می‌تواند مسائل امنیتی متعددی را ایجاد کند. بنابراین مکانیسم‌های امنیتی مانند سیستم تشخیص نفوذ و سیستم‌های پیشگیری از نفوذ برای شناسایی و جلوگیری از حملات به رایانش ابری مورد نیاز است.

۹- انواع امنیت رایانش ابری

مدل محاسبات ابری به طور قابل توجهی و تصاعدی به سمت توسعه خود حرکت کرده است و به یک پدیده انقلابی در فناوری اطلاعات تبدیل شده است زیرا به مصرف کنندگان و ارائه دهندگان خود صرفه جویی قابل توجهی در هزینه ها و فرصت های تجاری جدید ارائه می‌دهد. رایانش ابری توسط مشتریانی تعریف می‌شود که به‌صورت دلخواه از خدمات ابری استفاده می‌کنند، از منابع تلفیقی به‌عنوان سرویسی استفاده می‌کنند که می‌تواند به سرعت و انعطاف‌پذیری بالا یا پایین رشد کند، کسانی که فقط برای آنچه استفاده می‌شود هزینه می‌کنند و از طریق زیرساخت شبکه‌ای به خدمات دسترسی دارند. زیرساخت ابری در حال تغییر مدل سنتی ارائه خدمات فناوری اطلاعات است .نتایج شرکت و فناوری اطلاعات شامل کاهش هزینه، مقیاس پذیری، کارایی، استفاده از دارایی، بهبود کارایی و تحرک است. رایانش ابری راهی برای ذخیره داده‌های ابری و دسترسی از راه دور با پیوند دادن برنامه ابری به اینترنت ارائه می‌دهد. مشتریان می توانند با انتخاب سرویس‌های ابری متاداده خود را در سرور داده ابری ذخیره کنند. اطلاعات ذخیره شده در مرکز داده ابری می‌تواند توسط فروشندگان خدمات ابری بازیابی یا مدیریت شود. داده‌های جمع‌آوری شده برای پردازش داده ها در یک مرکز داده ابری، باید به صورت حرفه‌ای انجام شود. دسته بندی امنیت رایانش ابری که در شکل ۴ نشان داده شده است عبارتند از: هویت، اطلاعات، زیرساخت، امنیت شبکه و نرم‌افزار[۱۹].



شکل۴: نمایی از انواع امنیت محاسبات ابری[۱۹].

امنیت هویت: به عنوان روش‌شناسی حریم خصوصی و حرفه‌ای توصیف می شود که "به افراد احراز هویت شده اجازه می‌دهد تا منابع را در زمان مناسب و برای اهداف خوب بازیابی کنند". حریم خصوصی و امنیت داده‌ها و برنامه‌ها را حفظ می‌کند و در عین حال دسترسی آن‌ها به افراد تایید شده را افزایش می‌دهد.

امنیت اطلاعات: تعهدات برای حفاظت از اطلاعات شامل نگهداری مجموعه‌ای از عملیات تجاری است که منابع داده را بدون توجه به اینکه داده‌ها رمزگذاری شده‌اند یا در حال انتقال، پردازش یا ذخیره شده اند، ایمن می‌کند.

امنیت شبکه: امنیت شبکه یک پیش نیاز محاسباتی ضروری است که شامل برداشتن گام‌های سخت‌افزاری و نرم‌افزاری دفاعی برای جلوگیری از تهدید به زیرساخت‌های شبکه موجود در برابر افراد غیرمعتبر (تایید نشده)، نقض، خرابی، تنظیم، تخریب یا انتشار نامناسب است. در نتیجه یک انجمن پایدار برای ماشین‌ها، مشتریان و خدمات فراهم می‌کند تا عملکردهای حیاتی خود را در یک محیط امن اجرا کنند. نگرانی‌های سطح شبکه می‌تواند بر سیستم وب تأثیر بگذارد که اساساً بر ظرفیت تأثیر می‌گذارد و تأخیر دستگاه را افزایش می‌دهد.

امنیت نرم‌افزار: برای ایجاد یک فرآیند تحلیل امنیتی، مسائل امنیتی برای برنامه‌ها باید با مفهوم برنامه شروع شود و از طریق فرآیندهای طرح بندی و اجرا ادامه یابد. همه این مراحل برای ارائه بهترین سطح حفاظت نرم افزار بر دیگری تکیه دارند . اگرچه تلاش‌های زیادی در توسعه نرم‌افزارها از نظر پیچیدگی وجود دارد، اما همه آنها نیاز به ضمانت امنیتی دارند.

امنیت زیرساخت: برای اینکه بتوان نیازهای کسب و کار را جهت برخورداری از زیرساخت و زیربنای ایمن بررسی کرد، این بخش برای یک شرکت کاملاً ضروری است. عناصر نیز باید جدا نگهداری شوند. جداسازی ماژول‌ها از مدیریت به کاربران شبکه اجازه می‌دهد تا از دسترسی راحت به درایورهای حافظه یا کدهای رمزنگاری اجتناب کنند.

راه حل: الگوریتم رمزگذاری پیشرفته به محاسبات ابری برای بهبود دفاع امنیتی اضافه شده است. رمزگذاری بر اساس ویژگی، رمزگذاری هومومورفیک و رمزگذاری متقارن انواع اصلی رمزگذاری هستند. رمزگذاری ویژگی، شامل رمز امنیتی متن یا کد کلید است که برای شفاف‌سازی متون رمزگذاری

شده و همچنین اعداد مخفی فاکتور متن رمزگذاری شده، که مشتری برای رمزگشایی در پشت آن باقی می‌ماند(منظور این است که از رمز اطلاعی ندارد)، استفاده می‌شود. استفاده از رمزگذاری هوموورفیک در رایانش ابری امکان پردازش آسان محتوای رمزگذاری شده را فراهم می‌کند. رمزگذاری متقارن نیاز به یک رمزنگاری ابتدایی دارد که قابلیت‌های جستجوی محافظت شده را بر روی داده‌های حساس تسهیل می‌کند. این اشکال رمزگذاری را می‌توان با محصولات فعال تقویت کرد تا امنیت داده‌ها را تضمین کند[۱۹].

۱۰- استانداردهای امنیت رایانش ابری

استانداردهای امنیتی متدولوژی و رویه های اجرای یک برنامه امنیتی را مشخص می‌کند. برای حفظ یک محیط امن، که حفاظت و امنیت را ایجاد می‌کند، برخی از پیشرفت‌های خاص با اعمال فعالیت‌های مربوط به ابر توسط این استانداردها انجام می‌شود. مفهومی به نام "دفاع در عمق" به عنوان بخشی از ابر برای ایجاد امنیت استفاده می شود. این ایده دارای لایه‌هایی از مانع است. به این ترتیب، در صورت خرابی یکی از سیستم‌ها، می‌توان از تکنیک همپوشانی برای تامین امنیت استفاده کرد زیرا نقطه‌ای از خرابی واحد ندارد .به طور سنتی، نقاط پایانی دارای سیستمی برای مراقبت از امنیت هستند، جایی که دسترسی به آن توسط مشتری کنترل می‌شود.

استانداردهای امنیت رایانش ابری اساساً به عنوان بخشی از معاملات تجاری برای مکاتبات امن بین همدستان آنلاین استفاده می‌شود. این یک استاندارد مبتنی بر XML است که برای احراز هویت جهت دادن مجوز در بین کاربران استفاده می شود. استانداردهای امنیت رایانش ابری سه نقش را تعریف می کند: اصلی (کاربر)، ارائه دهنده خدمات و ارائه دهنده هویت . استانداردهای امنیت رایانش ابری پرس و جوها و پاسخ هایی را برای تعیین مجوز و اطلاعات احراز هویت ویژگی های کاربر در قالب XML ارائه می‌دهد که یک صفحه وب آنلاین است که اطلاعات امنیتی را دریافت می‌کند[۲۰].

احراز هویت باز[6]: تکنیکی است که برای ارتباط با اطلاعات ایمن استفاده می‌شود که اساساً برای دسترسی به اطلاعات استفاده می‌شود. مشتریان می‌توانند به طراحان و خریداران دسترسی به داده‌ها را بدون اشتراک‌گذاری هویت آنها اعطا کنند.

OpenID: OpenID یک روش یک بار ورود به سیستم است. این یک فرآیند ورود به سیستم معمولی است که به مشتری امکان می‌دهد یک بار وارد سیستم شود و سپس از تمام چارچوب های شرکت کننده استفاده کند. این بر اساس مجوز مرکزی برای اعتبارسنجی مشتریان نیست.

امنیت لایه انتقال[7]/ لایه سوکت‌های امن[8]: لایه سوکت‌های امن برای ارائه ارتباط امن از طریق TCP/IP استفاده می‌شود. لایه سوکت‌های امن اساساً در سه مرحله کار می کند: در مرحله اول، مذاکره بین مشتریان برای شناسایی رمزهای مورد استفاده انجام می شود. در مرحله دوم از الگوریتم تبادل کلید برای اعتبارسنجی استفاده می‌شود. این الگوریتم‌های تبادل کلید، الگوریتم کلید عمومی هستند. مرحله آخر و سوم شامل رمزگذاری پیام و رمزگذاری است[۲۰].

۱۱- انواع شبکه و حملات در امنیت رایانش ابری

داده ها باید در هنگام تحویل بین کاربر پایانه و رایانه و همچنین بین رایانه و مرورگر وب محافظت شوند. از جمله تکنیک‌های مختلف امنیت شبکه که ممکن است در این بررسی استفاده شود عبارتند از[۲۱]:

حملات انکار سرویس توزیع شده: حملات انکار سرویس توزیع شده از مقدار قابل توجهی ترافیک شبکه برای از کار انداختن سرورها و شبکه‌ها استفاده می‌کند و مصرف کنندگان از دسترسی به یک سرویس مبتنی بر اینترنت خاص محروم می‌شوند. در بدترین سناریوی شناخته شده، مهاجمان از باتنت‌ها برای راه‌اندازی حملات انکار سرویس توزیع شده استفاده می‌کنند. مشترکین یا ارائه دهندگان ممکن است برای جلوگیری از هدف قرار دادن شبکه توسط مهاجم مورد باج‌گیری قرار گیرند. نقاط پایانی رابط برنامه نویسی برنامه سرویس وب آمازون بر روی زیرساخت بزرگ، در مقیاس اینترنتی و در سطح جهانی میزبانی می‌شود که از همان مهارت مهندسی بهره می‌برد که به آمازون کمک کرد تا به بزرگترین خرده فروش آنلاین جهان تبدیل شود. راه‌حل‌های کاهش حملات انکار سرویس توزیع شده که اختصاصی هستند مورد استفاده قرار می‌گیرند. برای ارائه تنوع دسترسی به اینترنت، شبکه‌های آمازون در میان

[6] Open Authentication
[7] Transport Layer Security
[8] Secure Sockets Layer

برخی از ارائه‌دهندگان چند خانه هستند[۲۱]. در واقع مهاجمان می توانند ارتباطات کنترل کننده-سوئیچ را سیل کنند که منجر به اشباع جدول جریان سوئیچ و انکار سرویس شود. این حملات شامل چندین ربات است که ترافیک تقلبی ایجاد می‌کنند که ترافیک واقعی را تقلید می کند، منابع بسیار زیاد و ایجاد اختلال در خدمات را ایجاد می‌کند. با این حملات ، مهاجم از یک میزبان از قبل آلوده استفاده می‌کند تا منابع شبکه را سیل کرده و خدمات ارائه شده را متوقف کند[۲۲].

حمله مرد میانی[۹]: این نوعی استراق سمع فعال است که در آن مهاجم ارتباطات جداگانه ای با قربانیان برقرار می‌کند و پیام‌هایی را بین آنها مخابره می‌کند و این تصور را ایجاد می-کند که آنها به طور خصوصی صحبت می‌کنند در حالی که در واقعیت، مهاجم کل بحث را کنترل می کند. رابط‌های برنامه-نویسی کاربردی[۱۰] وب سرویس آمازون از طریق نقاط پایانی محافظت شده با لایه سوکت های امن با احراز هویت سرور قابل دسترسی هستند. در راه‌اندازی اولیه، آمازون EC2 AMI گواهی‌های میزبان پوسته سوکت امن [۱۱]جدیدی ایجاد می‌کند و آنها را در کنسول نمونه ثبت می‌کند. قبل از ورود به نمونه برای اولین بار، مشتریان ممکن است از رابط‌های برنامه‌نویسی کاربردی امن برای تماس با کنسول و دریافت گواهی‌های میزبان استفاده کنند. برای کل معاملات خود با وب سرویس آمازون، به مشتریان توصیه می‌شود از لایه سوکت های امن استفاده کنند[۲۱]. در واقع حمله مرد میانی نوعی حمله شبکه است که در آن مهاجم خود را بین فرستنده و گیرنده قرار می دهد و می تواند داده های ارسال شده بین دو طرف را رهگیری یا تغییر دهد. [۲۲].

جعل پروتکل اینترنت[۱۲]: تولید بسته‌های پروتکل کنترل انتقال/پروتکل اینترنت[۱۳] با استفاده از آدرس پروتکل اینترنت شخص دیگری است. هنگامی که یک مزاحم به رایانه دسترسی غیرمجاز پیدا می‌کند، پیام‌هایی را با یک آدرس پروتکل اینترنتبه رایانه ارسال می‌کند که نشان می‌دهد ارتباط از یک میزبان قابل اعتماد است. ترافیک شبکه جعلی را نمی‌توان از نمونه های آمازون EC2 ارسال کرد. یک نمونه نمی‌تواند ترافیک را با یک پروتکل اینترنتمنبع یا آدرس MAC به غیر از آدرس خود در سراسر معماری فایروال مبتنی بر میزبان آمازون ارسال کند[۲۱].

اسکن پورت: اگر مشترک گروه امنیتی را طوری تنظیم کند که ترافیک از هر منبعی به یک پورت خاص اجازه دهد، آن پورت در معرض اسکن پورت قرار می‌گیرد. از آنجایی که یک پورت جایی است که مرکز داده و خروجی آن از کامپیوتر انجام می‌شود، اسکن پورت دروازه های باز به کامپیوتر را شناسایی می‌کند. از آنجایی که بازدید از یک سرور اینترنتی، یک پورت را نشان می‌دهد که دری را به روی رایانه شما باز می‌کند، هیچ راهی برای جلوگیری از پورت اسکن رایانه شما در حالی که آنلاین هستید وجود ندارد. خط مشی استفاده قابل قبول محاسبات الاستیک آمازون ابر مشتریان را از اسکن پورت ها منع می‌کند. با نقض "سیاست‌های استفادهٔ صحیح" به طور جدی برخورد می‌شود و هر کدام که گزارش می‌شود بررسی می‌گردد. مشتریان این گزینه را دارند که سوء استفاده مشکوک را گزارش کنند. هنگامی که اسکن پورت کشف شود، مسدود می‌شود. پس از اسکن نمونه‌های آمازون EC2 در بیشتر موارد ناموفق است زیرا تمام پورت‌های ورودی در نمونه‌های آمازون EC2به طور پیش فرض بسته هستند و باید توسط مشتری باز شوند[۲۱].

بویشگر(استشمام) بسته (بوییدن بسته سایر مهمانان): بوییدن بسته مستلزم گوش دادن به دستگاه شبکه خام (از طریق نرم افزار) برای بسته‌های مورد علاقه است. هنگامی که برنامه بسته‌ای را شناسایی می‌کند که شرایط خاصی دارد، آن را در یک فایل ثبت می‌کند. کلماتی مانند "ورود" یا "رمز عبور" رایج ترین معیار برای یک بسته جذاب هستند. برای یک نمونه مجازی غیرقانونی نمی‌توان ارتباطاتی را که برای یک نمونه مجازی دیگر ارسال می‌شود، بپذیرد یا «بوی» کند. مشتریان می‌توانند حالت بی‌وقفه را روی رابط‌های خود فعال کنند، اما هایپروایزر هیچ ترافیکی را که خطاب به آنها نباشد، ارائه نمی‌کند. با وجود نمونه‌های مجازی‌شده که متعلق به یک مشتری است و روی یک میزبان فیزیکی اجرا می‌شود، قادر به استراق سمع ترافیک یکدیگر نیستند. حملاتی مانند مسمومیت کش ARP[14] با آمازون EC2 امکان پذیر نیست. در حالی که

[9] Man in the middle attack
[10] Application programming interface
[11] Secure socket shell

۴ IP
۵ TCP/IP
[14] Address Resolution Protocol

آمازون EC2 حفاظت کافی را در برابر مشتری که ناخواسته یا عمداً تلاش می‌کند به داده‌های دیگری دسترسی پیدا کند، فراهم می‌کند، مشتریان باید ارتباطات مهم را به عنوان یک عمل معمول رمزگذاری کنند[۲۱].

۱۲- مقایسه مشکلات امنیتی (تهدیدات امنیتی و اقدامات متقابل) در رایانش ابری

بر اساس گزارش تهدید امنیت ابری در سال ۲۰۱۹، حملات جدید میان ابری به سرعت در حال افزایش هستند. حملات بدافزار پس از نقض اطلاعات در تهدیدات امنیتی در رتبه دوم قرار دارند. مدل سرویس ابری خدمات مختلفی را در اختیار کاربران قرار می‌دهد و اطلاعاتی را آشکار می‌کند که باعث افزایش مشکلات و خطرات امنیتی سیستم‌های رایانش ابری می‌شود. در رایانش ابری، از دست دادن داده‌ها یک مشکل اساسی امنیتی است. هکرهای کارمندان خارجی و داخلی می‌توانند به صورت ناخواسته یا عمدی به داده‌ها دسترسی داشته باشند. هکرهای خارجی ممکن است از تکنیک‌های هک (به عنوان مثال ربودن و استراق سمع) برای دسترسی به پایگاه داده در چنین محیط هایی استفاده کنند. ویروس‌ها و اسب‌های تروجان نیز به خدمات ابری اضافه می‌شوند که برای ایجاد آسیب طراحی شده‌اند. بنابراین شناسایی تهدیدهای ابری احتمالی برای پیاده سازی سیستمی با مکانیسم های امنیتی بهتر ضروری است. در جدول ۱ برخی از مشکلات امنیتی با توضیحات آنها خلاصه شده است.

جدول ۱: خلاصه ای از مشکلات امنیتی رایانش ابری

توضیحات	دسته بندی
مرور و بررسی زیرساخت های ابری	**حسابرسی**
داده هایی که در اختیار کاربران غیرمجاز قرار نمی گیرند	**محرمانه بودن داده ها**
دسترسی به داده های برون سپاری شده به ابر را محدود کنید	**قابلیت کنترل دسترسی به داده ها**
کاربران هویت خود را پنهان می کنند و از اقدامات خود در داده ها و اطلاعات بازیابی شده از ابر محافظت می کنند	**قابلیت حفظ حریم خصوصی**
کاربران اطمینان حاصل می کنند که دیگران ناآگاهانه از داده های آنها سوء استفاده نمی کنند.	**مسئولیت‌پذیری داده‌ها**

حسابرسی: حسابرسی هر جنبه تجاری و کاربرد عملکرد ضروری را بررسی می‌کند. با مدل‌های مختلف در رایانش ابری، مانند عمومی، خصوصی یا ترکیبی سروکار دارد. به دلیل پیچیدگی آن، حسابرسی ابری در محیط ابری اهمیت زیادی دارد. این بدان معناست که زیرساخت ها باید حسابرسی شوند. هدف اصلی ممیزی این است که تعیین کند آیا مدیریت و مدیریت سیستم های اطلاعاتی سازمان یک سری از معیارها و الزامات ارائه شده توسط یک مرجع استاندارد خارجی را برآورده می‌کند. چارچوب سیستم حسابرسی شامل کاربران ابری، ارائه دهندگان خدمات ابری و حسابرسان شخص ثالث است. مدیریت حسابرسی به ارزش‌های خاص گزاره‌ها توجه می‌کند. اصول و مزایای آینده رایانش ابری عبارتند از: راه حل‌هایی برای هر نیاز و بودجه، حداکثر تطبیق پذیری، استفاده بهینه از انرژی، عملکرد عالی و چابکی، گشودگی به فناوری های نوظهور و امنیت. در زمینه گسترده‌تر امنیت ابر، اهمیت حسابرسی ابری در جنبه‌های کلیدی زیر منعکس می‌شود.

محرمانه بودن داده‌ها: در محرمانه بودن داده‌ها، داده ها نباید به کاربران غیرمجاز فاش شوند. پردازش داده‌ها در فضای ابری نگهداری می‌شود و مستقیماً توسط مدیر مدیریت می شود. داده‌های حساس فقط توسط کاربران مجاز قابل دسترسی هستند و هیچ شخص دیگری، از جمله ارائه‌دهنده خدمات ابری، نباید به اطلاعات مربوط به داده‌های کاربران دسترسی داشته باشد. سرویس‌های ذخیره‌سازی ابری، مانند پردازش داده‌ها، محاسبات داده‌ها و اشتراک‌گذاری داده‌ها، بدون افشای محتوای داده‌ها برای ارائه‌دهنده خدمات ابری یا دشمنان، از مالکان داده‌ها استفاده می‌کنند.

قابلیت کنترل دسترسی به داده‌ها: کنترل دسترسی به معنای محدود کردن داده‌های منتقل شده به ابر توسط مالک داده است. مالک فقط می‌تواند به کاربران قانونی اجازه دسترسی به داده‌های آنها را بدهد، در حالی که دیگران می‌توانند بدون اجازه به داده‌ها دسترسی داشته باشند. با این حال، مالکان فقط می‌توانند مجوز دسترسی را در محیط های ابری نامعتبر کنترل کنند.

قابلیت حفظ حریم خصوصی: کاربران هنگام دسترسی به داده‌ها یا خدمات ابری باید از حریم خصوصی خود آگاه باشند. کاربران معمولاً هنگام استفاده از خدمات داده ابری می‌خواهند هویت خود را پنهان کنند. علاوه بر این، کاربران می‌خواهند از داده‌های بازیابی شده برای اقدامات خود محافظت کنند. به عنوان مثال، کلمات کلیدی برای نتایج پرس و جو برای داده های برون سپاری شده و بازگشت‌های ابری نباید عمومی

شوند. علاوه بر این، هیچ طرف دیگری در ابر نباید رفتار یا عادات دسترسی کاربر را استنباط کند.

مسئولیت‌پذیری: این را می‌توان به عنوان شناخت اقدامات و فعالیت های درون شبکه و شناسایی فرد خاص تعریف کرد که برای انجام تحقیقات پزشکی قانونی و ارزیابی رویدادهای تاریخی و افراد یا رویه های مرتبط استفاده می شود. سه لایه سیستم و داده‌ها و لایه‌های گردش کار برای تسهیل پاسخگویی و اعتبار سنجی تعریف شده است. سرویس‌دهنده دسترسی مستقیم به مشتریان و نرم‌افزار در سرویس‌های ابری دارد. این بدان معنی است که دستکاری نادرست یا استفاده از داده‌های مشتری شناسایی نخواهد شد. در سمت کلاینت، استفاده از یک ابر ترکیبی می‌تواند افزایش داده و کنترل کند که چه کسی می‌تواند به داده‌های مشتری دسترسی داشته باشد و آن را تغییر دهد.

جدول ۲: تهدیدات امنیتی و اقدامات متقابل

راه حل‌ها	خدمات ابری تحت تأثیر قرار گرفته	مشکلات	تهدیدها	ناحیه
رمزگذاری داده ها، اثبات ذخیره سازی، محاسبات ایمن به کمک سرور	IaaS, SaaS, and PaaS	دسترسی یا بازیابی غیرمجاز داده ها، برنامه ها یا خدمات	نقض داده ها	تهدیدات زیرساختی
نظارت بر وضعیت شبکه و ارائه ثبت و احراز هویت قوی	IaaS, SaaS, and PaaS	از دست دادن تقلب در خدمات اعتبارسنجی و حملات شدیدتر به دلیل ورود ناشناس	سوء استفاده از خدمات ابری	
یک مکانیسم احراز هویت قوی، سیاست‌های امنیتی و یک کانال ارتباطی امن را اتخاذ کنید	IaaS, SaaS, and PaaS	کنترل غیر قانونی برخی از خدمات مجاز توسط کاربران غیرمجاز .اطلاعات حساب کاربری به سرقت رفته	هواپیماربایی	
خدماتی را ارائه دهید که زیرساخت های ابری را نظارت و کنترل می کند	IaaS, SaaS and PaaS	از دست دادن کنترل زیرساخت ابری	ارائه خدمات	تهدیدات خدماتی
انتقال داده ها رمزگذاری شده است و مکانیسم های احراز هویت وجود دارد	IaaS, SaaS, and PaaS	صدور مجوز نامناسب و احراز هویت نادرست انتقال محتوا	رابط کاربری ناامن	
فرآیندهای امنیتی و مدیریتی که از گزارش‌های پروتکل و اعلان‌های نقض استفاده می‌کنند	IaaS, SaaS, and PaaS	نفوذ به منابع سازمانی، از بین رفتن زیان بهره وری دارایی و تاثیر بر عملیات	نفوذی‌های مخرب	تهدیدات پلتفرم
از گذرواژه‌های چندلایه قوی و مکانیسم‌های احراز هویت استفاده کنید	IaaS, SaaS, and PaaS	یک مهاجم می تواند هویت یک کاربر معتبر را برای دسترسی به منابع استفاده به دست آورد	سرقت هویت	

۱۳- راه حل‌هایی برای محاسبات ابری امن

افزایش خطرات امنیتی با مقیاس‌پذیری و انعطاف‌پذیری ابر همراه است. این بخش به استراتژی‌های امنیت فضای مجازی فعلی و آینده برای حفاظت از سیستم‌های مبتنی بر ابر می‌پردازد[۷]:

تشخیص نفوذ در سیستم‌های ابری: آسیب‌پذیری‌ها زمانی رشد می‌کنند که سیستم‌های بیشتری به ابر منتقل شوند. مجوزها، لیست سفید، احراز هویت چند عاملی، فایروال‌ها و سیستم‌های تشخیص نفوذ تکنیک‌های امنیتی حیاتی برای حفاظت از محیط‌های ابری هستند.

شناسه‌های مشارکتی در سیستم‌های ابری: هدف سیستم‌های تشخیص نفوذ مشترک افزایش امنیت کلی شبکه با ترکیب چندین سیستم تشخیص نفوذ مجزا است که می‌تواند تهدیدات پیچیده‌ای مانند حمله منع سرویس توزیع شد و حملات روز صفر را شناسایی کند که می‌توانند با تبادل داده‌های حمله از یک سیستم تشخیص نفوذ اجتناب کنند.

فایروال‌ها: داده‌ها توسط فایروال‌های ابری محافظت می‌شوند که ترافیک شبکه را فیلتر کرده و دسترسی برنامه‌ها را محدود می کند.

آموزش کارکنان: برای بالا بردن سطح عمومی امنیت اطلاعات، آموزش مداوم امنیتی در زمینه مهارت فنی باید ارائه شود.

رمزگذاری داده‌ها: ایمن‌سازی داده‌های حساس در فضای ابری با استفاده از تکنیک‌های حفاظت از داده‌ها مانند رمزگذاری، رمزهای عبور، فایروال‌ها و ذخیره‌سازی داده‌ها توصیه می‌شود. بدون کلید رمزگذاری، داده های رمزگذاری شده غیرقابل استفاده هستند زیرا دسترسی به آنها امکان‌پذیر نیست. رمزگذاری داده‌ها فرآیند استفاده از کلیدهای مخفی برای تبدیل داده‌ها به یک کد مخفی است. رمزگشایی داده ها نیاز به یک کلید رمزگذاری دارد.

مدیریت هویت و دسترسی: در یک محیط ابری، **مدیریت هویت و دسترسی** دسترسی مجاز به منابع را تضمین می‌کند. رمزهای عبور موثر با تاریخ انقضا برای مدیریت هویت ضروری هستند. احراز هویت از احراز هویت چند عاملی یا بیومتریک برای تأیید هویت کاربران استفاده می‌کند. به کاربران احراز هویت شده از طریق مجوز دسترسی به منابع داده می شود. **مدیریت هویت و دسترسی** امنیت ابر را حفظ می‌کند و از داده ها محافظت می‌کند.

۱۴- نتیجه‌گیری

رایانش ابری در حوزه علوم کامپیوتر محبوبیت پیدا کرده و معمولاً به عنوان یک فناوری میزبانی داده جدید نامیده می‌شود. به لطف بازپرداخت هزینه‌های تحمیل شده به شرکت‌ها، این فناوری بسیار محبوب شده است. افزایش ناگهانی منابع و هزینه‌های زیرساخت، مؤسسات را به سمت رایانش ابری سوق می‌دهد. این تصمیم می‌تواند در صرفه جویی در هزینه ها و افزایش انعطاف پذیری کمک کند. ابر زیرساخت‌ها، برنامه‌ها و خدمات ذخیره‌سازی را در اختیار کاربران قرار می‌دهد که باید توسط برخی خط‌مشی‌ها یا رویه‌ها محافظت شوند. در واقع، امنیت در فضای ابری محافظت از داده‌ها و زیرساخت‌های کاربر در برابر کاربران مخرب با ارائه محرمانه بودن، یکپارچگی، در دسترس بودن و تشخیص نفوذ به موقع است. رایانش ابری نقشی جدایی ناپذیر در علوم رایانه ایفا می‌کند و به توسعه علوم رایانه به شیوه‌ای بسیار سریع کمک می کند. رایانش ابری را می‌توان به عنوان روشی برای به اشتراک گذاری منابع با مشتریان به روشی کارآمدتر تعریف کرد و با ایده مجازی‌سازی کار می‌کند و انواع مختلفی از ارائه دهندگان خدمات وجود دارد که مشکلاتی در امنیت و داده‌های ذخیره شده در سرور ابری دارد. نگرانی اصلی در رایانش ابری امنیت است. با توجه به معماری توزیع شده و باز، یک سیستم تشخیص نفوذ نقش مهمی را برای محافظت از یک سیستم کامپیوتری ایفا می‌کند. از جاییکه مسئله امنیت در ابر بسیار مهم است تلاش شده در این مقاله به امنیت رایانش ابری، مسائل / الزامات امنیت ابری، چالش‌های امنیتی رایانش ابری، انواع امنیت رایانش ابری، استانداردهای امنیت رایانش ابری و انواع شبکه و حملات در امنیت رایانش ابری، پرداخته شود و امید است که خوانندگان محترم تا حدودی با این مسائل آشنا شوند و مفاهیم پایه‌ای مناسبی برای آنها جهت ادامه دادن تخصصی‌تر این مسئله در رایانش ابری باشد.

۱۵- کارهای آینده

رایانش ابری به دلیل ویژگی‌های ذاتی مقیاس‌پذیری و انعطاف‌پذیری، پذیرفته شده‌اند و با وجود این مزایا، نگرانی‌های امنیتی همچنان یک چالش مهم ارائه دهندگان ابری است زیرا آسیب‌پذیری‌های جدیدی از جمله دسترسی غیرمجاز، نقض داده‌ها و تهدیدات داخلی را معرفی می‌کند. ادغام مکانیسم‌های امنیتی قوی برای رسیدگی به این چالش‌های امنیتی بسیار مهم است که یکی از این مکانیسم‌ها سیستم تشخیص نفوذ است که در حفاظت از شبکه ها و محیط های ابری ضروری است زیرا یک سیستم تشخیص نفوذ ترافیک شبکه و فعالیت‌های سیستم را نظارت می‌کند. از این رو لازم است که یک سیستم تشخیص نفوذ مناسب جهت بالا بردن امنیت محیط‌های ابری لازم است و استفاده از روش‌های یادگیری ماشینی و یادگیری عمیق را می‌توان برای افزایش عملکرد سیستم تشخیص نفوذ مورد بررسی قرار داد. با استفاده از این تکنیک‌ها، سیستم‌های تشخیص نفوذ می‌توانند با تهدیدات در حال تکامل سازگار شوند، حملات قبلی را شناسایی کرده و موارد مثبت کاذب را کاهش دهند. برای مقالات پژوهشی آتی می‌توان یک سیستم نوین تشخیص نفوذ هوشمند برای افزایش امنیت و شناسایی فعالیت های مخرب در رایانش ابری مبتنی بر ترکیب الگوریتم یادگیری عمیق و الگویتم‌های تکاملی ارائه داد، که باعث نوآوری در موضوع پژوهش شود. به طوریکه می‌توان از الگوریتم تکاملی

برای "استخراج ویژگی" جهت کاهش بعد و بهبود کیفیت داده-ها و استفاده از الگوریتم طبقه‌بندی استاندارد و مناسب جهت تشخیص زودهنگام نفوذ در رایانش ابری برای بالا بردن امنیت رایانش ابری، استفاده کرد.

۱۳- منابع

1. *Seyed Mohsen HashemiGhiri, A.A., Amin Shamohammadi, Mohammadnabi Omidvar, A Flexible Dynamic Load Balancing Model for Independent Tasks in Grid Computing. International Journal of Advanced Research inComputer Science & Technology (IJARCST 2015)72Vol. 3, Issue 3 (July - Sept. 2015), 2015.*
2. *Sood, D., H. Kour, and S. Kumar, Survey of computing technologies: Distributed, utility, cluster, grid and cloud computing. Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org, 2016. 6(5).*
3. *Chaudhary, M.S.a.J., A REVIEW OF CLOUD COMPUTING ARCHITECTURE AND SECURITY ISSUES. All content following this page was uploaded by Jyoti Chaudhary on 14 October 2023. The user has requested enhancement of the downloaded file., 2023.*
4. *Aslan, Ö., et al., A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 2023. 12(6): p. 1333.*
5. *Otieno, M., Techniques and protocols for enhancing data privacy in cloud computing: A review. World Journal of Advanced Engineering Technology and Sciences, 2023. 8(1): p. 391-404.*
6. *Ang'udi, J.J., Security challenges in cloud computing: A comprehensive analysis. World Journal of Advanced Engineering Technology and Sciences, 2023. 10(2): p. 155-181.*
7. *ALhadi, F.I., N.A. AL-Shaibany, and S.A. AL-Homdyl, Survey on Cloud Computing Security. Sana'a University Journal of Applied Sciences and Technology, 2024. 2(4): p. 381-390.*
8. *Uzoma, B.C. and I.B. Okhuoya, A RESEARCH ON CLOUD COMPUTING. 2022.*
9. *Diaby, T. and B.B. Rad, Cloud computing: a review of the concepts and deployment models. International Journal of Information Technology and Computer Science, 2017. 9(6): p. 50-58.*
10. *Giri, S.V.a.D., Survey Paper of Cloud Computing. International Journal of Engineering Research & Technology (IJERT) http://www.ijert.org ISSN: 2278-0181 IJERTV11IS010154 2022.*
11. *Islam, R., et al., The Future of Cloud Computing: Benefits and Challenges. International Journal of Communications, Network and System Sciences, 2023. 16(4): p. 53-65.*
12. *Banger, N., K. Pallavi, and S. Shetty, A Review Paper on Cloud Computing ArchitectureTypes Advantages and Disadvantages. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 2022. 2(2): p. 14-22.*
13. *Kondi, U.M., et al. A Review of the Challenges and Opportunities in Cloud Computing Services. in Proceedings of the International Conference on Innovative Computing & Communication (ICICC). 2022.*
14. *Alshareef, H.N., Current development, challenges, and future trends in cloud computing: A survey. International Journal of Advanced Computer Science and Applications, 2023. 14(3).*
15. *Basu, S., et al. Cloud computing security challenges & solutions-A survey. in 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC). 2018. IEEE.*
16. *Zouhair, C., et al., A review of intrusion detection systems in cloud computing. Security and Privacy in Smart Sensor Networks, 2018: p. 253-283.*
17. *Rana, P., et al., Intrusion detection systems in cloud computing paradigm: analysis and overview. Complexity, 2022. 2022.*
18. *Alashhab, Z.R., et al., Distributed Denial of Service Attacks against Cloud Computing Environment: Survey, Issues, Challenges and Coherent Taxonomy. Applied Sciences, 2022. 12(23): p. 12441.*
19. *Zulifqar, I., S. Anayat, and I. Khara, A review of data security challenges and their solutions in cloud computing. International Journal of Information Engineering and Electronic Business, 2021. 12(3): p. 30.*
20. *Khan, S., et al., Cloud computing: security issues and security standards. International Journal of Engineering and Management*

Research, Special Issue (ACEIT-2018): p. 31-36.

21. *Ese, O.J.O.M.S., A Review of Security Issues in Cloud Computing. BOOK Chapter | Web of Deceit - June 2022 - Creative Research Publishers - Open Access — Distributed Free 2022.*
22. *Shehzad, H.M.F., et al., A Review on Cloud Computing Threats, Security and Possible Solutions.*

حمید زنگی آبادی زاده، دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز، دانشگاه پیام نور مرکز بین الملل کیش می باشد و نشانه رایانامه ایشان عبارتند از:
Hamid.zangiabadi@gmail.com

مهدی قاسمی، دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز، دانشگاه پیام نور مرکز بین الملل کیش می باشد و نشانه رایانامه ایشان عبارتند از :
Mahdikmg1@gmail.com

فرشید وظیفه دوست، فارغ التحصیل در مقطع کارشناسی ارشد رشته مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز از دانشگاه پیام نور مرکز بین الملل قشم می باشد و نشانه رایانامه ایشان عبارتند از :
Vazifehdoostfarshid@gmail.com

سمیه کدخدا ده خانی، فارغ التحصیل مقطع کارشناسی ارشد رشته مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز دانشگاه پیام‌نور قشم می باشد، او به عنوان کارشناس فناوری در دانشگاه پیام‌نور استان کرمان مشغول به کار می باشد و نشانه رایانامه ایشان عبارتند از :
Emailsk65@gmail.com

مائده رحمانی، دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار ، دانشگاه پیام نور مرکز بین الملل کیش می باشد و نشانه رایانامه ایشان عبارتند از :
Maede9708@gmail.com

ح. زنگی آبادی زاده، م. قاسمی، ف. وظیفه دوست ، س. کدخدا ده خانی و م. رحمانی. امنیت رایانش ابری: مروری بر مفاهیم پایه‌ای، چالش‌های امنیتی ، مسائل ، الزامات، استانداردهای امنیتی و انواع حملات در رایانش ابری. دو فصلنامه محاسبات و سامانه‌های توزیع شده، سال ششم، شماره ۱، شماره پیاپی ۱۱، صفحه ۱۳۷ تا ۱۵۳، سال ۱۴۰۲

How to cite: H.Zangiabadi Zadeh ،M.Ghasemi ،F.Vazifehdoost ،S.kadkhodadehkhani ،M.Rahmani. Cloud Computing Security: A Review of Basic Concepts, Security Challenges, Issues, Requirements, Security Standards and Types of Attacks in Cloud Computing, Journal of Distributed Computing and Systems (JDCS), Vol 6, Issue 1, Page 137-153, 2023.

Cloud Computing Security: A Review of Basic Concepts, Security Challenges, Issues, Requirements, Security Standards and Types of Attacks in Cloud Computing

H.Zangiabadi Zadeh[1] ،M.Ghasemi[2] ، F.Vazifehdoost[3] ، S.kadkhodadehkhani[4] ،M.Rahmani[5]

[1] Payam Noor University, Kish International Center.
[2] Payam Noor University, Kish International Center.
[3] Payam Noor University, Qeshm International Center.
[4] Payam Noor University, Qeshm International Center.
[5] Payam Noor University, Kish.

Abstract

Cloud computing is a computing paradigm that can provide dynamic and scalable virtual resources to on-demand users via an Internet service and is also an extension of distributed computing, parallel computing, and network computing. One of the most challenging features of cloud computing is security, and data is stored on storage devices that cannot be hacked or used by anyone else. This technology has a fast and reliable storage

service, provided that all security measures are properly provided for it from the beginning. Indeed, security in this environment is very critical. Moreover, due to the unclear level of transparency of cloud security by many cloud service providers, security is a significant concern for organizations. Organizations that are thinking of moving their IT services to the cloud are unsure of several areas in the cloud and some of these areas are not expected to be cleared by the provider. In this article, we will discuss cloud computing security, cloud security issues/requirements, cloud computing security challenges, types of cloud computing security, cloud computing security standards, and types of networks and attacks in cloud computing security.