رایانش ابری: فناوری، مسائل امنیتی و راه‌حل ها

چکیده

مفهوم رایانش ابری را می‌توان تقریباً از وسط قرن گذشته بررسی کرد. پارادیم ابر امکاناتی همچون مقیاس‌پذیری، قا رذذۀبلیت حمل، مستقل بودن از پلت10فرم، حضوری در همه‌جا، انعطاف‌پذیری در اشتراک‌گذاری، قابلیت پایداری و //رایانشی تقریباً همگانی را فراهم ساخته است. رایانش ابری به‌عنوان یک راه‌حل تنها نرم‌افزاری یا بر اساس سخت‌افزاری پیشرفته که توسط فناوری مجازی‌سازی پشتیبانی شده است پیاده‌سازی گشته است. در این مقاله ما فناوری اساسی که پشت رایانش ابری است را ارائه می‌دهیم. رایانش ابری به‌عنوان یک مدینه فاضله برای حل بسیاری از چالش‌های زمان فعلی مطرح‌شده است. اما در عمل، امنیت یک مانع اصلی برای پذیرش آن به شکلی گسترده است. در این مقاله در مورد مسائل امنیتی رایانش ابری بحث خواهیم کرد. علاوه بر این در این مقاله راه‌حل‌های امنیتی برای مجازی‌سازی و وب‌سرویس‌ها را توضیح خواهیم داد که این دو مورد دو فناوری اصلی توانمندسازی رایانش ابری هستند. همچنین در این مقاله مفهوم جدیدی از ادغام امنیت چند سطحی در تمامی ابرها توضیح و ارائه‌شده است که در تقابل با مفهوم امنیت به‌عنوان یک سرویس است. درنهایت در این مقاله به دستورالعمل‌های مهمی برای توسعه موافقت‌نامه‌های سطح سرویس اشاره‌شده است.

کلمات کلیدی: ارائه‌دهندگان خدمات ابر، تولیدکنندگان و مصرف‌کنندگان، چهارچوب فناوری رایانش ابری، هایپروایزر (Hypervisor)، ناظر ماشین مجازی VMM، ماشین مجازی VM، مسائل امنیتی ابر، امنیت یکپارچه‌شده چند سطحی، توافقنامه سطح سرویس SLA.

1. مقدمه

پارادیم رایانش ابری دارای مشخصاتی است که تقریبا از اواسط قرن گذشته پیش‌بینی شده بود. رایانش ابری به ما مقیاس‌پذیری یا انعطاف‌پذیری رایانشی را بر روی محدوده تقریبا کاملی از دستگاه‌های محاسباتی ارائه می‌دهد، از تمامی فناوری‌های نرم‌افزاری و ابزارهای موجود و قدیمی پشتیبانی می‌کند و از طریق شبکه‌ای متمایز خدمت‌رسانی می‌کند و از این نظر مستقل از پلتفرم، قابل حمل و در همه جا حاضر است. به طور مشابهی توانایی خدمت‌دهی در حین تقاضا، به اشتراک‌گذاری و قابلیت سفارش منابع محاسباتی قابل پیکربندی و همچنین انصراف از آن‌ها را به دلیل انعطاف‌پذیر بودن دارا است، قابلیت پایداری و رایانشی تقریباً همگانی از جمله سایر ویژگی‌های رایانش ابری است. رایانش ابری سرویس‌هایی را در سه دسته اصلی ارائه می‌کند که به شکل نرم‌افزار به عنوان یک سرویس (SaaS) ، پلتفرم به عنوان یک سرویس (PaaS) و زیرساخت به عنوان یک سرویس (IaaS) است [1]. SaaS اشاره به سرویس‌های برنامه‌های کاربردی نرم‌افزاری دارد، PaaS اشاره به سرویس‌های زیرساختی برنامه‌های کاربردی دارد و در نهایت IaaS اشاره به سرویس‌های زیرساخت سیستمی دارد. پیاده‌سازی آن تحت چهار طرح ابری خصوصی، گروهی، عمومی و ترکیبی است [1].

رایانش ابری به عنوان یک مفهوم رسمی یعنی پردازش را به زندگی روزمره افراد بیاورد یعنی هر شخصی دارای یک دستکتاپ مجازی بر روی ابر دارد. و همانطور که می‌دانید جهان گشنه به منابع است و اکنون با زمان سختی مواجه است تا بتواند منابع خود را برای نیازهای رو به رشد محاسباتی مانند مفهوم شهرهای هوشمند و عملیات آن [2] تخصیص دهد و به تکامل داده‌های حجیم بپردازد. قابلیت پیاداری فناوری اطلاعات نیز بیش از پیش مورد پرسش قرار گرفته است [3]. رایانش ابری مانند یک گلوله نقره‌ای است که برای مواجه با طیف وسیعی از چالش‌های کنونی جهان مورد استفاده قرار می‌گیرد. احتمالا تنها مانع یا بلوک در مسیر این نوش‌دارو تهدیدات امنیتی یا مشکل در دسترسی به کدی کاملا تایید شده است.

بازار خدمات ابر عمومی در حدود 175 میلیارد دلار در سال 2015 بوده است و انتظار می‌رود که تا حدود 16. 5 درصد در سال 2016 رشد داشته باشد [4]. این نشان از قابلیت پذیرش عموم نسبت به ابر عمومی است. مزایای رایانش ابری چند بعدی هستند مانند اقتصادی، عملیاتی، کسب و کار و فناوری. انگیزه‌های اخذ این فناوری شامل

عوامل مختلفی مانند سود مالی به دلیل پرداخت هزینه آن به ازای استفاده، عدم تعهد طولانی مدت به ارائه‌دهندگان سرویس، سهولت در اجرا و مدیریت منابع فناوری اطلاعات و ارتباطات ICT، مقیاس‌پذیری به دلیل ادغام مراکز داده‌ها، استفاده بیشتر از منابع به دلیل محیط چند مستاجری آن (به اشتراک‌گذاری) و مجازی‌سازی آن [5] از جمله این دلایل است.

از سویی دیگر، موانع متعددی برای اخذ ابر در مقالات ارائه شده است. مطالعه [6] موانعی را پس از بررسی 95 صنعت و شرکت کوچک و متوسط (SME) ارائه کرده است. اولین و مهم‌ترین مانع آن به دلایل امنیتی با توجه به کل خود پارادیم بوده است مانند حملات شبکه‌ای. سایر نگرانی‌های امنیتی مانند محرمانگی، قابلیت اطمینان، درستی و در دسترس‌پذیری از اولویت‌هایی هستند که در رایانش ابری باید به آن‌ها اهمیت داد. امروزه داده‌ها دارای موقعیتی یکسان مانند منابع مادی هستند و در تمامی پردازش‌های دیجیتالی‌شده سازمانی بدون چشم‌پوشی از دقت، حریم خصوصی و مالکیت مورد نیاز است. داده‌ها همچنین برای برآورده‌سازی محرمانگی و الزامات قانونی ملت‌های مختلف نیز مورد نیاز است. و در زیرساخت‌های ICT چند حزبی و بین کشوری، اطمینان از دقت داده‌ها یک بازدارنده قوی برای متقاضیان بالقوه ابر است. به همین ترتیب فقدان مورد کسب و کار قوی با تجزیه و تحلیل سود و هزینه و مشکل در تعویض ارائه‌دهندگان خدمات به عنوان موانع در[6] ذکر شده است.

بنابراین، زمانی که مزایایی آشکار در ابرهای عمومی وجود دارد، طبیعی است که نگرانی‌هایی واقعی نیز در مورد امنیت، حفظ حریم شخصی و کنترل داده‌ها، دسترس‌پذیری، مقیاس‌پذیری، عملکرد و بهره‌وری هزینه‌ای از زیرساخت‌های ابرعمومی نیز به دلیل تلاش مستمر ارائه‌دهنده سرویس ابر عمومی وجود داشته باشد. هدف از این مطالعه موارد زیر است:

- فناوری زیرساختی رایانش ابری و نهادینه‌سازی آن.
- تهدیدات امنیتی موجود در رایانش ابری.
- راه‌حل‌های امنیتی اتخاذ شده توسط جامعه رایانش ابری.

این مقاله به پنج بخش تقسیم می‌شود. بخش اول که مقدمه است، در مورد مفهوم اصلی ابر مطالبی را ارائه می‌دهد، از جمله مزایا و موانع اتخاد ان و اهداف این مطالعه. بخش دوم، فناوری رایانش ابری نام دارد، و اجزای مهم فناوری که سبب فعالیت رایانش می‌شود و مدل پیاده‌سازی آن‌ها را ارائه داده است. بخش سوم، تهدیدات امنیتی رایانش ابری نام دارد، به بررسی کارهای پیشین این حوزه می‌پردازد تا ریسک‌های امنیتی فراگیر را در فضای ابرهای عمومی شناسایی کند و یک چهارچوب طبقه‌بندی خطرات امنیتی را ارائه دهد. بخش چهارم، راه‌حل امنیت ابری است و در مورد اهمیت دستورالعمل و چهارچوب‌هایی برای ایمن‌سازی مجازی‌سازی و وب سرویس‌ها بحث می‌کند. در این بخش همچنین یک مفهوم جدید چند سطحی ادغام شده از مفاهیم امنیت ابری ارائه شده است و دستورالعمل مهمی برای طراحی سند توافق‌نامه‌های خدماتی است. در نهایت در بخش پنجم به جمع‌بندی این مقاله خواهیم پرداخت.

2. فناوری رایانش ابری

تکامل رایانش ابری را می‌توان از زمان ارائه مفهوم مجازی سازی و بی واسطگی که در سال 1980 ارائه شد دنبال کرد [7] یا حتی در اواخر 1950 که مفهوم حافظه مجازی [8] مطرح شد. مجازی‌سازی در زمینه رایانش ابری اشاره به میزبانی یک‌پارچه و یکنواخت از منابع سخت‌افزاری متنوع برای سیستم مهمام و نرم‌افزارهای کاربردی دارد. رایانش ابری تکیه بر اجزای مهمی با نام هایپروایزر دارد که تسهیلاتی است که سبب به اشتراک‌گذاری سخت‌افزار از طریق یک یک تغییر ظاهر معروف با نام مجازی‌سازی می‌شود. به طور کلی دو نوع هایپروایزر وجود دارد، که آن‌ها را با نام ناظر ماشین مجازی (VMM) نیز می‌شناسیم. گونه 1 یا هایپروایزر ماشین لخت/فلز لخت Bare Machine/Metal () بر بالای سخت‌افزار اجرا می‌شود و سیستم‌عامل‌های گوناگون یا ماشین‌های مجازی (VM) را مدیریت می‌کند. هایپروایزر گونه 2 که به آن هایپروایزر وابسته نیز گفته می‌شود بر بالای سیستم‌عامل اجرا می‌شود و به مدیریت VMهای مختلف مانند فرآیندها می‌پردازد. چندین هایپروایزر در بازار وجود دارد مانند Xen, VMware ESX and ESXi, Microsoft HyperV, Citix XenServer, Redhat KVM, Oracle VM Server وجود دارد.

هایپروایزر گونه2 در اکثر حلقه حافظه ویژه 0 اجرا می‌شود که در آن سیستم‌های عامل مهمان یا VMها برای حلقه‌های حافظه‌ی بالاتر مانند 1 اجرا می‌شود [8]. و VMM به عنوان میزبان سیستم‌عامل برای سایر سیستم‌های عامل مهمان عمل می‌کند و منابع CPU، حافظه، هارد دیسک و پهنای باند را به هر VM تخصیص می‌دهد. اگرچه برای دستیابی به نرم‌افزاری منحصر مجازی‌سازی، نیاز به تغییر در کدهای سیستم‌عامل داریم. این امکان که به عنوان فرا مجازی‌سازی (paravirtualization) شناخته می‌شود، تنها در سیستم‌های منبع باز امکان پذیر است. امکان دیگر برگردان باینری یا پچ کردن است و می‌توان آن را بر روی سایر سیستم عامل‌های اختصاصی که کدهای آن در دسترس نیستند اعمال نمود.

نرم‌افزار منحصر مجازی‌سازی دارای چندین معایب است از جمله ناصافی حلقه‌های خافظه و خرابی سیستم‌عامل مهمان که به دلیل بازسازی ناقص مفهوم رخ می‌دهد، برای موارد بیشتر می‌توان به [8] مراجعه کرد. بنابراین پشتیبانی مجازی‌سازی سخت‌افزاری مانند عملیات ریشه‌ای و عملیات غیرریشه‌ای، مشکل نرم‌افزار منحصر مجازی‌سازی را حل می‌کند. در این سناریو VMM و سیستم‌عامل مهمان یا VM هر دو بر روی حلقه‌های حافظه مورد نظر خود اجرا می‌شوند. اما کنترل آن همچنان بر عهده VMM باقی می‌ماند و توسط عملیاتی در سطح ریشه در مقابل VM اجرا می‌شود که VM در سطح غیر ریشه‌ای عمل می‌کند. بدین شکل نیازی به فرا مجازی سازی یا برگردان باینری (پتچ کردن) وجود ندارد و سیستم عامل مهمان به شکل محصولی نرم‌افزاری با تولید انبوه مورد استفاده قرار بگیرد.

گونه 1 یا هایپروایزر ماشین لخت/فلز لخت(Bare Machine/Metal) بر خلاف گونه 2 به شکل مستقیم بر روی سخت‌افزار اجرا می‌شود. این گونه سبب فراهم‌سازی محیطی سخت‌افزاری برای سایر سیستم‌عامل‌های مهمانی می‌شود که در بالای آن‌ها اجرا می‌شود. آن‌ها معمولا به شکل یک سیستم‌عامل هستند و دارای اجزایی هستند که در ادامه به آن‌ها اشاره می‌کنیم: هسته (بوت و حافظه و مدیر زمان‌بندی) بخش غیر حافظه‌ای (مدیر باس، رابط ورودی خروجی، شبیه‌سازی پردازنده‌ها، و ترجمه بلاک کد در حال اجرا) و بخش مدیریت (پیکربندی، ورود به سیستم، و مدیریت پچ داغ) است [7].

در لایه بالاتر، مفهوم معماری سرویس گرا (SOA) نقشی حیاتی دارد. سرویس‌های رایانش ابری در قالب وب‌سرویس‌هایی ارائه شده است و از استانداردهای صنعتی همچون زبان توصیفی وب سرویس‌ها (WSDL)، پروتکل ساده دسترسی به شی (SOAP)، و شرح جهانی، کشف و ادغام (UDDI)[9] پیروی می‌کند. در داخل ابر این سرویس‌ها می‌توانند از طریق SOA هماهنگ و مدیریت شوند. به طور مشابهی در سمت سرویس‌گیرنده برای بهبود عملکرد برنامه‌های غنی اینترنتی (RIA) سمت سرویس‌گیرنده بر روی مرورگرهای وب یا موارد دیگر یکپارچه شده است. و این RIAها از AJAX [10] استفاده می‌کنند. با برنامه‌های کاربردی تحت وب AJAX می‌توانیم داده‌ها را از سوی سرورها به صورت یکپارچه بازیابی کنیم و هیچ‌گونه تاثیری هم بر تصویر فعلی کاربر نخواهیم گذاشت. شبکه نیز یک موجودیت مهم است که سبب فراهم‌سازی لینک بین تولیدکننده ابر و مصرف‌کننده مانند LAN/WAN WLAN، ماهواره، شبکه‌های موبایل 3G یا 4G و سایر موارد می‌شود. شکل 1 اجزای مختلف مهم فناوری رایانش ابری را نشان می‌دهد.

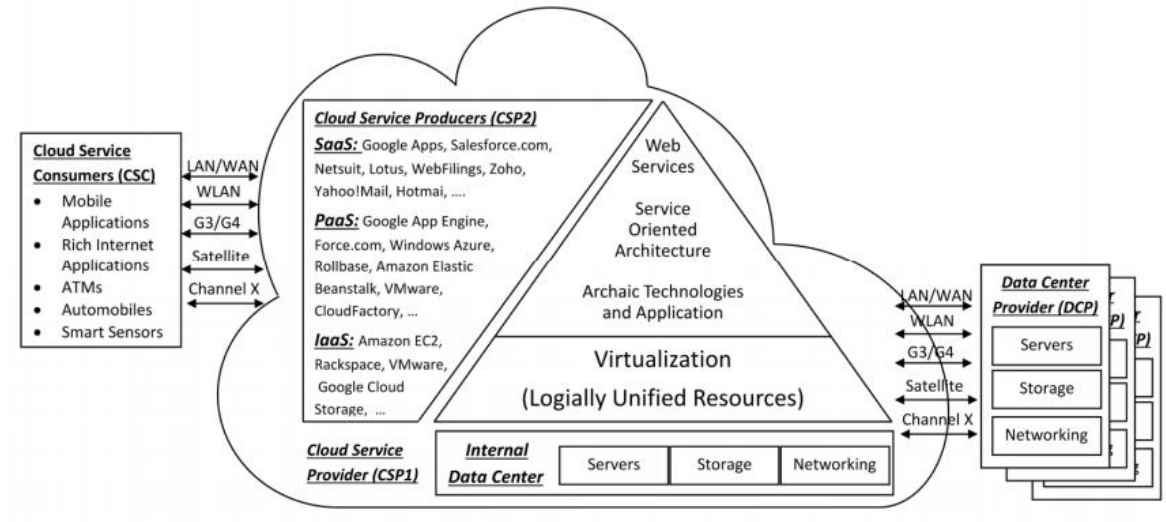
شکل 1 همچنین چند نهادی که در پارادیم رایانش ابری دخالت دارند همچون ارائه‌دهنده‌های خدمات ابری (CSP1)، تولیدکنندگان خدمات ابری (CSP2)، مصرف‌کننده خدمات ابری (CSC) و ارائه‌دهندگان مراکز داده (DCP) را نشان می‌دهد. این شکل همچنین نشان‌دهنده برخی از مثال‌های خدمات در خوشه‌های مختلفی از SaaS، PaaS و IaaS است [1]. همچنین لینک های ارتباطی مختلف بین تولیدکنندگان ابر و مصرف‌کنندگان را نشان می‌دهد. CSP1، CSP2 و DCP می‌تواند یک سازمان واحد مانند Google و DCP باشد که در داخل ابر قرار دارند. یا ابر میتواند از DCP های خارجی با یا بدون DCP داخلی استفاده کند. عوامل دیگر نیز مانند واسطه‌ها، مشاوره‌ها، سازمان‌های استاندارد صنعتی و سازمان های دولتی در میان سایر موارد حضور دارند که در مدل مفهومی مرجع، مؤسسه ملی استاندارد و فناوری (NIST) نشان داده شده است.[12]

3. مسائل امنیتی رایانش ابری

رایانش ابری را می‌توان به عنوان نقطه اوجی برای تمامی مجموعه‌های مختلف فناوری اطلاعات و ارتباطات (ICT) دانست که اجزای تشکیل‌دهنده آن در کنار یکدیگر کار می‌کنند. در یک مورد ساده زمانی که خرید یک صابون یک

دلاری از طریق یک برنامه تحت وب که بر روی محیط ابر اجرا شده است، یک دستگاه موبایل از زیرساخت‌های گسترده و جهانی ICT به ارزش تریلیون دلار استفاده خواهد کرد. این تراکنش ساده از صدها سرور عبور خواهد کرد مانند سرورهای مسیریابی اینترنتی، سرورهای پایگاه داده، سرورهای شبکه‌های موبایل، سرورهای وب، سرورهای برنامه‌های کاربردی، سرورهای ابر و سایر موارد. به طور مشابهی، از طریق حضور مجازی سازمان‌های متعدد مانند سازمان تولید، سازنده ابر، ارائه‌دهنده ابر، سازمان‌مالی و غیره، عبور می‌کند. در عین حال این تراکنش ساده در معرض بسیاری از تهدیدات موجود در زیرساخت های گسترده فیزیکی یا مجازی ICT از طرف مهاجمان مخرب و بیگانه ها قرار دارد.

شکل 1) چهارچوب فناوری رایانش ابری



چندین مطالعه در مورد کارهای پیشین وجود دارد که به شناسایی تهدیدات امنیتی در پارادیم رایانش ابری پرداختند. برخی از مطالعات مانند [20]-[13] که از محدوده 2009 الی 2016 بوده است انتخاب گشته است تا به بررسی نگرانی‌های امنیتی بپردازیم. مطالعه [13] سعی در دسته‌بندی این مشکلات بر اساس مدل‌های خدمات ابری دارد (IaaSوSaaS, PaaS). به طور مشابهی [14] نگرانی‌های امنیتی را بر اساس فناوری طبقه‌بندی کرده است (ارتباط و معماری) و مسائل کسب و کار (جنبه‌های مفهومی و حقوقی) بررسی کرده است. در حالیکه مطالعه [15] این تهدیدات را در ابعاد مختلفی از رایانش ابری ارائه کرده است. مطالعه [16] مسائل امنیتی را ارائه کرده است که باید در سطح توافق‌نامه‌های سطح خدمات در نظر گرفته شود. همچنین بر روی تهدیدات امنیتی مرتبط با نقاط دسترسی

مختلف مانند سرور، اینترنت و پایگاه داده تاکید داشته است. علاوه بر این بر روی حفظ حریم خصوصی داده‌ها و امنیت دسترسی به برنامه‌ها نیز تاکید داشته است.

با نگاهی بر اهمیت رایانش ابری، سازمان‌های مختلفی مانند NIST، دستورالعمل‌هایی را برای اخذ رایانش ابری صادر کردند. این دستورات مسائل امنیتی را به 9 دسته طبقه‌بندی کرده است [17]. مشابه با سایر سازمان‌های مهم مانند سازمان متحد اروپا برای امنیت شبکه و اطلاعات (ENISA) بینش‌هایی را برای SMEها در مورد مسائل مرتبط با ریسک‌های شبکه و اطلاعاتی فراهم کرده است و این پیش از اتخاذ رایانش ابری است [18]. آخرین و مهم‌ترین نکته، اتحاد امنیت ابری (CSA) یکی از برترین گروه هایی است که بر روی تهدیدات امنیتی فعالیت می‌کند و اخیرا 12 مورد از تهدیدات خائنانه ابری را بر اساس نظرسنجی از کارشناسان این صنعت منتشر کرده است [19].

همانطور که وب سرویس‌ها و SOA بخش جدایی ناپذیر از ارکستر ابر هستند، امنیتی در این حوزه نیز از اهمیت زیادی برخوردار است. پروژه امنیت برنامه‌های کاربردی تحت وب باز (OWASP) اقدام به انتشار مهم‌ترین خطرات امنیتی برنامه‌های تحت وب از سال 2003 کرده است. از زمان عرضه آن از سال 2013 لیست‌های 10 مورد برتر از بیش‌از 500000 آسیب‌پذیری در صدر سازمان‌ها و هزاران برنامه کاربردی را منتظر کرده است [20]. بررسی این مطالعات نشان می‌دهد که محدوده مسائل امنیتی رایانش ابری از یک سو شامل منابع فیزیکی ICT، اینترنت، برنامه‌های تحت وب، و دسترسی به داده و حفظ حریم شخصی، مراکز داده‌ها و از سویی دیگر مجازی‌سازی و معماری ابر، استقرار ابر و مدل‌های خدمات، و توافقنامه سطح سرویس است. ماهیت دسته اول مربوط به زیرساخت‌های سنتی ICT است و دسته دوم بیشتر مربوط به حوزه رایانش ابری است.

علاوه بر این برای درک گستره وسیعی از مسائل امنیتی، مهم است که علم‌رده‌بندی منطقی و ساده داشته باشیم. در این مقاله این علم‌رده‌بندی بر اساس تحلیل محتوای ساده و تمایز آن‌ها از رایانش ابری صورت می‌گیرد. جدول 1 طبقه‌بندی یا علم‌رده‌بندی مسائل امنیتی را در داخل حوزه‌های متمایز و زیردامنه‌ها ارائه می‌دهد. این طبقه‌بندی به عنوان راهنمایی در زمینه حفاظت و حل مشکلات امنیتی عمل می‌کند. پنج حوزه مانند مجازی‌سازی سیستم، برنامه‌نویسی برنامه‌های کاربردی، داده، شبکه و ارتباطات و کسب و کار و مسائل امنیتی وجود دارد. هر کدام از این

پنج حوزه دارای زیردامنه‌های بیشتری مانند محیط میزبان و محیط، برنامه‌های تحت وب و SOA، مسائل مرتبط با ذخیره‌سازی و خطرات آن، اینترنت، درون ابر، مدیریت هویت و کنترل دسترسی، و موافقت‌نامه‌های سطح خدمات، طرز اداره، و ارائه‌دهندگان خدمات و واسطه ها است. علاوه بر این موارد نگرانی‌های امنیتی مرتبط را در داخل دامنه‌ها و زیر دامنه‌های مختلفی نگاشت می‌کند. بنابراین تهدید امنیتی فردی به راحتی می‌تواند در داخل نهادهای مسئول ردیابی و حل شود.

جدول 1 علم طبقه‌بندی یا طبقه‌بندی مسائل امنیتی در محیط رایانش ابری [20]-[13]

نگرانی در مورد مسائل امنیتی	زیردامنه	دامنه
پیچیدگی هایپروایز ، حملات برداری، مدیریت مجازی‌سازی	محیط میزبان	مجازی‌سازی سیستم
به اشتراک گذاری تصویر VM، جداسازی VM، فرار از VM، مهاجرت VM، رد VM و هرزه رویی VM	محیط مهمان	
تزریق، خرابی تصدیق هویت و جلسه مدیریت، اسکریپت بین سایتی (XSS)، اشاره مستقم به شی به شکل غیر ایمن، فاش‌سازی داده‌های حساس، از دست دادن کنترل تابع سطح دسترسی ، جعل درخواست بین‌سایتی (CSR)، استفاده از اجزای آسیب‌پذیر شناخته شده، تغییرمسیرهای نامعتبر و ارسال‌های نامعتبر، APIهای غیر ایمن	برنامه‌های کاربردی تحت وب	برنامه‌نویسی برنامه‌کاربردی
برنامه‌های کاربردی معماری سرویس‌گرا ماشین به ماشین، معماری برنامه‌های کاربردی ابر، کنترل امنیت APIها	معماری سرویس گرا	
سرقت یا از دست دادن دستگاه، خرابی داده‌ها، داده‌های کمکی، امنیت دسترسی به پایگاه داده	خطرات	داده

حفظ حریم خصوصی داده، تمامیت، قابلیت اطمینان، بکاپ و بازیابی آسیب‌پذیری، تمیزسازی رسانه‌های نامناسب	مسائل ذخیره‌سازی	
خودداری از خدمات، مرد میانی، استراق سمع، جعل IP مبتنی بر سیل، جعل هویت، ربودن حساب کاربری، تهدید های مداوم پیشرفته (APTs)؛ حفاظت از سمت سرویس‌گیرنده و سرور	اینترنت	شبکه و ارتباطات
زیرساخت ارتباطی مشترک؛ شبکه مجازی اشتباهات امنیتی پیکربندی ؛ گزارش بروزرسانی؛ مدل استقرار، باس شرکت خدمات (ESB)؛ شخص ثالث، مهندسی حملات اجتماعی	ابر درونی	
هویت ضعیف، مدرک معتبر و مدیریت دسترسی؛ احراز هویت؛ کنترل دسترسی ؛ مدیریت رابط کاربر گرافیکی و سازگاری با API؛	مدیریت هویت و کنترل دسترسی	
مشکلات پاسخگویی؛ تداوم خدمات کسب و کار؛ پاسخگویی حادثه؛ اختلالات اداری یا قانونی؛ قطعی موقت دائمی و دائمی؛ مالکیت داده؛ دسترسی مجاز کاربر، پایداری طولانی مدت؛ خدمات ترکیبی؛ مدیریت ریسک	توافق‌نامه سطح سرویس	مسائل قانونی و کسب و کار
موقعیت داده؛ قانون و مقررات؛ کشف الکترونیکی، قضاوت خارجی مسائل	شیوه اداره	
نارسایی به دلیل کوشش پیوسته، سوء استفاده و استفاده نادرست از خدمات ابر، محدودیت واسطه‌ها، اضافه‌بار، هزینه‌های غیر منتظره، ارزش افزوده	تامین‌کنندگان سرویس و واسطه‌ها	

4. راه‌حل‌های امنیتی رایانش ابری

این موضوع مهمی است که تفاوت تهدیدات امنیتی مختلفی که ناشی از هسته‌های اصلی و اثرات بدخیم آن‌ها را در محیط رایانش ابری درک کنیم. از آنجایی که قدرت کل بستگی به قدرت ضعیف‌ترین عنصر دارد و ابرها باید قبل از اینکه بتوانند جزء جدایی‌ناپذیری از سازمان‌ها و جوامع باشند، آزمون‌هایی آزمایشی را در مورد محرمانگی، یکپارچگی و دسترسی به خدمات را بگذرانند. یکی دیگر از معیارهای مهم برای هر راه‌حل امنیتی که برای دوام در محیط ابری لازم است این است که باید در راستای فلسفه ابر باشند یعنی مقیاس‌پذیر باشند، قابلیت حمل داشته باشند، مستقل از پلت‌فرم باشند، انعطاف‌پذیری داشته باشند، قابلیت دوام، در همه‌جا حاضر، و قابلیت اشتراک‌گذاری (چند مستاجره بودن) و خدمات مفید برای رایانش را داشته باشند. از جمله طیف گسترده ای از مسائل امنیتی، سیستم مجازی‌سازی و برنامه نویسی برنامه‌های کاربردی مهمترین مسائل است که باید قبل از مهاجرت به ابر باید مورد توجه قرار گیرد. از آنجایی که مکانیزم های امنیتی در این مناطق اصلی، تهدیدات را در ابعاد دیگر محدود می‌کند. به طور مشابهی از دیدگاه تجاری برای کاهش ریسک‌ها، توافقنامه سطح خدمات یک سند مهم است که باید به شکلی دقیق طراحی شده باشد. همانطور برای سایر چالش‌های امنیتی سنتی باید راه‌حل‌های امنیتی قدیمی را اتخاذ کنیم که از جمله آن‌ها می‌توان به افزونگی، پشتیبان‌گیری و بازیابی و رمزنگاری اشاره کرد.

A. مجازی‌سازی سیستم

خطرات امنیتی متعددی در ارتباط با مجازی سازی مهمان وجود دارد مانند هایپروایزها یا VMM ها و مجازی‌سازی میزبان مانند ماشین‌های مجازیVMها. چالش‌ها در صورتی اتفاق می‌افتند که هایپروایزها دسترسی به دستکاری برخی از VMها داشته باشند. سپس این VM بدخیم می تواند عملیات مخرب را با دیگر VM ها در محیطی موقت انجام دهد. این اتفاق زمانی می‌افتد که هکرها حفره‌های حلقهای در نرم افزار هایپروایزها را پیدا کنند. برای مقابله با این وضعیت وب سرویس‌های آمازون از نسخه های متنوع XEN HV[7] استفاده می کنند. به طور مشابهی عملیات VM مانند اشتراک گذاری تصویر (ایجاد VM)، مهاجرت و ردیابی از جمله چالش‌های امنیتی مستعد هستند [14]. همچنین مسائل امنیتی مربوط به جداسازی VM و هرزه‌رویی باید با دقت مدیریت شوند.

CSA [21] دستورالعمل‌هایی برای ایمن‌سازی محیط مجازی‌سازی ارائه شده است. در این دستورالعمل‌ها بر روی استفاده از هایپروایزرهای جاسازی شده در APIها برای نظارت بر ترافیک داده VM تاکید شده است. CSP2 باید خط‌مشی سیاست‌های امنیتی را بروزرسانی کند. داده‌هایی که توسط VMها مورد استفاده قرار می‌گیرند باید توسط سیاست مبتنی بر سرورهای کلیدی رمزگذاری شوند و این کلیدها باید به طور جداگانه برای داده و خود VMها ذخیره شده باشد. VMها باید شامل فایروال‌ها و سیستم‌های پیشگیری از هک و نفوذ (HIPS و NIPS) و سایر ابزارهای امنیتی سنتی باشند. در جایی که CSP1 مسئول پاک سازی پشتیبانی و خرابی VMها در طی عملیات پاک‌سازی VM باشند. CSP1 باید همچنین سوابق انزواشده را ثبت کند و در صورت نقض این انزوا باید ساز و کار اطلاع رسانی داشته باشد.

B برنامه‌نویسی برنامه‌های کاربردی

رایانش ابری به شدت به برنامه‌های تحت وب یا وب سرویس‌ها و SOAها وابسته است. فهرست OWASP لیستی از مهمترین ریسک‌ها امنیتی برنامه های وب که اهمیت زیادی دارند را ارائه داده است [20]. این مطالعه همچنین به سوءاستفاده، شیوع، مطلوبیت و اثرات فنی هر کدام از این ریسک‌ها اشاره کرده است. تزریق یا اینجکشن (SQL، سیستم عامل OS و پروتکل دسترسی دایرکتوری سبک وزن LDAP)، شی مرجع مستقیم نا امن (DOR)، خطای امنیتی در پیکربندی اشتباه، از دست دادن تابع کنترل سطح دسترسی را به راحتی می‌توان مورد سو استفاده قرار داد. مشابه با شکستن تصدیق هویت و جلسات مدیریت و استفاده از اجزایی که دارای مشکلات آسیب‌پذیری هستند به شدت در حال گسترش است در حالیکه مشکل سوءاستفاده از اسکریپت سایت (XSS) به شدت گسترده شده است. بدترین بخش این است که XSS، DOR غیر امن، خطای امنیتی در پیکربندی اشتباه، درخواست جعلی بین سایتی (CSRF) و تغییر مسیر نامعتبر و ارسال‌های نامعتبر به راحتی توسط مهاجمین قابل ردیابی است. اما بخش مثبت قضیه این است که آن‌ها را به سادگی و با استفاده از باگ‌زدایی و آزمون‌های مناسب می‌توان برطرف کرد. به طور مشابهی تاثیرات تکنیکی تزریق، شکستن تصدیق هویت و جلسه مدیریت، افشای داده‌های حساس سطح سرور هستند. با این حال اثر کسب و کار هر کدام از این ریسک‌ها در ارتباط با ارزش داده‌ها و میزان شیوع اختلالات است.

OWSAP همچنین منابع متعددی را برای کاهش خطرات امنیتی برنامه‌های وب توسعه داده است. در بین آن‌ها استاندارد اعتبارسنجی امنیت برنامه‌های کاربردی (ASVS) برای ارزیابی نیازهای امنیتی برنامه‌ها است، راهنمای توسعه‌دهنده ها و جداول جلوگیری از تقلب برای طراحی امنیت از ابتدا باید مورد توجه قرار بگیرد و API امنیت شرکتی (ESAPI) برای توسعه امنیت APIهای برای تولید امنیت در برنامه‌های کاربردی تحت وب مورد نیاز است. به طور مشابهی از استاندارد اعتبارسنجی امنیت برنامه‌های کاربردی (ASVS) می‌توان برای اعتبارسنجی کدها استفاده کرد. همچنین برخی از ابزارهای منبع باز برای اعتبارسنجی کدها مانند O2 و FindBugs وجود دارد. در نهایت ابزارهای تست امنیت و نفوذ مانند WebScarab و Zip را می‌توان برای از بین بردن تهدیدات امنیتی مورد استفاده قرار داد.[20]

C امنیت یکپارچه چندسطحی

مقالات زیادی در مورد مفهوم امنیت به عنوان یک سرویس وجود دارند و به حمایت و کاوش در مورد آن پرداختند. اما همچنان معانی کاملا منفی برای این ایده وجود دارد که برای گسترش رایانش ابری بسیار مخرب هستند. نخست، این بدان معنی است که یک نفر باید به شکل مستقیم برای امنیت هزینه کند و این یک بازدارنده اصلی در زمان کمبود منابع رقابتی است. دوم اینکه این امر بیانگر این است که امنیت یک نهر فرعی گران‌قیمتی است که تلاش می‌کند شکافی دیجیتال را از بین ببرد. یا بدترین نتیجه این است که از این مفهوم سیگنال‌هایی مخابره می‌شود که اینگونه از آن برداشت می‌شود که بدون اشتراک امنیت به عنوان یک سرویس، منابع شما در امنیت نیستند، و این محدودیتی بسیار جدی برای متقاضیان احتمالی این فناوری است.

رویکرد صحیح این است که ویژگی‌های امنیتی که تمامی ابرهای SaaSو PaaS یا IaaS ارائه می‌دهند را ادغام کنیم. و سطوح مختلفی برای آن می‌توان تعریف کرد از جمله نرمال، بالا یا بحرانی. به طور مشابهی API های کنترل امنیتی را می وان برای اجرای این سطوح توسعه داد. در زمان اشتراک سرویس، کاربر باید سطح دلخواه را براساس نیاز خاص دامنه تعریف کند. و در طی تنظیمات سرویس، می توان از طریق اجرای API های کنترل امنیتی مختلف، اجرای آنها را انجام داد. هزینه این تلاش‌ها را می‌توان سعی کرد که با استفاده بیشتر از محاسبات، ذخیره سازی و

پهنای باند یا افزایش پایگاه مشتریان به سود رساند. گزینه دیگر، که کمتر مطلوب است، از طریق صورتحساب مستقیم اشتراک این API ها است. در هر دو مورد مفهوم امنیت یکپارچه در ابر باقی خواهد ماند. به طور مشابه، مدل فشار امنیتی باید از CSP1، CSP2 به CSC پیروی کند. در جایی که تقریبا تمام تقسیم‌بندی امنیتی باید بر اساس CSP1و CSP2 به ترتیب قرار بگیرد. و سطح CSC کاربران باید به آنها اعمال شود یا آن‌ها را تشویق کنیم که روندهای استاندارد امنیت عملیاتی را از طریق مدل‌های فشاری رعایت کنند.

D. توافق‌نامه سطح خدمات

این سند موقعیت بسیار مهمی در محاسبات ابری دارد تا مسئولیت های مربوط به حفاظت از منافع همه طرف‌های درگیر را به عهده بگیرد. چهار احزاب به طور مستقیم در اجرای محاسبات ابری دخالت دارند:

ارائه دهندگان خدمات ابر (CSP1)، تولید کننده خدمات ابر (CSP2)، مشتریان خدمات ابر (CSC) و ارائه دهندگان خدمات داده (DCP). علاوه بر این، مشارکت چندین واسطه مانند حسابرسان امنیتی، نهادهای استاندارد صنعتی و سازمان های حکومتی، سازمان های دولتی و غیره نیز وجود دارد.

این سند، باید به وضوح مسئولیت‌های هر یک از سهامداران مانند CSP1،CSP2، CSC و DCP را در تامین منافع فردی تقسیم کند. معیارهای اساسی عملکرد مانند محرمانه بودن، یکپارچگی و دسترسی دارایی های اطلاعاتی باید دقیق و مشخص باشند. علاوه بر این، باید رهنمودهای واضحی برای ساز و کارهای حل اختلاف، طریقه اداره سازمان‌های دولتی و اختلاف نظر در مورد حوزه‌های حقوقی وجود داشته باشد. به طور مشابه، مالکیت، امنیت و حریم خصوصی مصنوعات نرم افزاری و داده ها نیز باید به وضوح تعریف شود. و با توجه به فلسفه رایانش ابری در مورد تأمین فوری و آزاد سازی منابع، منابع باید در قالب قابل استفاده بدون هیچ گونه نقضی توسط احزاب فردی در صورت قطع خدمات باشند.

5.جمع‌بندی

رایانش ابری مطمئنا نتیجه تلاشی از تقریبا نیم قرن گذشته در زمینه محاسبات و تلاش برای تبدیل محاسبات به خدمات نرم‌افزاری مانند انرژی و آب است. این فناوری بر اساس سه فناوری مهم استوار است مجازی‌سازی، برنامه های

کاربردی‌وب و معماری سرویس گرا، و برنامه‌های غنی اینترنتی در سمت مشتری یا سرویس‌گیرنده است. با این وجود کل پارادایم ICT وارد بازی می‌شودو مهمتر از همه مراکز داده و شبکه است.

در این مقاله بر برخی از نکاتی که در مورد فناوری‌های بنیادین رایانش ابری مانند مجازی‌سازی و برنامه‌های کاربردی یا وب سرویس‌ها وجود داشته است تاکید شده است. سپس چالش‌های امنیتی که در کارهای پیشین مورد شناسایی قرار گرفته است مورد بررسی قرار گرفت. این مسائل به طور عمده در دو اصلی قرار دارند، که دسته اول بیشتر مسائل سنتی است و در زمینه وب‌سرویس‌ها اهمیت بیشتری دارد و دسته دیگری در مورد پیاده‌سازی فناوری ابر مانند مجازی‌سازی، معماری ابر، مدل های استقرار ابر، مدل‌های خدمات ابر و توافق‌نامه سطح سرویس است. علاوه براین مدل طبقه‌بندی نگرانی‌های امنیتی برای کمک به حل و فصل مسائل امنیتی ارائه شده است. سپس راه‌حل‌های امنیتی و دستورالعمل‌های ارائه شده توسط CSA و OWASP در این حوزه مجازی‌سازی و وب سرویس‌ها به ترتیب همراه با روش وب‌سرویس‌های آمازون برای محافظت از هایپروایزرها ذکر شده است.

این مقاله همچنین مفهومی با اهمیت در مورد امنیت ابری چندسطحی یکپارچه شده را در تقابل با مفهوم امنیت به عنوان یک سرویس مطرح کرده است. همچنین بر روی مدل فشار برای پیاده‌سازی امنیت از CSP1، CSP2 به CSC تاکید داریم. علاوه بر این اصول مهمی برای طراحی توافق‌نامه‌های سطح سرویس مورد بحث قرار گرفته است. کارهای آینده می‌تواند بر روی توسعه مدل هایی برای ارائه سناریوهای متفاوتی از پیاده‌سازی نمونه‌های رایانش ابری و خطرات احتمالی بالقوه ناشی از آن تمرکز کند. پس از آن، ارزیابی کمی و کیفی از مزایا و تهدیدات امنیتی در مناطق مختلف انجام خواهد شد. و با اثبات راه حل‌هایی برای کاهش تلفات در شرایط مختلف دنبال خواهد شد. از این رو برای متقاضیان بالقوه ابر تصمیم گیری آگاهانه برای اتخاذ رایانش ابری آسان‌تر می شود.

رایانش ابری مطمئنا به دلیل پیاده‌سازی ساده و پشتیبانی انتزاعی تقریبی از هر نوع فناوری قدیمی بسیار سودمندتر و پایدارتر از محاسبات شبکه‌ای یا سایر مفاهیم مرتبط است. بنابراین قادر به استفاده از تمام پتانسیل ICT برای حفظ خود است. علاوه بر این، این مفهوم در زمان حاضر بسیار مهم است زیرا دنیا در حال تجربه محدودیت منابع برای پیشرفت در آینده‌ای جدید است. و قابلیت‌پایداری و شهرهای هوشمند معنایی نزدیک از هنجارهای امروزی هستند.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology Draft (NIST) Special Publication 800-145*, 2011. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[2] N. Ahmad and R. Mehmood, "Enterprise systems and performance of future city logistics," *Http://Dx.Doi.Org/10.1080/09537287.2016.1147098*, vol. 27, no. 6, pp. 500–513, 2016.

[3] N. Ahmad and R. Mehmood, "Enterprise systems: are we ready for future sustainable cities," *Supply Chain Manag. An Int. J.*, vol. 20, no. 3, pp. 264–283, 2015.

[4] Gartner, "Gartner Says Worldwide Public Cloud Services Market Is Forecast to Reach $204 Billion in 2016," 2016. [Online]. Available: http://www.gartner.com/newsroom/id/3188817.

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Clearing the clouds away from the true potential and obstacles posed by this computing capability.," *Commun. ACM*, vol. 53, no. 4, pp. 50–59, 2010.

[6] S. Trigueros-Preciado, D. Pérez-González, and P. Solana-González, "Cloud computing in industrial SMEs: Identification of the barriers to its adoption and effects of its application," *Electron. Mark.*, vol. 23, no. 2, pp. 105–114, 2013.

[7] H. Orman, "Both Sides Now: Thinking about Cloud Security," *IEEE Internet Comput.*, vol. 20, no. 1, pp. 83–87, 2016.

[8] S. Campbell and M. Jeronim, "An Introduction to Virtualization," 2006.

[9] L. Wang, G. Von Laszewski, M. Kunze, and J. Tao, "Cloud computing : A Perspective study," *New Gener. Comput.*, vol. 28, no. 2, pp. 137–146, 2008.

[10] D. S. Linthicum, *Cloud computing and SOA convergence in your enterprise: a step-by-step guide*. Pearson Education, 2009.

[11] Gartener, "Cloud Computing as Gartener Sees it," in *Gartner's Application Architecture, Development & Integration Summit*, 2009.

[12] F. Lui, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badget, and D. Leaf, "NIST Cloud Computing Reference Architecture," *National Institute of Standards and Technology (NIST) Special Publication 500-292*, 2011. [Online]. Available: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505.

[13] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[14] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Inf. Sci. (Ny).*, vol. 305, pp. 357–383, 2015.

[15] M. Jouini and L. B. A. Rabai, "A Security Framework for Secure Cloud Computing Environments," *Int. J. Cloud Appl. Comput.*, vol. 6, no. 3, pp. 32–44, 2016.

[16] B. R. Kandukuri, R. Paturi V, and A. Rakshit, "Cloud Security Issues," in *2009 Ieee International Conference on Services Computing*, 2009, pp. 517–520.

[17] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," *National Institute of Standards and Technology Draft (NIST) Draft Special Publication 800-144*, 2011. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

[18] M. A. C. Dekker and L. Dimitra, "Cloud Security Guide for SMEs," *European Union Agency for Network and Information Security*, 2015. [Online]. Available: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

[19] "The Treacherous 12: Cloud Computing Top Threats in 2016," *Cloud Security Alliance (CSA) Top Threats Working Group*, 2016. [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf.

[20] OWASP Top 10, "The Ten Most Critical Web Application Security Risks," 2013.

[21] "Security guidance for critical areas of focus," *Cloud Security Alliance (CSA)*, 2011. [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf.