اولین کنفرانس بین المللی جهش علوم مدیریت اقتصاد و حسابداری
1st international conference on the mutation of management science, economics and accounting
www.mmea.ir
موسسه آموزش عالی ادیب مازندران
کد اختصاصی: ۰۰۲۰۱-۹۱۰۴۶

Arch

تاثیر امنیت داده ها برعملکرد فناوری اطلاعات در محاسبات رایانش ابری

محمدملکی نیا[a]، سیدعلیرضاموسوی قیداری[b]

[a] (استاد،گروه مدیریت، عضو هیئت علمی دانشکده مدیریت و حسابداری واحد تهران جنوب دانشگاه آزاد اسلامی، تهران ، ایران)

[b] (دانشجوی دکترای تخصصی، مدیریت فناوری اطلاعات، دانشگاه آزاد اسلامی، کیش)

نویسنده مسئول: alireza.musavi@srbiau.ac.ir

چکیده: عملکرد موفق فناوری اطلاعات درحوزه امنیت از مهمترین الزامات در رایانش ابری است، که توجه به آن برای هرگونه پیشرفت در یک سیستم باید در نظر گرفته شود. امنیت، شاخصی مهمی است که از طریق تهدیداتی که بر عملکرد بخش‌هایی از ابر در حین ارائه خدمات تأثیر گذار است، باید در نظر گرفته شود. امنیت وتاثیر آن بر عملکرد سیستم ، میزان کارایی رایانش ابری را در بر خواهد داشت، بنابراین امنیت از معیارهای مهم برای توسعه ابرها می باشد. در این مقاله رابطه بین عملکرد سیستم های مبنی بر رایانش ابری و امنیت مورد بررسی قرار می گیرد و میزان تأثیر آن بر پیشرفت رایانش ابری مشخص و تعیین می شود.

کلمات کلیدی: رایانش ابری؛ امنیت؛ محاسبات توزیع شده؛ SLA (قرارداد سطح سرویس).

۱. مقدمه

امروزه رایانش ابری یک فناوری جدید در دنیای بی انتهای اطلاعات است ، رایانش ابری مدلی است برای فراهم کردن دسترسی آسان بر اساس تقاضای کاربر از طریق شبکه، به مجموعه‌ای از منابع رایانشی قابل تغییر و پیکربندی (مثل:شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها) که این دسترسی بتواند با کمترین نیاز به مدیریت منابع یا نیاز به دخالت مستقیم فراهم‌کننده سرویس به سرعت فراهم شده یا آزاد گردد [۱] . محاسبات ابری مدلی برای برپاسازی شبکه ای است با قابلیت استفاده در همه جا و آسان و مناسب، بسته به تقاضا که به دریایی از منابع محاسباتی قابل پیکربندی، به اشتراک گذاشته شده و بستر فناوری اطلاعات، مانند: شبکه ها، سرورها، واحدهای ذخیره سازی، برنامه ها و سرویس هایی که قابلیت دسترسی دارند و این منابع نیز با کمترین مشکل مدیریتی یا تعاملی با ارائه دهنده ی سرویس، می توانند به سرعت در اختیار گرفته شوند [۲]. در پردازش ابری، بخش خدمات، منابع را به منظور فراهم کردن فضای ذخیره سازی ارائه می دهد. به عنوان مثال، ایمیل که مفهوم رایانش ابری را نشان می دهد، از منابع برای ذخیره پیام‌ها، استفاده می شود و این منابع بر روی رایانه شخصی نیستند، بلکه در منبعی در جای دیگری و ناشناخته برای کاربر هستند [۳]. ابر در چندین سطح پخش می شود، ازجمله سطح خصوصی، محلی، عمومی و مختلط، در حالی که مدل های خدمات شام(PAAS) ، (IAAS) و (SAAS) هستند [۴]. ابرها با پیشرفت اینترنت عمومی توسعه می‌یابد، زیرا قابلیت‌های ابرها به منظور تأمین امنیت بر اساس عملکرد، محدود است. اکثر شرکت هایی که به دنبال استفاده از خدمات ابری هستند از یک طرف سیاست سرعت و از طرف دیگر امنیت و عملکرد را دنبال می کنند، زیرا از طریق تماس با سرویس های ابری عمومی از امنیت خود چشم پوشی می کنند که در این صورت منابع پیش فرض بدست می آید. این امر محتوا و داده های سازمانی را در معرض آسیب های اینترنتی قرار می دهد [۵]. امنیت و حریم خصوصی ،چابکی فوق العاده ای در توسعه ابر ایجاد می کند. امنیت و حریم خصوصی باید توسط ارائه دهندگان خدمات ابری و همچنین قابلیت اطمینان، در دسترس بودن و عملکرد موفق، ارائه شوند [۶] . برای شرکت‌هایی که در فناوری اطلاعات متخصص هستند و خدمات ابری را ارائه می‌کنند، در دسترس بودن، عملکرد و امنیت، چالش‌هایی هستند که مشتریان رایانش ابری را برای استفاده از خدمات اتخاذ می‌کنند. نقص امنیتی خطر از دست دادن داده را به همراه دارد و همچنین سطح عملکرد به دلیل پهنای باند محدود، یا فضای دیسک، حافظه و قدرت پردازنده و تأخیر اتصال شبکه می تواند ضعیف شود و سطح عملکرد درخدمات ابری عاملی در پذیرش کاربران از ابر است [۷].

۱. ویژگی های رایانش ابری

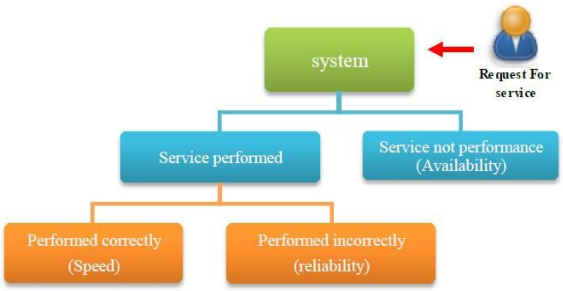
مکانیسم عمل رایانش ابری، بر اساس تقاضاو براساس سلف سرویس است[۸]. می توان از طریق چندین دستگاه مانند: تلفن همراه، رایانه و ایستگاه های کاری به ابر دسترسی پیدا کرد، جایی که ادغام منابع با استفاده از یک مدل چند مقیم در سیستم انجام می شود. اگرچه کاربران نمی توانند بدانند منابع موجود کجا هستند و ابر منابع را به شیوه ای انعطاف پذیر و سریع مطابق با تقاضای مصرف کننده فراهم می کند و در حین ارائه منابع، ابر اندازه گیری خدمات را دنبال می کند. منابع محاسبات ابری کنترل شده را می توان اندازه گیری کرد و شفافیت را هم برای ارائه دهنده خدمات و هم برای مصرف کننده سرویس مورد استفاده فراهم کرد. سرویس‌های رایانش ابری از قابلیت‌های اندازه‌گیری استفاده می‌کنند که کنترل و استفاده بهینه از منابع را ممکن می‌سازد [۹].

۲.عملکرد رایانش ابری

منظور از عملکرد که بر اساس استاندارد ISO 25010 ارائه شده است، عملکرد سیستم محاسبات ابری با تجزیه و تحلیل ویژگی های مربوط به عملکرد، در یک سرویس موثر و قابل اعتماد برای برآوردن نیازهای ذکر شده در شرایط مرزی سیستم با حداکثر تراکنش تعیین می شود. عملکرد محاسبات ابری عملکرد یک خروجی برای هر سیستمی است. معیارها و استانداردها برای سه عنصر کاربران، تامین کنندگان و ناظران اعمال می شود. مطابق شکل (۱) نشان داده شده است که هر سیستم خروجی، بر چند احتمال استوار است، یعنی ممکن است سیستم یک سرویس را به درستی یا نادرست ارائه دهد و یا این سرویس

www.SID.ir

به طور کلی رد شود و این مورد بر عملکرد سیستم تأثیر می گذارد [۱۰].



شکل ۱. خروجی سیستم محاسباتی بر اساس درخواست خدمات

رایانش ابری، یکی از سیستم های توزیع شده است که با منابع پراکنده سر و کار دارد و مبتنی بر پردازش داده های بزرگ است و این نیازمهم ، مستلزم کنترل و تحلیل عملکرد است. تکنیک های توسعه آن ها، هم برای کاربران و هم برای ارائه دهندگان خدمات مهم است. جایی که درآن سطح عملکرد بر پذیرش خدمات ابری توسط کاربران تأثیر می‌گذارد، اطلاعات و شاخص‌های عملکرد را ارائه می‌کند [۱۱]. بنابراین بررسی عملکرد در سرویس های ابری مهم و ضروری است، زیرا این عملکرد برکاربران و ارائه دهندگان خدمات تأثیر می گذارد. برای ارزیابی عملکرد، باید چندین معیار را برای ارزیابی و عوامل موثر بر عملکرد محاسبات ابری در نظر گرفت، از جمله میانگین پاسخ در واحد زمان و میانگین زمان انتظار در واحد زمان و موارد دیگر [۱۲] .

۲,۱.دسته بندی ارزیابی عملکرد ابرها:

ارزیابی(SaaS): توسط کاربران به طور مستقیم بسته به معیارهای عملکرد، سرعت پاسخگویی، قابلیت اطمینان خدمات فنی و دردسترس بودن انجام می شود.
ارزیاب(PaaS): توسط کاربران به طور مستقیم یا غیرمستقیم بسته به معیارهای عملکرد در پاسخ به عملکرد فنی، بهره وری، قابلیت اطمینان، خدمات فنی و قابلیت میان افزار انجام می شود.
ارزیابی(IaaS): معیارهای عملکرد زیرساخت، ظرفیت، قابلیت اطمینان، در دسترس بودن و مقیاس پذیری تعیین می شوند [۱۳].

۲,۲.معیارهای عملکرد

چندین گزینه برای معیارهای عملکرد رایانش ابری توسط ارائه دهندگان خدمات وجود دارد: تاخیر در سرویس و دقت عملکرد و ارزیابی بسته به زمان پاسخگویی، بهره وری و زمان بندی در اجرای وظایف، یعنی پردازش وظایف در دوره مناسب، اندازه گیری می شود. سایراقدامات دیگردر جدول ۱ وجود دارد [۱۴] .

جدول۱. الزامات عملکرد در سیستم های ابری

امکانات	معیارها	شرح
ارتباط	- فرکانس از دست دادن بسته - اتصال در میزان خطا - سرعت انتقال بیت/بایت	تبادل داده بین سرویس داخلی یا مصرف کننده خارجی در ابر
محاسبات	CPU load Benchmark OP Rate Instance Efficiency (CPU Peak)	پردازش داده های محاسباتی در سیستم های ابری
حافظه	-میانگین زمان(های) موفقیت -سرعت حافظه (بیت / بایت) -نرخ بروز رسانی حافظه تصادفی زمان پاسخگویی	استفاده سریع از اطلاعات ذخیره موقتی سرعت ناکافی درایو دیسک سخت یا دسترسی آهسته
زمان	- زمان محاسبه - زمان ارتباط	تکمیل پروژه در بهترین زمان با حفظ کیفیت برای موفقیت پروژه بسیار مهم است.

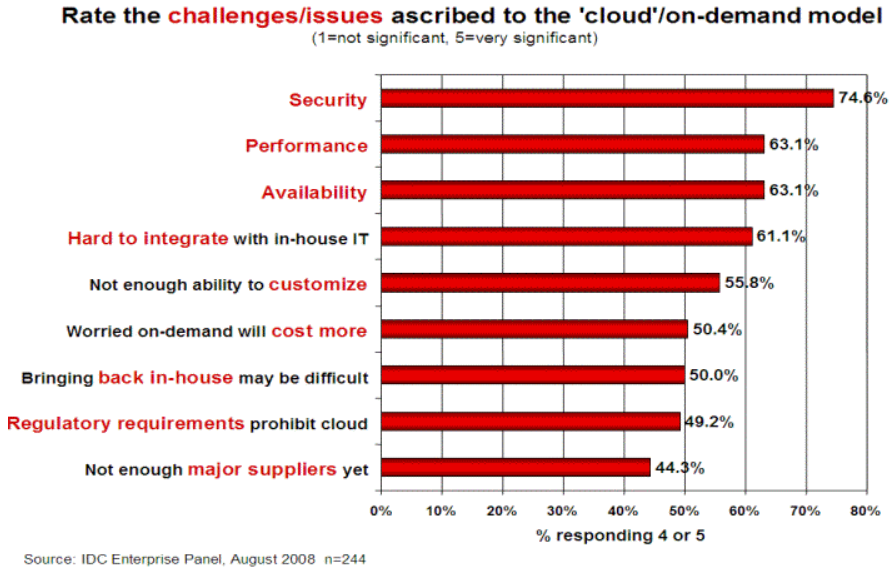
قرارداد (SLA) مشتریان و ارائه دهندگان خدمات ابری را محدود می کند. سطح خدمات یا کیفیت خدمات (QOS) باید در نظر گرفته شود. عملکرد سرویس با زمان پاسخ، بهره وری، در دسترس بودن و امنیت مشخص می شود [۱۵].
کیفیت خدمات (QoS) در ابر نشان‌دهنده سطح عملکرد و قابلیت اطمینان است، علی‌رغم این واقعیت که ویژگی‌های کیفیت خدمات قبل از تکامل محاسبات

www.SID.ir

ابری، عملکرد، همگنی و سایر استانداردها مورد توجه قرار گرفته است [۱۶].

سرعت یکی از ویژگی های (QoS) است که توسط (EG 202 009-1) تعیین شده است. این استاندارد عملکردی است که بازه زمانی را نشان می دهد و برای انجام یک عملکرد یا میانگینی که در آن عملکرد و امنیت به دست می‌آید، یعنی هر گونه قابلیت خدماتی برای اطمینان از محرمانه بودن بخشی از اطلاعاتی که با آن کار شده ، مبادله شده یا ذخیره شده است، حفظ حریم خصوصی ارتباطات، صحت و ایمنی اطلاعات مبادله شده یا اطلاعات ذخیره شده و همچنین حفاظت از کاربر و وسایل ارتباطی متقضی در برابر هر نوع تهدید، علاوه بر سایر کیفیت های دقت، قابلیت اطمینان، انعطاف پذیری و سهولت استفاده می شود[۱۷].

در شکل (۲) نشان داده می شود که تحلیل(IDC) ، عملکرد را به عنوان دومین مورد مهم، بعد از امنیت در محیط ابری در نظر می گیرند. معیارهای عملکرد بر اساس قابلیت‌های برنامه‌های کاربردی است، جایی که عملکرد به دلیل کمبود منابع، فضای دیسک، پهنای باند محدود، سرعت پایینCPU ، حافظه و اتصالات شبکه ضعیف می‌شود [۱۸].



شکل ۲. میزان مسائل و چالش های نسبت داده شده به فضای ابر

۳.امنیت در رایانش ابری

امنیت در پردازش ابری یک عامل بسیار حساس و مهم است، زیرا ابر با داده های حساس و محرمانه در مراکز داده ابری سروکار دارد. بنابراین حفاظت و یکپارچگی داده ها وظیفه ارائه دهندگان خدمات ابری است. حریم خصوصی و امنیت رایانش ابری به ارائه‌دهنده خدمات ابری بستگی دارد تا کنترل‌های امنیتی قوی و سیاست حفظ حریم خصوصی را برای محافظت از داده‌های مشتریان خود اعمال کند. زیرا مشتریان به اطمینان و شفافیت از نظر عملکرد و امنیت نیاز دارند [۱۹]. ارائه‌دهندگان ابر، خدماتی را به چندین سازمان مستقر در یک شبکه ارائه می‌دهند که بدون اجازه سازمان دیگری که در همان زمینه مراکز داده ابری کار می‌کند، به داده‌ها دسترسی پیدا کنند. علاوه بر آن، امنیت فیزیکی ارائه‌دهنده خدمات ابری، منبع نگرانی در نظر گرفته می‌شوند [۲۰].

حفاظت از داده ها در فضای ابری یک موضوع امنیتی مهم است و باید در این موضوع از نظر نحوه دسترسی، ذخیره، الزامات حسابرسی و هزینه داده ها در نظر گرفته شود [۲۱]. نقض حریم خصوصی یکی از مسائل امنیت در فضای ابری است، بنابراین از نظرمتخصصان در توسعه خدمات امنیتی و شیوه های حفظ حریم خصوصی در خدمات ابری ضروری است، یک استراتژی ارزیابی موثر که حفاظت از داده ها، انطباق، حریم خصوصی و مدیریت هویت، عملیات ایمن، و سایر مسائل قانونی مرتبط را پوشش می دهد، ارائه شود [۲۲]. در رایانش ابری، ویژگی ها و معیارهای عملکرد بین ارائه دهندگان و مشتریان از طریق توافق نامه های سطح خدمات(SLA) تعیین می شود که به مبنای قانونی خدمات و سطح کیفیت خدمات مربوط می شود [۲۴]. عدم انطباق با قرارداد سطح سرویس (SLA) توسط ارائه دهندگان خدمات ابری، علاوه بر نگرانی در مورد امنیت و محرمانه بودن داده های ذخیره شده در ابر، منجر به کاهش سرعت پذیرش و کاهش سطح عملکرد و همچنین حریم خصوصی می شود [۲۵]. توافق نامه ها، سطح خدمات و مقیاس های اندازه گیری مختلفی را بر اساس کیفیت خدمات (QoS) توصیف می کنند [۲۶]. زمانی که ابر توسعه می‌یابد، این پیشرفت با موانعی در زمینه کیفیت خدمات (QoS) مواجه است که نشان‌دهنده سطوح عملکرد، قابلیت اطمینان و در دسترس بودن امنیت است [۲۷]. این عملکرد گسترده است و شامل قابلیت اطمینان، بهره وری انرژی و گسترش است. محیط‌های رایانش ابری نیز گسترده هستند و چندین منبع ارائه‌دهنده و کاربر را ترکیب می‌کنند. در اینجا، عامل امنیتی مؤثر بر عملکرد از طریق تأثیر امنیتی بر زیرساخت شبکه وجود دارد، به عنوان مثال، در مورد حملات DDoS که تأثیر گسترده ای بر عملکرد شبکه دارند، اگر این خطر یا هر خطری که خود محیط ابری را تهدید کند، نگرانی عمده ای برای کاربران و ارائه دهندگان خواهد داشت و این حملات برای محاسبات ابری مضر هستند [۲۸]. انجام حمله در SQL به مهاجم اجازه دسترسی به پایگاه داده را می دهد. همچنین در حملات سیل، مهاجم به قدری سریع درخواست منابع را به ابر ارسال می کند تا

www.SID.ir

بتواند از منابع غیرقابل دسترس توسط کاربران عادی سوء استفاده نموده و حملات بسیاری که امنیت ابر را تهدید می کند، رخ می دهد [۲۹]. امنیت یک اولویت مهم برای مشتریان ابری است و تصمیم برای استفاده از خدمات ابری بر اساس سطح محرمانه بودن، یکپارچگی، انعطاف پذیری و خدمات امنیتی موجود، خواهد بود و این نشانه رقابت بین ارائه دهندگان خدمات است که منجر به توسعه رایانش ابری می شود [۳۰]. برخی از مشکلات پیش روی کاربران رایانش ابری از نظر دسترسی به داده ها از طریق اینترنت وجود دارد. هرگونه ضعف در سطح امنیت در فضای ابری، محرمانه بودن داده های ذخیره شده، کاربران را تهدید می کند. علاوه بر این، کیفیت اتصال بر سطح عملکرد در ارائه خدمات، هزینه بالای محاسبات کامپیوتری خصوصی در مقایسه با بخش‌های عمومی و مختلط، به هزینه کیفیت، عملکرد و امنیت تأثیر می‌گذارد [۳۱].

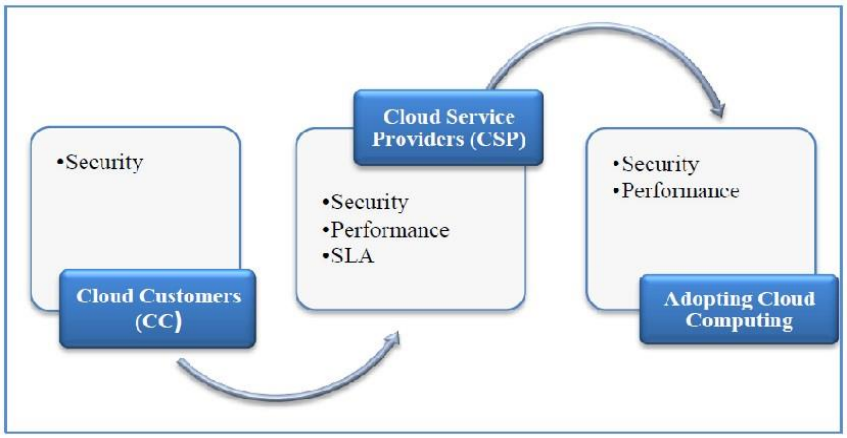
۳,۱. مخاطرات امنیتی در رایانش ابری:

سرقت داده ها و منابع اطلاعاتی، از دست دادن منابع اطلاعاتی، دزدیده شدن اکانت و ترافیک، API بی اعتبار و نا امن، خیانت همکار، استفاده غیر قانونی از سرویس ابری، اندک بودن رتبه دیجیتالی شدن، درخطر بودن فناوری هایی که به اشتراک گذاشته شده است، از مخاطرات مهم امنیتی به شمار می رود [۳۲].

۴.ارتباط امنیت و عملکرد حوزه فناوری اطلاعات در ریانش ابری

مقیاس توسعه در هر سیستم کامپیوتری بر اساس سطح عملکرد سیستم است، اما بین امنیت و عملکرد رابطه وجود دارد. عملکرد، شاخصی برای سرعت اجرا و تبادل داده ها است. در حالی که امنیت نشان دهنده محافظت در برابر تهدیدات است، هر دو از یک سو به اجزای نرم افزار و سخت افزار سیستم و از طرف دیگر به کاربر و ارائه دهنده خدمات بستگی دارند. امنیت یکی از استانداردهای کارایی در نظر گرفته می شود که در آن کارایی شاخص اصلی سطح عملکرد است، در حالی که عملکرد عنصر کمکی در حفاظت از سیستم است. در نتیجه، رابطه بین عملکرد و امنیت مکمل یکدیگر هستند و یک عامل کلیدی برای توسعه سیستم است. رایانش ابری خدماتی را از طریق ارائه دهندگان خدمات به کاربران ارائه می دهد. کاربر یک درخواست خدمات ارسال می کند، که ارائه دهنده خدمات، با ارائه خدمات، پاسخ می دهد. با این حال، این فرآیند بر اساس توافق بین دو طرف است که در پرتو آن تماس و استفاده، ساخته شده است. و این توافقنامه قرارداد سطح سرویس، SLA نامیده می شود. علاوه بر این، مسائل اجتناب‌ناپذیر دیگری نیز بین کاربر و ارائه‌دهنده خدمات وجود دارد، مانند امنیت و عملکرد سرویس، که عواملی هستند که بر پذیرش کاربر برای استفاده از خدمات ابری تأثیر می‌گذارند.

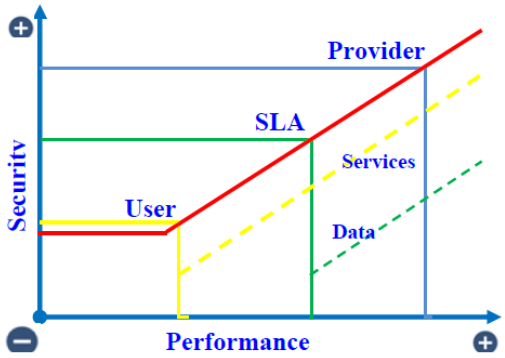
شکل ۳. رابطه بین عملکرد و امنیت در ابر



شکل۳، رابطه بین امنیت و عملکرد در ابر را نشان می دهد. امنیت و عملکرد پیش نیاز کاربر است و بنابراین ارائه دهنده خدمات موظف است، آن را در اختیار کاربر قرار دهد، در حالی که عملکرد از طرف کاربر اجباری نیست، زیرا کاربر نمی داند داده در کجا ذخیره شده است و هیچ اطلاعی ندارد. کنترل بر داده ها و امنیت برای کاربر ضروری است، با این وجود، در صورتی که کاربر از خط مشی امنیتی پیروی نکرده باشدو در صورتی که کاربر یک نقض امنیتی در فضای ابری را نشان دهد، یعنی کاربر ممکن است، باعث پایین آمدن سطح امنیت شود و این منجر به عملکرد سطح پایین خدمات می شود. همچنین اگر سطح پایین امنیت بر عملکرد تأثیر بگذارد و با توجه به مقیاس عملکرد، عملکرد بر امنیت ارائه‌دهنده خدمات تأثیر می گذارد.بنابراین امنیت و عملکرد چالش‌هایی را در فضای ابری نشان می‌دهند، زیرا هر یک، چالشی برای دیگری است. امنیت بهتر، یعنی عملکرد بهتر و عملکرد بهتر، ناشی از امنیت بهتر است و به این معنی که رابطه مثبت است.

عملکرد و امنیت برای سرویس، یک الزام در سطح کاربر و ارائه دهنده است، در حالی که داده ها در سطح ارائه دهنده مورد توافق هستند. به این دلیل است که کاربر مکان ذخیره سازی را نمی شناسد و مانند شکل (۴) کنترلی روی داده ها ندارد.

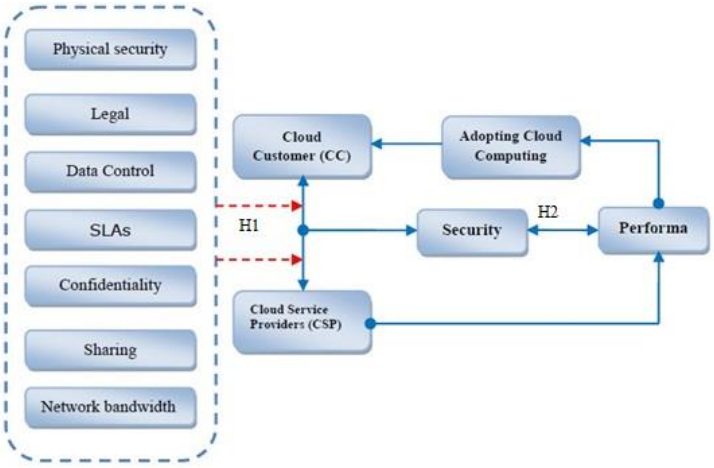
www.SID.ir



شکل ۴. سطح تأثیر بین عملکرد و امنیت در رایانش ابری

۵.مدل تحقیق

رایانش ابری در حال پیشرفت است، اما چندین عامل و چالش برای پذیرش کاربر از فناوری رایانش ابری وجود دارد. بنابراین، مدل پذیرش فناوری (TAM) به عنوان یک مدل در ایجاد مدل تحقیق، برای نشان دادن پذیرش کاربر از رایانش ابری مانند شکل (۵) در نظر گرفته می‌شود. [۳۳].



عملکرد و امنیت به عنوان عوامل و چالش‌های اساسی در نظر گرفته می‌شوند که بر پذیرش فناوری محاسبات ابری توسط کاربر تأثیر می‌گذارند.

H1: امنیت بر عملکرد تأثیر می گذارد که به سطح امنیتی بالا یا پایین بستگی دارد .تأثیر سطح امنیت توسط کاربر و ارائه دهنده مورد نظر است، در این صورت امنیت سطح بالا، منجر به افزایش سطح عملکرد محاسبات ابری می شود، جایی که سطح امنیت به عوامل خارجی از جمله خطرات امنیتی، محرمانه بودن داده ها، توافق سطح خدمات و امنیت فیزیکی بستگی دارد.

H2: سطح عملکرد ارائه دهنده خدمات برسطح امنیت تأثیر می گذارد .در صورت عملکرد سطح بالا، منجر به بالا بردن سطح امنیتی رایانش ابری می شود، جایی که این سطح عملکرد به عوامل خارجی مانند تهدیدات امنیتی، محرمانه بودن داده ها، قوانین و مقررات، توافقنامه سطح خدمات و خط ارتباطی بستگی دارد.

۶.نتیجه گیری

رابطه بین عملکرد و امنیت یک رابطه مثبت است. امنیت بر عملکرد تأثیر می گذارد و از سوی دیگر سطح عملکرد کاربر، ارائه دهنده و اجزای ابر، بر امنیت تأثیر می گذارند وهمچنین بر اعتماد مشتری در پذیرش ابر تأثیر گذار هستند و از آنجا که امنیت به عنوان یک چالش بزرگ در پذیرش محاسبات ابری در نظر گرفته می شود مانع بزرگی است که شرکت ها را از پذیرش محاسبات ابری باز می دارد، زیرا یک ابر با زیرساخت ناامن می تواند منجر به مشکلاتی بین پذیرنده و متخصصانی مانند مشتریان، شرکا، ارائه دهندگان فناوری اطلاعات یا حتی دولت ها شود .در این میان سطح خدمات در رایانش ابری که متاثر از سطح عملکرد می باشد و سرعت و کیفیت خدمات است که منجر به رضایت کاربر و اتخاذ ابر برای استفاده از سرویس الکترونیکی آن می‌شود و این شاخصی است که بر توسعه و پیشرفت ابر تأثیر گذاشته و با توجه به این موضوع، سطح امنیت و عملکرد به عنوان یک چالش که میتواند مانعی برای پیشرفت در توسعه رایانش ابری است، باید در نظر گرفته شود.

www.SID.ir

Arch

منابع

[1] https://csrc.nist.gov/projects/cloud-computing
[2] http://www.businessofsoftware.ir/257/cloud-computing-definition/
[3] Anurag S. Barde, (2013) "Cloud Computing and Its Vision 2015!!" International Journal of Computer and Communication Engineering, Vol. 2, No. 4.
[4] Chang, V, "Delivery and Adoption of Cloud Computing Services in Contemporary Organizations" Information and communication sciences", IGI Global, 2015.
[5] Four Key Elements of a Secure, High-Performance Hybrid Cloud Networking Strategy Delivering an optimized bridge to the cloud with Citrix Cloud Bridge, Cloud Bridge White Paper 2012. https://www.citrix.com.
[6] Secure, private, and trustworthy: enterprise cloud computing with Force.com, White Paper2013.
[7] Malvinder Singh Bali & Shivani Khurana, (2013)" Performance Analysis of Cloud Computing under the Impact of Botnet Attack", Proceedings in International Conference on Recent Trends in Communications and Computer Network.
[8] https://www.sciencedirect.com/science/article/pii/B978012822844900013X.
[9] Gupta & Manish, "Handbook of Research on Emerging Developments in Data Privacy ", IGI Global, 2014.
[10] Bautista L., Abran A. and April A., (2012) "Design of a Performance Measurement Framework for Cloud Computing", Journal of Software Engineering and Applications, Vol. 5, No. 2, pp 69-75.
[11] Giuseppe Aceto & Alessio Botta, (2013)" Cloud monitoring: A survey" Elsevier computer network, Vol. 57, No.9, pp 2093–2115.
[12] Niloofar Khanghahi & Reza Ravanmehr, (2013)" Cloud Computing Performance Evaluation: Issues And Challenges", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.3, No.5.
[13] Shailesh Paliwal, (2014) "Performance Challenges in Cloud Computing", https://www.cmg.org
[14] Amid, K Bardsiri & Seyyed, M Hashem, (2014) "QoS Metrics for Cloud Computing Services Evaluation", International Journal of Intelligent Systems and Applications, Vol. 6, No. 12, pp 27-33.
[15] Elisabeth Stahl & Lydia Duijvestijn and others, (2012) "Performance Implications of Cloud Computing", ibm.com/Redbooks pp 4875.
[16] Danilo Ardagna & Giuliano Casale and others (2012), "Quality-of-service in cloud computing: modeling techniques and their applications", Journal of Internet Services and Applications a Springer, Vol.5, No. 11.
[17] Technical Report," CLOUD; SLAs for Cloud services",ETSI TR 103 125 V1.1.1 (2012), http://www.etsi.org/
[18] Cloud computing in higher education a guide to evaluation and adopting- Cisco 2010. https://www.cisco.com/web/strategy/docs/education /Cloud_Computing_in_Higher_Education.pdf.
[19] Shirley Radack, (2012) "Cloud Computing: A Review of Features, Benefits, and Risks, and Recommendations for Secure, Efficient Implementations". http://www.itbusinessedge.com.
[20] April Reeve, (2013) "Managing Data in Motion: Data Integration Best Practice Techniques", Elsevier Science Technology.
[21] Avinash R. Dhok & Ashwini P. Kolhe, (2015) "A Survey on Scalable Data Security and Load Balancing in Multi Cloud Environment", IJIRST –International Journal for Innovative Research in Science & Technology, Vol. 1 , No. 8, pp 232:236.
[22] Sherin Sreedharan & G.Kalpana, (2013) "Security Issues and Solutions for Cloud Computing", International Journal of Computer Trends and Technology (IJCTT), Vol.4, No.4, pp 494-498.
[23] Nir Kshetri, (2013) "Privacy and security issues in cloud computing: The role of institutions and institutional evolution", Telecommunications Policy, vol. 37, No. 4, pp 372-38.
[24] Stefan Frey & Claudia Luthje, and Christoph Reich, (2013) "Key Performance Indicators for Cloud Computing SLAs", the Fifth International Conference on Emerging Network Intelligence, pp 60-64.
[25] Safiya Okai & Mueen Uddin and Amad Arshad, Raed Alsaqour, Asadullah Shah, (2014) "Cloud Computing Adoption Model for Universities to Increase ICT Proficiency", SAGE Open, Vol.4, No.3, pp 1-10.
[26] K. Vaitheki, (2014) "A SLA violation reduction technique in Cloud by Resource Rescheduling Algorithm (RRA)", International Journal of Computer Application and Engineering Technology Vol. 3, No.3, pp. 217-224.
[27] Danilo Ardagna & Giuliano Casale and Michele Ciavotta, Juan F Pérez and Weikun Wang, (2014) "Quality-of-service in cloud computing: modeling techniques and their applications", Journal of Internet Services and Applications springeropen.com, Vol. 5, No.11, pp 1-17.
[28] Niloofar Khanghahi & Reza Ravanmehr, (2013)" cloud computing performance evaluation: issues and challenges", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.3, No.5, pp 29-41.
[29] Sara Qaisar & Kausar Fiaz Khawaja, (2012) "Cloud Computing: Network/Security Threats and counter measures", Interdisciplinary Journal of Contemporary Research in Business, ijcrb.webs.com, January, Vol. 3, No.9, pp 1323 – 1329.
[30] Zaigham Mahmood, (2014) "Cloud Computing: Challenges, Limitations and R&D Solutions", Springer.
[31] Heru Susanto & Mohammad Nabil Almunawar and Chen Chain Kang, (2012) "Toward Cloud Computing Evolution: Efficiency vs Trendy vs Security", Computer Science Journal.
[32] هانیه هداوند میرزایی ۲۰۲۱ https://arazcloud.com/blog/cloud-computing-security
[33] Tobias Ackermann, (2012)" IT Security Risk Management: Perceived IT Security Risks in the Context of Cloud Computing", Springer Science & Business Media.

www.SID.ir