نشریه علمی-تخصصی
پژوهش های نوین علوم مهندسی
ISSN: 2538-3809
سال نهم، شماره ۱ (پیاپی: ۴۷)، بهار ۱۴۰۳

مروری بر ادبیات مسائل امنیتی در رایانش ابری: فرصت‌ها و چالش‌ها

امین محمدی کوهبنانی[1*]

تاریخ دریافت: ۱۴۰۳/۰۱/۰۳
تاریخ پذیرش: ۱۴۰۳/۰۲/۰۵
کد مقاله: ۷۷۸۶۹

چکـیده

رایانش ابری به پردازش با سازگاری بالا اشاره دارد. برنامه‌ها، انبارها و مراحل به‌عنوان کمک به سازمان‌ها، مردم و دولت‌ها. در همین راستا، انجمن‌های SMB (کسب‌وکار کوچک و متوسط) به‌طور مداوم مدیریت‌های پردازش ابری را برای صرفه‌جویی در هزینه‌ها و افزایش بهره‌وری در شرایط تجاری خود تنظیم می‌کنند. در حالی که مزایا و قدرت مدیریت ابری قابل درک است، اما اکنون نگرانی بیشتری در مورد امنیت در رایانش ابری وجود دارد "شرایط رایانش ابری چقدر ایمن است؟" متوجه شدیم که امنیت یکی از موانع اساسی برای ادامه توسعه رایانش ابری است. برای برخی از خطرات و مسائل امنیتی مهم، شرکت‌ها و افراد تمایلی به ارسال اطلاعات و برنامه‌های خود در شرایط ابری ندارند. در این مقاله، هدف اصلی شناسایی خطرات و مسائل امنیتی قابل‌توجهی است که باید در هنگام ارسال و پیشرفت مدیریت‌ها در فضای ابری در نظر گرفته شوند و مسیری برای تعدیل این خطرات و مسائل امنیتی است. با این وجود، توجه به این نکته قابل توجه است که شکل‌گیری ابر اساساً متزلزل نیست، فقط باید بر آن نظارت کرد و با خیال راحت به آن رسید.

واژگـان کلـیدی: مسائل امنیتی، رایانش ابری، فرصت‌ها، چالش‌ها، مدل تحویل.

۱- کارشناسی ارشد مهندسی کامپیوتر گرایش رایانش ابر
aminmohamadi.info@gmail.com

۱- مقدمه

شرکت‌های IT (فناوری اطلاعات) هرچند وقت یک‌بار نوآوری را به حوزه دیگری سوق می‌دهند. اینترنت یکی از اصلی‌ترین نوآوری‌های امروزی در کلاس خود است. در حال حاضر این کشور در لبه تحول است، جایی که دارایی‌ها به‌طور جهانی به هم مرتبط هستند. متعاقباً، دارایی‌ها را می‌توان به‌طور مؤثر به اشتراک گذاشت، از هر مکان و هر زمان که نظارت می‌شود. رایانش ابری مؤلفه اصلی این استاندارد است که ظرفیت بسیار زیادی را ایجاد می‌کند که در آن دارایی‌ها از هرکجا برای همه به‌عنوان کمک و نه به‌عنوان یک آیتم قابل دسترسی هستند. در طول تاریخ مهندسی نرم‌افزار، تلاش‌های مختلفی برای رهایی مشتریان از نیازهای تجهیزات رایانه شخصی (مثلاً ذخیره‌سازی) و برنامه‌نویسی انجام شده است، زیرا برنامه‌های اشتراک‌گذاری زمانی تصور شده در دهه ۱۹۶۰، سازمان‌دهی رایانه‌های شخصی در دهه ۱۹۹۰ و شکل‌گیری شبکه‌های تجاری به (محاسبات ابری) در سال‌های پایانی اضافی.

رایانش ابری درست زمانی که به آنچه فناوری اطلاعات در هر مورد نیاز دارد تمرکز می‌کند: رویکردی برای گسترش ظرفیت‌های یک چارچوب در پرواز بدون کمک هیچ پایه جدید، آماده‌سازی کارکنان دیگر و مجوز برای هر برنامه‌نویسی جدید. امروزه اداره‌های ابری کمک‌های مبتنی بر عضویت یا پرداخت به ازای استفاده را می‌دهند. دولت‌ها از طریق اینترنت در زمان واقعی ارائه می‌دهند، که در آن توانایی‌های اساسی فناوری اطلاعات به منطقه‌ای قوی گسترش می‌یابد. سازمان‌های SMB درک می‌کنند که اساساً با بهره‌گیری از شرایط ابری، می‌توانند دسترسی سریع به بهترین دفاتر برنامه‌های کاربردی تجاری را افزایش دهند و بنیاد دارایی‌های خود را با حداقل هزینه به‌شدت حمایت کنند (Jensen et al., 2009). مدیریت‌های ابری اساساً مرکز کاهش نیازهای کلی مشتری (تجهیزات و برنامه‌نویسی) و ماهیت چندوجهی هستند. از زمانی که مدیریت‌های ابری در سال ۱۹۹۰ ارائه شدند، مدل انتقال فناوری اطلاعات را برای مدیریت‌ها تغییر داده است. با توجه به‌اندازه‌گیری‌ها نشان داده شد که پیشرفت‌ها و اجرای هیولاهای مدیریت‌های تصویرسازی ابری احتمالاً بین ۱۵۰ تا ۲۲۲,۵ میلیارد دلار به‌صورت جداگانه در سال‌های ۲۰۱۴ و ۲۰۱۵ به دست خواهند آورد.

اگرچه مزایای متعددی در استفاده از پردازش ابری ارائه شده است، اما ترتیب باورنکردنی خطرات و مسائل مربوط به اجرا، عوامل اجرایی، بازیابی شکست، تطابق کسب‌وکار، دستورالعمل‌ها و قوانین و عدم وجود اصول و قوانین در نوآوری‌های رایانش ابری است (Hashizume et al., 2013). همان‌طور که توسط یک نظرسنجی IDCI در سال ۲۰۰۹ مشخص شد، ۷۴٪ از مقامات IT و CIO (مدیر ارشد اطلاعات) ذکر کردند که امنیت بهترین شکل مدیریت مالی مبتنی بر ابر است. هیئت مدیره ابری به‌طور مداوم تحت فشار برای تسکین کافی از خطرات برای کاهش نوسان در تجارت سود می‌برد (Fernandes et al., 2014).

برخی از چالش‌های امنیتی قابل‌توجهی درنتیجه محاسبات ابری ظاهر می‌شوند که در آن برنامه‌نویسی برنامه‌ها و پایگاه‌های داده به سمت ایجاد مزارع سرور بزرگ منتقل می‌شوند. رایانش ابری زمانی موردتوجه قرار می‌گیرد که به آنچه فناوری اطلاعات در هر مورد نیاز دارد فکر می‌کنید: چگونه می‌توان قدرت یک هواپیما را در هواپیما بدون نیاز به نصب پایگاه جدید به حداکثر رساند، خدمه دیگر را آماده کرد و هر سیستم جدیدی را مجاز کرد.

این مفهوم برای بسیاری از مسائل امنیتی مانند آسیب‌پذیری‌های برنامه‌های کاربردی وب، نصب و رمزگذاری SQL (زبان سیستم)، دسترسی فیزیکی و مسائل کنترل امنیتی از طرف اشخاص ثالث که کنترل بر داده‌های حساس را دارند، شخصیت و گواهی مدیران مشکل نوظهور با توجه به جزئیات اعمال می‌شود. قابلیت اطمینان و حریم خصوصی با احراز هویت تا ابزارهای پاسخگو مرتبط است. نقطه کانونی اساسی این بررسی، به تصویر کشیدن مسائل امنیتی مختلف به دلیل مدل‌های انتقال مدیریت ابری است و چند پیشنهاد برای کاهش خطرات رایانش ابری با توجه به قوانین و هنجارهای پیشرفت برای شرایط پردازش ابری ایمن ارائه می‌دهد. رایانش ابری به دلیل ترکیبی از نوآوری ثبت شبکه ایجاد شد. در اواسط دهه ۱۹۹۰، رایانه‌های شخصی نخبه از طریق اتصال سریع اطلاعاتی به یکدیگر متصل شدند تا به تخمین غیرقابل پیش‌بینی و منطقی کمک کنند. پردازش شبکه یک تجهیزات و پایه برنامه‌نویسی را مشخص می‌کند که دسترسی ثابت، اجتناب‌ناپذیر و متوسطی را به دفاتر محاسباتی برتر از طریق سازمان‌دهی ارتباطی می‌دهد.

۲- بیان مسئله

مدیریت مبتنی بر راهنمایی مبتنی بر صنعت فناوری اطلاعات، انواع مزایای وب را به‌صورت ایمن یا ناامن ارائه می‌دهد. رایانش ابری یکی از مدل‌های مدیریتی است که برای تنظیم در شرایط کسب‌وکار، امنیت رضایت‌بخشی لازم است. به مزایای وب ایمن نیاز دارد که به‌ندرت قابل دسترسی است. تدابیر امنیتی مختلف تقریباً در هر مقاله مورد بحث قرار می‌گیرد و روشی برای تفکر و کاهش آن مسائل ارائه می‌دهد. پیشگام که توسط برخی از افراد خارجی برای اطمینان از امنیت خاصی (حریم خصوصی داده‌ها، قابلیت اطمینان و دسترسی) در محیط ابری مبتنی بر PKI (چارچوب دکمه باز) معرفی شده است، امنیت ابری و کانال HTTP

(پروتکل) و XML را ارائه می‌دهد (Fernandes et al., 2014). (زبان تعارض گسترده) برای آسیب‌پذیری‌های DOS (Service Denial)، با استفاده از CTB (Cloud Trace Back)، (۲۰۱۰). دانشمندان (Chen et al., 2012) استدلال می‌کنند که سیستم مدیریت فرصت موجود برای محاسبات ابری بخشی از سازمان فناوری اطلاعات در سال ۲۰۱۰ است.

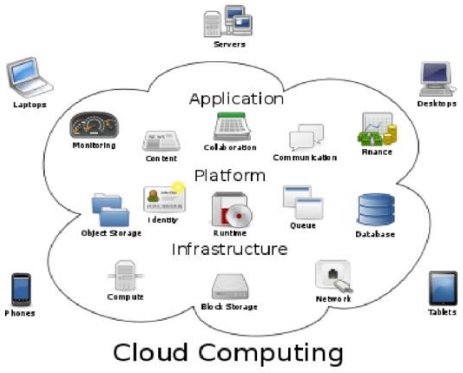
در کندو ابری و روغن هادوپ با XACML (زبان نشانه‌گذاری کنترل دسترسی توسعه‌یافته) سیستم‌های امنیتی مبتنی بر ارائه اطلاعات اولیه برای ورود به اتاق مشترک و اشتراک‌گذاری آن با ابر هستند که توسط محققان به چالش کشیده می‌شود (Tianfield, 2012). تست فناوری اطلاعات برای یافتن امنیت روزانه، حفاظت، حفاظت، راهنمایی و انعطاف‌پذیری است که در سال ۲۰۱۰ با آن مخالفت کرد (Bhadauria et al., 2011).

سازندگان زیادی وجود دارند که در چارچوب‌های مختلف با مسائل امنیتی ابری سروکار دارند، با این حال هدف، تأمین امنیت بهینه برای مدیریت ابر است. به نظر می‌رسد که هیچ‌یک از آنها آشکارا برنامه‌های استاندارد SLA (توافق سطح خدمات) را با هدف نهایی ارزیابی نمی‌کنند: آنچه مصرف کننده باید بداند و ارائه‌دهنده خدمات باید با سایر رتبه‌بندی‌های امنیتی و مدل‌های مدیریتی ارائه دهد.

۲-۱- چارچوب ساختاری رایانش ابری

محاسبات ابری مستلزم یک مدل کشف جدید امیدوارکننده است که در آن ماشین‌هایی با مزرعه‌های سرور بزرگ می‌توانند فعال، طراحی، مدیریت و برنامه‌ریزی مجدد شوند تا مزایا را به‌طور کارآمد ارائه دهند. این سیستم اطلاعات مهندسی IS است. جایی که نمایندگی به‌عنوان یک چشم‌انداز بالقوه یک ملاحظات است (Hamlen et al., 2010). همان‌طور که آن را در محاسبات ابری قرار می‌دهد، پردازش را برخلاف یک شی منتقل می‌کند. که در آن دارایی‌های اشتراک‌گذاری، سیستم‌عامل و رایانه‌های شخصی ارائه‌دهنده داده یا سایر ابزارهای الکترونیکی به‌عنوان اشیا در اینترنت در زمان واقعی استفاده خواهند شد. همان‌طور که در شکل ۱ نشان داده شده است، یک نمودار رسمی از ورود ابر رایانه وجود دارد.

در این زمینه، مدل‌های مدیریت رایانش ابری نقش عمده‌ای را در رایانش ابری و سیستم‌های عامل، محل‌های کاری، تلفن‌ها و تبلت‌ها ایفا می‌کنند که به‌عنوان مشتری برای دریافت مدیریت از ابر عمل می‌کنند. سرورها مدیریت را به مشتریان ارائه می‌دهند که با درخواست یا مبنای پرداخت آنها مشخص شده است. رایانش ابری یک مجموعه مشترک از دارایی‌های IT قابل تنظیم در صورت درخواست فراهم می‌کند، که در آن نیاز به تلاش هیئت مدیره می‌تواند نشانه‌هایی از بهبود مدیریت را نشان دهد. مدیریت مبتنی بر درک متفاوتی از SLA (توافقنامه سطح خدمات) بین سازمان‌های تخصصی و مصرف‌کنندگان است. برخی از ویژگی‌های مهم رایانش ابری مانند این وجود دارد.



شکل ۱- زیرساخت مبتنی بر ابر

۲-۱-۱- رابط برنامه‌نویسی کاربردی (API)

فعال کردن دستگاه برای اتصال به سیستم‌های ابری به همان شیوه ارتباط بین افراد / مشتریان و رایانه‌های شخصی از طریق مدیریت کانکتور.

۲-۱-۲- نگهداری

برنامه‌ها نباید با این روش ساده برای تقویت توجه به همه بخش‌های مشتری ارائه شوند.

۲-۱-۳- کارایی

مدیریت وب با استفاده از سیستم‌های دوست‌یابی رایگان و پروژه‌های قوی‌تر، کاوش چارچوب‌ها برای بهبود مدیریت ساخته‌شده است.

۲-۱-۴- مقیاس و دوام

هر تعداد هاب را می‌توان در هر زمان بدون تغییر پایه و سیستم زیاد نصب و پرتاب کرد. مشتری می‌تواند بدون عامل انسانی مدیریت لازم را به دست آورد. در بیشتر موارد قاب ابری به‌طور طبیعی نصب می‌شود.

۲- ۱-۵- دسترسی به شبکه گسترده

مدیریت‌های ابری از طریق سیستم قابل دسترسی هستند، در امتداد این خطوط یک مؤلفه استاندارد برای ارائه مزایای در مراحل ناهمگن استفاده می‌شود.

۲-۱-۶- استقلال مکان

کاربران در مورد حوزه دقیق اداره‌ها به غیر از سطح بالای مشورت به دولت‌ها، به‌عنوان مثال، ملت، دولت، آگاهی ندارند.

۲-۱-۷- قابلیت اطمینان

چندین مکان اضافی برای شرایط رایانش ابری ایجاد شده است تا به مدیریت پیشرفت و بهبود بلایا برای سازمان‌ها کمک کند.

۲-۱-۸- مقرون‌به‌صرفه بودن

بنیاد متمرکز به اشتراک‌گذاری هزینه‌ها در میانه تعداد زیادی مشتری از مناطق مشابه یا متفاوت، به‌عنوان مثال، زمین، نیرو (به‌عنوان مثال ترتیب مزایای ابری نزدیک به نیروگاه‌های متوسط) قدرت می‌دهد.

۲-۱-۹- پایداری

استفاده از دارایی مناسب برای چارچوب مؤثر.

۲-۱-۱۰- امنیت

درنتیجه یکپارچه‌سازی مزرعه سرور می‌توان سطح امنیت اطلاعات را بهبود بخشید. در حال حاضر امنیت برتر از هر یک از چارچوب‌های استاندارد است، زیرا ارائه‌دهندگان مدیریت می‌توانند نوعی راه‌حل مدیریتی را برای ارائه بالاترین امنیت ممکن ارائه دهند که بتواند هزینه‌های یک مشتری یا سازمان را به‌طور مستقل مدیریت کند. درهرصورت، زمانی که به اشتراک‌گذاری داده‌ها در سیستم گسترده‌تر سربار باشد، با استفاده از ابزارهای مختلف برای دسترسی به مدیریت، یک محیط امنیتی امن افزایش می‌یابد. درهرصورت، مدل مدیریت ابر خصوصی به سازمان کنترل بر داده‌ها یا امنیت داده‌ها را می‌دهد (Hamlen et al., 2010).

۲-۲- روش‌های مدیریت تحویل

ابری یک محیط رجیستری مبتنی بر اینترنت است که در آن کالاها، سیستم‌ها و داده‌های رایج به‌عنوان کمک به مصرف کننده (ها) در صورت درخواست خدمت می‌کنند. انواع اداری از یک سری اولویت‌های کلی پیروی می‌کنند تا مزایایی نسبت به سیستم فراهم کنند. سه مدل کمک اساسی وجود دارد، به‌عنوان مثال:

نرم‌افزار به‌عنوان سرویس (SaaS): استقرار یک برنامه کاربردی به‌عنوان یک سرویس اینترنتی از طریق یک رابط مشتری کوچک، به‌عنوان مثال، یک مرورگر اینترنت. SaaS نیاز به رایانه شخصی یا سرور مشتری برای ارائه، مدیریت و راه‌اندازی همه سیستم‌ها، به‌عنوان مثال، فیس بوک، Salesforce را به حداقل می‌رساند.

پلتفرم به‌عنوان سرویس (PaaS): انتقال یک پلت فرم مجازی به‌عنوان کمکی برای توسعه نرم‌افزار، قرار دادن فروشگاه و تسهیل اینترنت. کلاینت نیازی به کنترل چارچوب ابر مرکزی ندارد، اما کنترل استقرار سیستم‌ها را دارد، به‌عنوان مثال، WOLF (میان‌افزار ابری)، Windows Azure (سیستم عامل ابری).

زیرساخت به‌عنوان یک سرویس (IaaS): با جابجایی پایگاه به‌عنوان یک ابزار کنار هم برای برنامه‌ریزی و برنامه‌ریزی، اغلب در دسترس تر می‌شود. مدیریت بر اساس مقدار مواد استفاده شده توسط خریدار پرداخت می‌شود، به‌عنوان مثال، سرورهای مجازی استخدام شده توسط آمازون، Go Grid.

مدل‌های خدمات دیگری نیز وجود دارد که توسط سه قالب اصلی (SaaS، PaaS و IaaS) از هم جدا می‌شوند، به‌عنوان مثال، CAAS (ارتباط به‌عنوان یک سرویس)، STAAS (ذخیره‌سازی به‌عنوان یک سرویس)، DTAAS (دسکتاپ به‌عنوان یک سرویس)، ITAS (IT به‌عنوان یک سرویس)، CCAAS (محاسبه ظرفیت به‌عنوان یک سرویس) و BPAAS (فرایند تجاری به‌عنوان یک سرویس) (Hashizume et al., 2013). لایه‌های مهم طراحی محاسبات ابری مستند شده است، جایی که در مدل سرور مشتری چگونه مدیریت به‌طور مداوم ارائه می‌شود.

۲-۳- مدل‌های استقرار رایانش ابری

سه نوع اصلی از مدل‌های رایانش ابری وجود دارد، با این حال NIST (موسسه ملی استاندارد و فناوری) چهار مدل سازمانی را پیشنهاد کرد که همه آنها در فهرست درج شده‌اند (Chen et al., 2012).

ابر عمومی: در این مدل از چارچوب ابری به محیط ابری اطلاق می‌شود که به‌طور واضح و منطقی توسط یک سازمان یا متخصص خارجی برای همکاری ابری در دسترس است.

ابر خصوصی: این مدل پایه توسط یک سازمان خصوصی به‌طور آشکار نظارت و استفاده می‌شود. هدف اصلی این نوع مدل ابری حفظ سطح ایمنی و امنیت است.

ابر مشترک: این نوع مدل چارچوبی را در سازمان‌ها یا شبکه‌هایی ارائه می‌کند که یک مفهوم اساسی از پشتیبانی دارند، به‌عنوان مثال، امنیت، مکان. مدیریت توسط سازمان‌ها یا افراد خارجی نظارت می‌شود.

ابر ترکیبی: این نوع مدل سفارشی حداقل دو مدل ابری ایجاد می‌کند. آنها به هم پیوند خورده‌اند و با این حال هر یک از آنها یک‌چیز مهربان باقی می‌ماند.

۲-۴- الهام‌بخش رایانش ابری

کامپیوتر ابری یک ثبت آنلاین از ویژگی‌های جدید است که توسط تجسم ایجاد می‌شود. مدل دیگری از مدیریت فناوری اطلاعات مبتنی بر خدمات مشتری و مدیریت ارجاع را نشان می‌دهد. مجازی‌سازی شکل‌گیری یک فرم فیزیکی یا سیستمیک برخلاف فیزیکی است، به‌عنوان مثال، تجهیزات، فاز، ساختار عملکردی و قدرت ماده یا سیستم. محاسبات رایانه‌ای در فضای ابری با امکان‌پذیر ساختن یک سرور برای دریافت چندین تکالیف در یک‌زمان، نرخ استفاده بالایی را در برمی‌گیرد. فرآیند فکری اساسی برای رایانش ابری ارائه صمیمیت و دقت پلاگین ترافیک برای مزایای فناوری اطلاعات در سیستم است. در محیط کسب‌وکار، چشم‌انداز ابری کسب‌وکار به سرعت در حال توسعه برای گسترش دفاتر است. گام به گام تعداد فزاینده‌ای از افراد و سازمان‌ها با داده‌ها و اطلاعات در محیط ابری آشنا می‌شوند، به این ترتیب مسائل بزرگ مختلفی به وجود می‌آیند، به‌عنوان مثال، چه ارزشی باعث صرفه‌جویی در مدیریت آنها می‌شود، چگونه شرکت‌های تخصصی اطلاعات و کارایی را در فضای ابری ارائه می‌کنند. صرف‌نظر از اینکه کدام مشتری برای کمک تلاش کند، در حال حاضر تمایلی به ارسال کسب‌وکار خود به ابر ندارند. در آنجا، امنیت یک موضوع مهم برای کاهش سرعت توسعه رایانش ابری است. همان‌طور که توسط یک نظرسنجی اکریم به رهبری تلاش مشترک اکریم با KPMG در سال ۲۰۰۹ ذکر شد، نشان داد که ۶۳٪ از پاسخ‌دهندگان گفتند که مصرف‌کنندگان آنها به‌شدت تحت تأثیر مناطق آسیب‌دیده ابر قرار گرفته‌اند. علاوه بر این، تقریباً ۴۰٪ از کل پاسخ‌دهندگان اظهار داشتند که حملات بیشتری در مقایسه با مشتریان آنها با تخصص ویژه وجود داشته است (Tianfield, 2012). خطرات جدید و خطرات بالقوه در مدیریت خدمات ابری مورد بهره‌برداری قرار می‌گیرند. ارزیابی و درک خطرات و ریسک‌های رایانش ابری به‌منظور محافظت از چارچوب‌ها و اطلاعات در برابر خطرات مهم است. بهبود ابزارهای امنیت ابری رایانه از قبل برای اطمینان از یک محیط محاسبات ابری ایمن بسیار مهم است. خریدار ممکن است به یک رایانه ابری وابسته باشد اگر مدیریت آنها به‌اندازه کافی برای استفاده ایمن باشد. برخی از چالش‌های امنیتی وجود دارد که انتظار می‌رود برای مثال، امنیت برنامه، امنیت داده، و امنیت سهام و امنیت شناسایی‌شده با استفاده از دارایی‌های خارجی را تحت تأثیر قرار دهد.

۲-۵- مزایای رایانش ابری

ثبت‌های ابری یک عامل انعطاف‌پذیری عالی در خوشه مدیریت فناوری اطلاعات فراهم می‌کنند. مدیریت را برای مشتریان فردی، سازمان‌ها یا سازمان‌های بزرگ ارائه می‌دهد. بنابراین دفاتر فناوری اطلاعات و افراد از توسعه اپلیکیشن، آماده‌سازی، امنیت، دستیابی به تجهیزات و سیستم جدید و نگهداری و هزینه‌های به‌موقع مصون هستند. مدیریت ابری مصرف انرژی، سرمایش، ذخیره‌سازی را کاهش می‌دهد و از فضا برای مشتریان ابری یا مصرف‌کنندگان مبتنی بر ابر استفاده می‌کند. دو بخش مهم از یک

سازمان وجود دارد که باید در مورد آنها نگران بود: رفتن به پرونده سبز نهایی است. به‌طورکلی، بخش قابل‌توجهی از مزایا به‌ویژه در موارد حجم بحرانی مانند مقادیر بین ۱ تا ۱۳ قابل توجه است.

از این نمودار، احتمالاً کلید کلیدی بر روی بهینه‌سازی محاسبات ابری برای کاهش حاشیه هزینه متمرکز است. مزایای مختلف با قرار گرفتن در معرض حساس آنها به بهترین وجه ارائه می‌شود، به‌عنوان مثال، تطبیق‌پذیری، آمادگی، دارایی فناوری اطلاعات بهتر مدیران و مراکز تجاری، بهره‌وری، کیفیت و دسترسی تزلزل‌ناپذیر بالاتر، بهبود سریع، ارسال و تغییر مدیران، اجرای بهتر و موارد دیگر. تطبیق‌پذیری قابل توجه به‌هرحال، مشهود است که بهبود مکانیزاسیون، پشتیبانی و برد، امنیت و مزرعه‌های سرور IT سبز کمترین دفاتر قابل‌توجهی هستند که در بررسی‌ها کاهش یافته‌اند.

۲-۶- خطرات و مسائل امنیتی در خدمات ابری

جایی که همه‌چیزهایی که گفته می‌شود در محاسبات ابری انجام می‌شود، مزایای قدرتمندی را برای دنیای فناوری اطلاعات در رابطه با بهترین شیوه‌ها و مدل‌های مدیریتی آن‌ها فراهم می‌کند. با این حال، به‌طور کامل تائید نشده است و فرصت‌های نسبتاً کمی برای مسائل امنیت اطلاعات مانند سایر مدل‌های ارتباطی یا مدیریتی وجود دارد. کشتار ابرها تحت تأثیر مسائل امنیتی است. به این ترتیب، تعاونی‌های ویژه مسئولیت در نظر گرفتن معقول امنیت در چارچوب‌ها و اطلاعات را بر عهده دارند. مدیریت و مدیریت با تعدادی از روش‌ها و تکنیک‌ها مجاز به غلبه بر این مشکلات هستند، به‌عنوان مثال: سنجش چندگانه، ابزارهای تائید و فرآیندهای رمزنگاری، با این حال، این پیشرفت‌ها و تکنیک‌ها قطعات کمی در زمینه استفاده حرفه‌ای دارند (Bhadauria et al., 2011). به‌منظور ارزیابی و شناسایی خطرات امنیتی مربوطه مهم است، انتظار استفاده از طیف وسیعی از سیستم‌های نظارت و ارزیابی مبتنی بر ابر را داشته باشید. درک و کاهش خطرات و مسائل امنیتی در خط مقدم امنیت محاسبات ابری قرار دارد. در نقطه‌ای که داده‌ها، برنامه‌های کاربردی وب و مدیریت هنوز در فضای ابری توسط سازمان‌های تخصصی ساخته می‌شوند، کنترل آن دیگر در نقش کنترلی آنها نیست. در اینجا نیز چند مشکل کنترل رایگان برای تائید جزئیات ظاهر می‌شود.

چه چیز دیگری، بیشتر. مدیریت ابری بر اساس افزایش خطر تا حدی که اطلاعات غیرمجاز به دست می‌آید، نگرانی‌ها در مورد حفاظت از داده‌ها، مدیریت شخصیت، اطمینان، استحکام، حریم خصوصی، یکپارچگی، دسترسی، رمزگذاری، خطر کنفرانس وب (IP) به اشتراک گذاشته می‌شود. موارد IP به مصالحه‌ای که به قربانی حمله به مرکز اجازه می‌دهد اعتقاد ندارند) (Bhadauria et al., 2011)، امنیت و ایمنی فیزیکی را ترتیب دهید. مسائل مختلف دیگر فقط به موضوع جداسازی و امنیت نیاز دارند، به‌عنوان مثال، SLA (قرارداد مدیریت بین سازمان حرفه‌ای و مشتری) و مدیریت خارجی، اجراها، خطرات ادراک، عدم انطباق و ارزیابی استراتژیک و انطباق با قوانین و مقررات دستورالعمل‌ها.

مدل‌های مدیریت عملکرد ابری عبارت‌اند از SaaS، PaaS و IaaS که برنامه‌ریزی را به‌عنوان ابزار، پلتفرمی به‌عنوان مدیریت و چارچوبی را به‌عنوان پشتیبانی برای مشتریان یا مشتریان نهایی ارائه می‌دهند. همان‌طور که در "شکل ۱" نشان داده شده است، این سه سیستم کمکی کارآمدتر از یک سیستم هستند. درنتیجه، قابلیت‌های آنها به‌عنوان مسائل ایمنی و ریسک ارائه می‌شود. به این ترتیب، سازمان‌های تخصصی در مقایسه با روش‌های معمول، هیچ گزینه‌ای برای گرفتن کسری از آنها برای ارائه یک محیط امن ندارند. در این مقاله به‌وضوح مسائل امنیتی وابسته به این روش‌های مدیریت و آنچه باید برای یافتن ساختارهای مناسب فراهم شود را نشان می‌دهد.

۲-۷- مسائل امنیتی SaaS

طبق بخش SaaS، مصرف‌کننده باید به سازمان‌های تخصصی امنیت اطلاعات تکیه کند و تعاونی‌های حرفه‌ای باید با ارائه ابزار امنیتی مناسب برای تائید اطلاعات و استفاده پاسخ دهند. در این مثال مدل در فضای ابری به همراه سایر سازمان‌ها یا جمعیت‌شناسی قرار می‌گیرد. سازمان‌های ابر مجازی می‌توانند داده‌ها را در مکان‌های مختلف برای دستیابی به داده‌ها و بهره‌وری شبیه‌سازی کنند. در ارتباط با آن، برخی از مسائل امنیتی وجود دارد که به وجود می‌آید، به‌عنوان مثال، نحوه پردازش اطلاعات و کجا، چه نوع امنیت با کنترل اطلاعات و قابلیت‌ها به دست می‌آید. نکات کلید امنیتی و پیچ و مهره‌هایی وجود دارد که باید در طول سازمان‌دهی و توسعه SaaS به آنها توجه کرد که عبارت‌اند از: امنیت داده‌ها. زمانی که داده‌های نرم‌افزاری در فضای ابری قرار می‌گیرند، بازاریابان باید امنیت فیزیکی و روانی، مکانیسم‌های دسترسی ایمن و بررسی‌های امنیتی اضافی را به دلیل آسیب‌پذیری‌های امنیتی در برنامه‌ها و نگرانی‌ها در مورد عوامل مخرب، که می‌توانند از محدودیت‌های مدل امنیت اطلاعات سوءاستفاده کنند، فراهم کنند. قدرت اطلاعات بر مدیریت ابری، تائید و تائید تقلب کامل و امنیت دیجیتال نادرست را دشوار می‌کند. به اشتراک‌گذاری دارایی‌ها در حوزه‌های مختلف و ناامیدی از یکپارچگی داده‌ها از جزئیات کمی بیرون می‌آید.

۲-۸- امنیت شبکه

در فضای ابری اطلاعات وضعیت به اینترنت منتقل می‌شود، با این اقدامات امنیتی، گسترش خطوط موضوع مهمی برای حفظ فاصله خوب از نشت داده‌ها است. ردیابی بسته‌بندی یک دروازه‌باز می‌تواند از مقدار زیادی اطلاعات برای بررسی نقص در تنظیمات امنیتی شما استفاده کند. مهاجمان ممکن است برنامه‌های هک را پیدا کنند، به‌عنوان مثال، نوعی دسترسی از راه دور و افشای آسیب‌پذیری‌ها (SQL و فهرست بد). DOS (Denial of Service)، DDoS (iCloud DOS)، مرد در حادثه، حملات غیرقانونی به ارتباطات غیرقانونی و سایر حملات غیرمجاز مسائل امنیتی را فراگیر می‌کند.

۲-۸-۱- محرمانه بودن داده‌ها

مسائل مربوط به حریم خصوصی و تمایز زمانی که اطلاعات بین کلاینت‌ها، اسبابک‌ها و برنامه‌های مختلف به اشتراک گذاشته می‌شود، صورت می‌گیرد. در اینجا مدیریت انبوه و اجرای توابع مختلف (تخصیص دارایی: واحد پردازش مرکزی CPU) مراحل مختلفی از تمایز ریسک را معرفی می‌کند. پارتیشن بندی اطلاعات مبتنی بر ابر از طریق احراز هویت مشتری شناسایی می‌شود زیرا در سیستم امنیتی عادی و برنامه‌ریزی داده برای استفاده غیرمجاز از اطلاعات بسیار مهم است.

۲-۸-۲- یکپارچگی داده

حسن نیت داده تضمین می‌کند که داده‌ها فقط با اجازه دادن به چیزی حذف و تصحیح می‌شوند. با توجه به افزایش تعداد اشیاء و اشیاء ابری، تائید برای اشیاء مجاز برای برقراری ارتباط اطلاعات بسیار مهم است. در صورتی که دارایی‌های مبتنی بر ابر را بتوان به‌طور مناسب بین مشتریان متمایز کرد، در آن زمان مسائل امنیتی خاصی به‌منظور احترام به داده‌ها ایجاد می‌شود. فقدان رمزگذاری و سیستم مدیریت کلید یک هفته‌ای نیز می‌تواند باعث ایجاد یک وقفه امنیتی شود.

۲-۸-۳- دسترسی

مدیریت ابری در صورت درخواست توسط حلقه‌های دارای مجوز قابل دسترسی است، صرف‌نظر از اینکه سایر موارد مجاز به کار نادرست یا نقص امنیتی هستند. برای ارزیابی دسترسی برای فروشندگان SaaS، آنها باید روند اعتبار سنجی را بررسی کنند و مسائل کمبود برد را تنظیم کنند. مسائل مختلفی نیز باید در نظر گرفته شود، به‌عنوان مثال، محدودیت‌های مدیریت اطلاعات و داده‌ها، ظرفیت انتقال و سرعت دسترسی به سیستم در مدیریت ابری.

۲-۸-۴- مکان داده‌ها

در مدل SaaS، مشتریان نمی‌دانند اطلاعات آنها کجا و در کجا زندگی می‌کند. موارد کمی برای سازمان‌های خاص با قوانین حفاظت از داده‌ها در کشورهای مختلف تبدیل می‌شود. در این راستا، این مدل مدیریتی باید برای نشان دادن امنیت اطلاعات بر اساس مسائل محلی آماده باشد. کنترل دسترسی بسیاری از سازمان‌های SMB اطلاعات نمایندگان خود را در پایگاه داده ابری ذخیره می‌کنند.

سازمان‌ها رویکردهای خاص خود را برای دسترسی یا استفاده از اطلاعات وابسته به محصور شدن مشتری خود دارند. در امتداد این خطوط، زمانی که یک کارگر ترک می‌کند و به‌صورت محلی در دسترس است، کلاینت‌های SaaS باید به یاد داشته باشند که حساب مشتری را توانمند یا ناتوان کنند، در غیر این صورت ممکن است گسست امنیتی رخ دهد. تعاونی‌های متخصص SaaS باید برای پیروی از رویکردهای سازمان‌ها در فضای ابری سازگاری ارائه دهند تا از وقفه‌ای در اطلاعات توسط مشتریان تائید نشده دوری کنند.

۲-۸-۵- مسائل امنیتی PaaS

انگیزه اصلی این مدل بررسی جزئیات است. در این مدل، یک سازمان حرفه‌ای کنترل قابل‌فهمی را بر روی، به‌عنوان مثال، مرحله OS (سیستم عامل)، برنامه‌های توسعه سیستم و زمینه ظرفیت فراهم می‌کند و سیستم عامل یا سیستم را از طریق دارایی‌ها بالاتر از فاز ابزار قرار می‌دهد. با این حال، مگر اینکه کنترل بیشتری به مصرف‌کنندگان داده شود، در عین حال نیاز به تفکر و مدیریت سایر مسائل امنیتی تحت سطوح ورودی دارد، به‌عنوان مثال، سیستم و وقفه‌های خصومت. شرکت‌های حرفه‌ای باید از استفاده نادرست از خاموشی اطمینان حاصل کنند و اطلاعات در بین برنامه‌های مختلف در دسترس نباشد. بخش دیگری از مسائل امنیتی نیاز به فکر کردن در مورد آن پشته‌ای دارد که برای عبور از دسته‌های خاص برطرف می‌شود. آسیب‌پذیری‌ها در محیط

محاسبات ابری توسط برنامه‌های کاربردی مرتبط با وب و نرم‌افزار مهندسی برنامه‌ریزی مبتنی بر سیستم (SOA) شناسایی می‌شوند. ظاهراً سیستم‌های SOA به‌صورت منطقی و در فضای ابری مستقر می‌شوند.

۲- ۸- ۶- مسائل امنیتی IaaS

تفکر ابری که توسعه مجازی‌سازی را یکپارچه می‌کند، راه جدیدی برای ارائه مدیریت بهتر فناوری اطلاعات به مصرف‌کنندگان است. با توجه به معرفی مجازی‌سازی جدید، برخی از مسائل امنیتی را برای آموزش ارائه‌دهنده اطلاعات به‌منظور توجه کمتر به محیط مجازی نشان می‌دهد. مسائل امنیتی مختلفی برای انتقال مدل‌ها به IaaS ایجاد می‌شود. محیط ابر خصوصی در مقایسه با فضای ابری باز خطرات امنیتی کمتری دارد. نمای ابری به‌طور خاص برای اینترنت طراحی‌شده است، بنابراین هرگونه مشکل و خطر امنیتی با اینترنت مواجه است، زیرا مدیریت ابر باید حفظ شود. این بنیاد برای دارایی‌های ابزار، جایی که اطلاعات در آن زندگی می‌شود یا آماده می‌شود، آماده نیست، بلکه علاوه بر این، نحوه انتقال اطلاعات از رسانه به منبع از طریق سیستم باز است. چند پیامد احتمالی وجود دارد که اطلاعات را می‌توان با دستور زبان یا چارچوب هدایت کرد.

۲- ۸- ۷- حذف خطرات ایمنی

با برنامه‌ریزی، هیچ پاسخ امنیتی کاملی برای تائید اطلاعات و برنامه‌ها یا مدیریت وجود ندارد، اما مدیریت ریسک خوب می‌تواند خطر را کاهش دهد. در این مقاله، شما چند روش، متدولوژی و چند دستگاه را برای کاهش ریسک اطلاعات و استفاده از آن در روز روشن یا در فضای ابری خصوصی و ترکیبی از هر دو (متقاطع) بیان کرده‌اید.

۲-۸-۸- امنیت و کنترل داده‌ها

داده‌های مبتنی بر ابر باید به شکل‌های مربوطه مشاهده و نمایش داده شوند. سازمان‌های حرفه‌ای باید غذای کافی برای بستن، شناسایی و واکنش نشان دهند که توسط یک استراحت ایمنی جداگانه مشخص شده است. بررسی‌های منطقی و مدیریت رژیم‌های لجستیکی به‌طور منظم انجام می‌شود. درهرصورت، آزمایش‌های قانونی لازم وجود دارد که به دلیل اطلاعات بد سازمان‌ها، برای سازمان‌ها برای وقفه‌های امنیتی ضروری نیست. سازمان‌های حرفه‌ای باید مدیریت مستقیم (کنترل، امنیت و عملیات) را به مشتریان ارائه دهند.

۲-۸-۹- امنیت شبکه

چارچوب ایمن برای بستن تغییرات غیرمجاز و دسترسی به اطلاعات از طریق استفاده از راه‌اندازی یا دسترسی فایروال و امتیازات دسترسی. شرکت‌های حرفه‌ای نیز باید چند آزمایش انجام دهند و با استفاده از ابزارهای امنیتی با کیفیت ناامن، به‌عنوان مثال، SSL، سازمان‌دهی مدیران و جستجوهای بسته، موافقت کنند تا از اجرای یک جلسه قدرتمند و دسترسی به اطلاعات احراز هویت مشتری جلوگیری کنند. برای اطمینان از ترافیک اطلاعات، چند استراتژی باید در انتقال و در رویکرد سه لایه نشان داده شود. علاوه بر این، تعامل بین مشتریان مختلف و ارائه‌دهندگان مدیریت ابر نیز باید تنظیم شود.

۲-۸-۱۰- حریم خصوصی و یکپارچگی داده‌ها

برای جلوگیری از افشای غیرقانونی و اصلاحات اطلاعات، باید فرآیند تائید و تائید مناسب انجام شود. توسعه در مدل‌های مدیریتی و سازمانی باید برای توسعه‌دهنده واضح باشد تا استفاده از اطلاعات را تضمین و به حداقل برساند. پارامترهای امنیتی با شناسه‌های مناسب برای اطلاعات و ساختارهای رمزنگاری امن باید به‌صورت پولی انجام شوند، به‌عنوان مثال، یک تبادل کلید امن می‌تواند توسط RAS استفاده شود و اندازه کلید رمزگذاری باید به‌عنوان نشانه‌ای از نیاز آن به امنیت داده یا عملیات در نظر گرفته شود.

۲-۸-۱۱- داده‌ها و در دسترس بودن خدمات

سرعت اینترنت (سرعت انتقال) و در دسترس بودن باید در هنگام انتقال و استفاده از سیستم در نظر گرفته شود. متخصصان برنامه که نماینده برنامه هستند باید گزینه غربالگری بار یا ترافیک را برای تنظیمات رسمی بار و انتقال داده از طریق سیستم داشته باشند. استراتژی‌های تکثیر اطلاعات و استراتژی‌های تلفیق نیز باید استاندارد شده و شواهد قابل تحقیق در فرآیند به‌روزرسانی اطلاعات، ازجمله دقت و ویژگی در طول زمان، ارائه کنند.

۲- ۸- ۱۲- کنترل دسترسی

ارائه‌دهندگان خدمات باید نشان دهند که دارای یک جزء امنیتی کافی برای اطمینان از عدم مجاز بودن آنها هستند. هر ورودی یا تغییر در مدیریت ابری (دارایی‌ها و اطلاعات) باید گزارشی غیرقابل‌انکار از موفقیت‌آمیز بودن آن یا اینکه شما کوتاه آمده‌اید و با نگاهی به ساختار کلی تحقیق می‌کنید، ارائه دهد. ایجاد پروفایل مشتریان معتقد به معانی و فعالیت‌های آنها بستگی دارد. مدیریت نمایش و سیستم امنیتی دسترسی باید در زمان سفارشی خود نمایش داده شود و دیده شود.

۲- ۸- ۱۳-پیشنهادات

پیشرفت‌ها در تشخیص ابر با رویکردی متفاوت بسته به مدل‌های کمک و پیکربندی متفاوت مشخص می‌شوند. این یک پیشرفت است که در آن زمینه ارتقاء می‌یابد و بخش دیگری از خطرات امنیتی کاهش می‌یابد و قطعاً مسائل جدیدی ایجاد می‌شود. با کنترل‌های امنیتی مناسب، تمام مسائل ناشی از همه موضوعات (فروشندگان و خریداران) باید به‌وضوح ارزیابی شوند. درهرصورت، پس از بررسی برخی مقالات متوجه می‌شوید که چند جنبه مهم وجود دارد که باید بر امنیت در محیط محاسبات ابری متمرکز شود.

۱. هر جزء در ساختار ابر باید در مقیاس کوچک‌تر و بزرگ‌تر شکسته شود.

۲. یک برنامه کاربردی بر روی یک ماشین مجازی اجرا می‌شود، (به‌عنوان مثال، ماشین مجازی جاوا JVM) به این معنی نیست که برنامه بر روی یک محیط ابری اجرا می‌شود. درنتیجه، قبل از بهینه‌سازی محیط ابری، برنامه باید با تکنیک‌ها و داده‌های تست مناسب آزمایش شود.

۳. مشتریان باید با سازمان‌ها / فروشندگان خدمات ابری بررسی کنند زیرا آنها انواع مدیریت را بسته به هزینه‌های اداری، کارایی و ساختارهای امنیتی و مسائل خاص مختلف نشان می‌دهند.

۴. همه سازمان‌های حرفه‌ای باید یک ارزیابی استاندارد ریسک و اطمینان و ارزیابی برای مقابله با آن ارائه دهند.

۵. SLA ها (توافقنامه‌های سطح خدمات) باید در مورد بررسی‌های امنیتی ناامن و اطمینان در برابر خطر واقعی توصیه کنند.

۶. تائید اطلاعات و استفاده از آن به شایستگی آنها بستگی دارد، همه اطلاعات موجود در فضای ابری نباید تائید شوند، به‌عنوان مثال انتظار می‌رود اطلاعات دولتی و مجاز در مقابل اطلاعات باز یا نادرست به‌کندی پیش برود. قابل‌ذکر است که امنیت بر انتقال و تولید داده‌ها تأثیر دارد.

۷. (DDOS) امتناع توسط مدیریت یک موضوع مهم در برنامه‌ریزی است. تعداد کمی از دانشمندان باید نحوه کاهش خطر را راهنمایی کنند.

۸. در مدل‌های امنیت ابری کامپیوتر هیچ استاندارد یا ساختاری برای سازمان‌ها و مصرف‌کنندگان تخصصی وجود ندارد. برای ایجاد ابزارهای امنیتی استاندارد، قطعات و رویه‌هایی که همه فروشندگان و خریداران باید از آنها پیروی کنند. علاوه بر این، در صورتی که تاجران نیاز به اجرای تدابیر امنیتی داشته باشند، ممکن است در آن زمان به آنها اجازه دهند تا کنترل‌های خود را اعمال کنند.

۹. مشخص شده است که، همه مجموعه‌ها باید به قوانین و معیارهای خاص برای محیط‌های ابری ایمن، به‌عنوان مثال، قانون ابری NIST برای امنیت و حفاظت از محاسبات ابری باز پایبند باشند (Kshetri, 2013).

بدون یک مدل امنیتی ابری مناسب، مشتریان بالقوه هیچ گزینه لمسی برای گرفتن امتیاز متمرکز بر توسعه ابر رایانه‌ای نخواهند داشت. در آینده به دور از یک مؤلفه احراز هویت مشترک و فرآیند ایمن برای انتقال داده‌ها به مدیریت ابری.

۳-نتیجه‌گیری

مدل محاسبات ابری می‌تواند مدیریت و دارایی‌های مجازی را در صورت درخواست افزایش دهد. با در نظر گرفتن چارچوب استاندارد کلاستر، مدیریت ابر تنظیمات زیادی را ارائه می‌دهد. هیچ حدس و گمان بزرگی برای تازه کردن پایه، کار و پیگیری هزینه‌ها لازم نیست. درست است، زمانی که کالا در حال استفاده نیست، هزینه تقریباً صفر است (پرداخت به ازای استفاده). بقیه مقاله آشکارا در مورد خطرات و مشکلات امنیتی با دیدگاه‌های مختلف صحبت کردند، به‌عنوان مثال، CIAA (محرمانه بودن، یکپارچگی، در دسترس بودن و احراز هویت) و همچنین مسائلی که توسط مدل‌های مختلف انتقال خدمات شناسایی شده‌اند، به‌عنوان مثال، DOS، امنیت ویرایش، اطلاعات امنیت، و مدل‌های SaaS، سیستم و مدیریت وقفه در PaaS و IaaS نه‌تنها به این فکر می‌کنند که در کجا از اطلاعات استفاده می‌شود و همچنان کار می‌کند و رسانه‌ها را برای انتقال داده‌ها با استفاده از اینترنت آزار می‌دهد. کاهش ریسک و ریسک جزء مهمی از این مقاله است که در آن رویکردی مفهومی برای کاهش ریسک‌ها ارائه کرده‌ایم، به‌عنوان مثال، با استفاده از کنترل رسمی کشف، نظارت، نظارت و یک ابزار رایج امنیت اطلاعات درنهایت، چند

پیشنهاد بر اساس شرایط مالی ارائه می‌کنیم. اسناد و مدارک مختلف از اواخر. در این راستا، رایانش ابری به‌اندازه کافی بزرگ نیست، درنتیجه بسیاری از سؤالات تجاری به سمت رایانش ابری حرکت می‌کنند. نام‌گذاری ابری هنوز به‌عنوان یک تجربه مشتری است.

منابع

1. Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2011). A survey on security issues in cloud computing. arXiv preprint arXiv:1109.5388, 1-15.
2. Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. Paper presented at the 2012 international conference on computer science and electronics engineering.
3. Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014). Security issues in cloud environments: a survey. International journal of information security, 13, 113-170.
4. Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security issues for cloud computing. International Journal of Information Security and Privacy (IJISP), 4(2), 36-48.
5. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of internet services and applications, 4, 1-13.
6. Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). On technical security issues in cloud computing. Paper presented at the 2009 IEEE international conference on cloud computing.
7. Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37(4-5), 372-386.
8. Tianfield, H. (2012). Security issues in cloud computing. Paper presented at the 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC).