مجله پژوهش های معاصر در علوم و تحقیقات
سال اول، شماره ۸، اسفند ۱۳۹۸
ISSN: ۷۶۷۶-۵۷۶٤
www.jocrisar.ir

بررسی و مقایسه‌ی معماری‌های امنیتی رایانش ابری در راستای ارائه راهکارهایی جهت توسعه سازمان‌های امنیتی

زهرا سلیمی [۱]

[۱] کارشناسی ارشد مهندسی نرم‌افزار و استاد حق التدریسی دانشگاه پیام نور واحد کرمانشاه

چکیده

رایانش ابری یک مقوله مهم در عصر نوین فناوری اطلاعات بدل شده است. ازاین‌رو جدیدترین تحقیقات در این حوزه پیرامون فناوری ابری صورت می‌گیرد. به همین دلیل شناخت چالش‌های پیرامون رایانش ابری از اهمیت بالایی برخوردار است. مفاهیم تعامل‌پذیری، امنیت، استانداردسازی و معماری‌های امنیتی مهم‌ترین چالش‌های فضای ابری هستند. ازاین‌رو، این مقاله با هدف بررسی معماری امنیتی رایانش ابری در سازمان‌های امنیتی سعی در توسعه مفاهیم امنیتی رایانش ابری دارد. به همین دلیل در ابتدا معماری‌های مختلف رایانش ابری تعریف و بررسی شده است. سپس با بررسی نقاط ضعف و قوت معماری‌های پیشنهادی، با ارائه راهکارهایی به توسعه سازمان‌های امنیتی در راستای بهبود معماری امنیتی ریانش ابری پرداخته شده است.

واژه‌های کلیدی: رایانش ابری، معماری امنیتی، سازمان های امنیتی، معماری رایانش ابری

۱. مقدمه

اگرچه ظهور رایانش ابری یک پیشرفت متأخر بشمار می‌آید، درک جنبه‌های حساس امنیتی می‌تواند از تجارب گزارش‌شده سازگارترهای اولیه و همچنین از محققین که سکوهای ایجادگر ابری موجود و فناوری‌های دست‌اندرکار را تحلیل و آزمایش می‌کنند، جمع‌آوری شود. بخش‌های ذیل مسئلهٔ مربوطه به امنیت و حریم خصوصی را مشخص می‌کند که پنداشته می‌شود اهمیت بلندمدتی به رایانش ابری عمومی و در بسیاری از موارد به سایر مدل‌های سرویس رایانش ابری می‌دهند. در برخی از موارد این احتمال می‌رود که نمونه‌های مشکلات تعریف‌شده یا مشخص‌شده پیشین برای طرح مسئله‌ای ارائه نمودند. نمونه‌ها جامع نیستند و ممکن است که یک جنبه از یک موضوع کلی‌تر را پوشش دهند. در مسائل بسیاری، مشکلات خاص مطرح‌شده دوباره طرح و حل گشته‌اند. بااین‌وجود مسئلهٔ وسیع‌تر در اکثر موارد از خود سماجت و مقاومت نشان می‌دهد و دارای پتانسیلی است که از راه‌های دیگری دوباره خود را در میان مدل‌های سرویس مختلف بروز دهد. ملاحظات امنیتی و حریم خصوصی که از برون داد فناوری اطلاعات منقطع می‌شوند، نیز وجود دارد. در ادامه به بررسی معماری، امنیت و دفاع پرداخته شده است [۱، ۲].

امنیت و حریم خصوصی کاربران، برنامه‌های کاربردی، دستگاه‌ها، منابع شبکه و داده‌ها بخش‌های بسیار مهم معماری و طراحی آن هستند. امنیت در همه بخش‌های معماری تلفیق شده و بر سایر کارکردها در معماری و معماری‌های مبتنی بر شبکه اثر می‌گذارد. واجب است برای کارکرد مناسب امنیت در این حوزه، روابط بین سازوکارهای امنیتی و همچنین روابط بین معماری امنیت و دیگر اجزای معماری به خوبی شناسایی شوند [۳].

فضای مجازی یک سکوی دیجیتالی است که همه افراد، سازمان‌ها، نهادهای دولتی و شرکتی را در محیط اطلاعاتی بهم پیوند می‌دهد و در همه حوزه‌های فیزیکی نفوذ می‌کند و اساس و بنیان همه عملیات‌ها است. در یک محیط امنیتی آینده که با پیچیدگی و ابهام همراه است، نیروی‌های امنیتی پیوند ناگشودنی با توانایی فعالیت موثر وزارت دفاع در فضای مجازی خواهند داشت. در شرایط فعلی سیاسی، اقتصادی و تکنولوژی، از فناوری اطلاعات انتظار می‌رود قابلیت‌های بیشتری درحالی‌که منابع کمتری مصرف می‌کند، ارائه دهد. با افزایش حمایت‌های دولتی و تهدیدات امنیتی مستقل، دپارتمان‌های امنیتی اهمیت روزافزون یک فضای امنیتی امن و محکم را شناسایی می‌کند. در حال حاضر هم‌زمان رویدادهای مالی جهان یک نیاز جدید را ایجاد می‌کنند که سخت‌گیری‌های بیشتری پیرامون مسائل مالی و اشتباهات مالی اعمال می‌نماید. درنتیجه، این دپارتمان می‌بایست راه‌های به دست آوردن، عمل کردن و مدیریت فناوری اطلاعات را تغییر دهد تا افزایش بهره‌وری، تأثیرگذاری و امنیت را درک کند. دپارتمان‌های امنیتی جهت پیشبرد اهداف خود باید به بررسی مسائل روز فضای مجازی بپردازند. ازاین‌رو، استراتژی رایانش ابری یک عامل مهم در این حوزه است و شاخص‌های آن در محیط سازمان ابری باید لحاظ شود [۳، ۴].

دولت، صنعت و دیگر ذینفعان باید الزامات را تعریف کنند، استانداردهای امنیت، تعامل متقابل و قابلیت انتقال داوطلبانه بین‌المللی مبتنی بر توافق را توسعه دهند، و آن‌ها را در محصولات، فرایندها، و خدمات اجرا و پیاده سازند. (استانداردهای امنیت، تعامل متقابل و قابلیت انتقال). محصولات، فرایندها و خدمات مبتنی بر استانداردها برای سازمان‌های دولت آمریکا[۱] لازم و اساسی هستند تا اطمینان دهند که [۱، ۵]:

- سرمایه‌گذاری‌های عمومی بزرگ بالقوه دچار کهنگی فناوری زودهنگام نمی‌شوند،
- سازمان‌های دولتی قادر به تغییر ارائه‌دهندگان خدمات ابر هستند که می‌توانند از ماموریت‌هایشان به صورت انعطاف پذیر و مقرون به صرفه پشتیبانی کنند، و
- دولت آمریکا از یک میدان اقتصادی هموار برای ارائه‌دهندگان خدمات پیشتبانی می‌کند.

توسعه استانداردها با شناسایی الزامات مشخص و روشن، آغاز می‌شود. سازمان‌های USG الزاماتی مربوط به ماموریت را شناسایی کرده ند بستگی به استانداردهای امنیتی، قابلیت انتقال و تعامل متقابل فنی دارند. گروه کاری عمومی نقشه

[۱] United States Government (USG)

استانداردهای رایانش ابر NIST، استانداردهای فناوری اطلاعات کلی را فهرست کرده است که برای رایانش ابر استفاده می‌شوند، و استانداردهای نوظهوری که الزامات مختص فناوری‌های زیربنایی را هدف قرار می‌دهند که امکان رایانش ابری را فراهم می‌کند. این تلاش تنها سه استاندارد ابری نوظهور را تاکنون شناسایی کرده است، اگرچه سازمان‌های استانداردها در حال اتخاذ استانداردهای دیگری هستند. یافته‌های پروژه تسریع استانداردهای NIST جهت راه‌اندازی اتخاذ رایانش ابری نمونه‌های کاری را ارائه می‌دهد که نشانگر چگونگی پشتیبانی از پرونده‌های مهم استفاده فنی در سیستم‌های ابری است که ویژگی‌های سیستم ابر عمومی و ثبت شده را اجرا می‌کند. تسریع استانداردها جهت راه‌اندازی اتخاذ رایانش ابری دریافت که موارد استفاده فنی امنیتی، قابلیت انتقال، و تعامل متقابل بسیار بهم متصل و مرتبط اند، و نیاز به استانداردهای امنیتی، تعامل متقابل و قابلیت انتقال داوطلبانه بین‌المللی مبتنی بر توافق یکپارچه را برجسته می‌کنند [۱، ۵].

در شرایط فعلی سیاسی، اقتصادی و تکنولوژی، از فناوری اطلاعات انتظار می‌رود قابلیت‌های بیشتری درحالی‌که منابع کمتری مصرف می‌کند، ارائه دهد. با افزایش حمایت‌های دولتی و تهدیدات امنیتی مستقل، دپارتمان‌های امنیتی اهمیت روزافزون یک فضای امنیتی امن و محکم را شناسایی می‌کند. در حال حاضر هم‌زمان رویدادهای مالی جهان یک نیاز جدید را ایجاد می‌کنند که سخت‌گیری‌های بیشتری پیرامون مسائل مالی و اشتباهات مالی اعمال می‌نماید. درنتیجه، این دپارتمان می‌بایست راه‌های به دست آوردن، عمل کردن و مدیریت فناوری اطلاعات را تغییر دهد تا افزایش بهره‌وری، تأثیرگذاری و امنیت را درک کند. دپارتمان‌های امنیتی جهت پیشبرد اهداف خود باید به بررسی مسائل روز فضای مجازی بپردازند. ازاین‌رو، استراتژی رایانش ابری یک عامل مهم در این حوزه است و شاخص‌های آن در محیط سازمان ابری باید لحاظ شود [۱، ۵].

در ادامه این مقاله بخش دوم به بررسی مفهوم رایانش ابری؛ بخش سوم به بررسی استراتژی رایانش ابری؛ بخش چهارم به بررسی معماری رایانش ابری و مباحث امنیتی در معماری رایانش ابری پرداخته است. در ادامه بخش پنجم به بررسی و ارائه راهکارهای معماری امنیتی رایانش ابری پرداخته است. در نهایت، نتیجه گیری مقاله ارائه شده است.

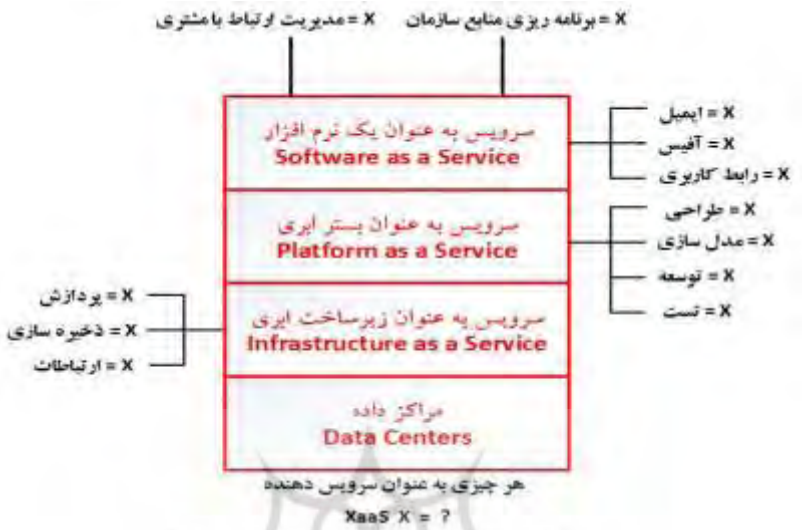
۲. رایانش ابری

در دیدگاه‌های مختلف یک معماری ۳ لایه‌ای و یک معماری ۴ لایه‌ای معرفی‌شده است. این معماری دارای ۳ لایه اصلی است و لایه زیر ساختار خود را به یکی از سه زیر لایه تبدیل کند. نخستین بار معماری بخش CaaS مطرح‌شده است و به برخی قابلیت‌های ارتباطی که از طریق شبکه‌های ابری اشاره دارد. در لایه‌ها، هر لایه زیر بنایی برای لایه بالایی خود است و اشکال مختلفی در رابطه با خدمات محاسبات ابری وجود دارد درواقع نوعی از منابع است که از طریق اینترنت در اختیار مشتریان قرار می‌گیرد. سلسله‌مراتب محاسبات ابری که به‌صورت شکل ۱ ارائه می‌گردد شامل موارد زیر است [۲]:

۱. سرویس نرم‌افزار ابری
۲. سرویس به‌عنوان بستر ابری
۳. سرویس به‌عنوان زیرساخت ابری
۴. مراکز داده‌ها

اگر از سمت مدل استقرار برنامه در سطح سازمانی به یکی از مدل‌های ابری برویم، بایستی در خصوص معماری‌های رایانش ابری مطالعه بیشتری بکنیم. ابرهای خصوصی و عمومی ویژگی مشابهی دارند. در کل سه نوع مدل خدمات اصلی وجود دارد که باید در نظر گرفت. سازمان‌های فناوری اطلاعات برنامه‌های خود را بر طبق کاربردشان روی ابرهای عمومی، خصوصی یا ترکیبی قرار دهند. اطلاعات عمومی، خصوصی و ترکیبی به مکان وابستگی ندارند. معمولاً ابرهای عمومی در اینترنت و ابرهای خصوصی در یک محدوده خاص می‌باشند. ابرهای خصوصی در فضاهای اشتراکی نیز می‌توانند قرار گیرند. شرکت‌ها در انتخاب مدل رایانش ابری خود نکات زیادی را موردتوجه قرار می‌دهند. مثلاً برای یک مسئله، مدل‌های گوناگونی را بکار

می‌گیرند. برای قرارگیری در ابر عمومی به یک برنامه کاربردی موقتی نیاز است، زیرا نیاز به خرید تجهیزات اضافی را یک نیاز موقتی برطرف می‌کند؛ بنابراین، یک برنامه‌ای که نیازمند کیفیت خدمات است، یا اینکه نیازمند مکان داده ازنظر جغرافیایی است، بهتر است که در یک ابر خصوصی یا ترکیبی باشد. جدول ۱ توضیحاتی کلی از لایه‌های سلسله مراتبی رایانش ابری را نشان داده است [۶].



شکل ۱ - سلسله‌مراتب لایه‌ای محاسبات ابری [۶]

الزامات مورد بحث در این بخش از نقشه فناوری رایانش ابری USG به این صورت شناسایی می‌شوند: الزمات امنیتی، تعامل متقابل و قابلیت انتقال راهبردی و تاکتیکی با اولویت بالا که سازمان‌های USG باید به آن‌ها دست یافبند تا مدل رایانش ابری را جهت دستیابی به اهداف استراتژی رایانش ابری اتحادی اتخاذ کند [۵].

جدول ۱ - خصوصیات، خدمات و سازمان ارائه کننده: لایه‌های سلسله مراتبی رایانش ابری [۵]

نوع	خصوصیات	برخی از خدمات	سازمان های ارائه کننده
نرم‌افزار به عنوان سرویس	نرم‌افزار به‌عنوان خدمات، خدمات مبتنی بر تقاضای مشتری، ارائه خدمات به چندین کاربر بصورت همزمان، اجرا کلیه خدمات بر روی محیط ابر	ذخیره سازی، پست الکترونیک، بازارهای الکترونیکی راه دور، اشتراک داده تصویر، مدیریت فرآیند کسب و کار	Gmail Drive Zimory.com SmugMug Appian Anywhere
سکو به عنوان سرویس	مبتنی بر استفاده، قابلیت فاز بندی در پروسه های پیاده سازی، قابلیت شبیه سازی بر روی بستر های مجازی سازی سیستم عامل، مشتری با سکو از طریق API قادر است ارتباط برقرار کند.	داده، پایگاه سازی، ذخیره محاسبات، پرداخت، صدور صورت حساب	Amazon EC۲, EC۳, SimpleDB, Network.com, salesforce
زیرساخت به عنوان سرویس	قابلیت‌های محاسباتی و ذخیره‌سازی در این لایه فراهم میشود. حجم کاری و سایر نیازهای اساسی برنامه‌های کاربردی در این قسمت تامین میشود.	خدمات زیر ساخت از جمله سرورها، سیستم‌های ذخیره‌سازی، سوئیچ‌ها، روترها	Xcalibre FlexiScale Joyenet

۳. استراتژی رایانش ابری

برای برنامه‌ریزی آینده، هر سه مدل عمده تحویل (IaaS, PaaS, and SaaS) در اینجا می‌مانند. همان‌طور که مشتریان درمی‌یابند که ارزش و منابع ذخیره‌ای بیشتری از سرویس‌های نرم‌افزار و سکو بجای زیر ساختار وجود دارد، محتمل است که IaaS سهم بازار به‌تدریج افت می‌کند. اگرچه وابستگی‌ها و فاکتورهای تکنیکی خاص سرویس‌های ابری IaaS شناور را برای مدتی نگه می‌دارد تا به مرحله انجام برسند. احتمالاً ما استحکام بیشتری را در فضای IaaS خواهیم دید زیرا بازار سرویس ابری IaaS مانعی بسیار خفیف برای ورود و ضریب کمترین تفکیک تکنیکی دارد. همان‌طور که IaaS کالایی تجاری می‌شود، بازگشت سرمایه افت می‌کند و ایجادگرهای ابری مجبور به نقل‌مکان به بخش‌های پرمنفعت‌تر PaaS و SaaS می‌شوند. ایجادگرهای خرده پا IaaS منابع مالی ندارند تا نرم‌افزار پیچیده را توسعه دهد تا در فضای PaaS و SaaS رقابت کنند و بنابراین استحکامات و شراکت‌ها برای ادامه حیات لازم خواهد بود. توسعهٔ PaaS و سرویس‌های کیفیت بالا به شرکت‌ها کمک می‌کنند تا کیفیت کد را بهبود بخشند، همکاری تیم توسعه را ارتقاء دهند و توسعه نرم‌افزار و چرخهٔ یکپارچه‌سازی مداوم را تسریع کنند. اکثر گروه‌های توسعه ترجیح می‌دهند از روش توسعه نرم‌افزار چابک در مقابل مدل آبشاری سنتی استفاده کنند. سکوهای توسعه PaaS و ابزارهای همکاری شرکت‌ها را با پس‌اندازهای اساسی پولی و زمانی تأمین می‌کند و بنابراین ما احتمالاً ابدعات بیشتری رو در این بخش خواهیم دید. تحلیل داده و اطلاعات تجارت ابری به‌عنوان یکی از سودمندترین بخش‌ها در بازار سرویس‌های ابری باقی می‌ماند [۱، ۲].

صنعت باید خدمات ابر را همواره و به وضوح طبقه‌بندی کند (فناوی و هدایت قابلیت انتقال و تعامل متقابل). ازاین‌رو، استراتژی رایانش ابری بدین صورت قابل تحقق است [۶]:

الف) مشتریان پیچیدگی‌های انواع مختلف خدمات ابر را درک کنند و بهتر بتوانند خدمات ابر مناسب را برای رسیدن به اهداف کسب و کارشان انتخاب کنند،

ب) مشتریان قادر خواهند بود بین محصولات فروشندگان ابر مختلف، ارزیابی و مقایسه و انتخاب کنند، و

ج) برای ارائه‌دهندگان مشخص خواهد شد که چه موقع قابلیت انتقال و تعامل متقابل باید در طبقه‌بندی‌های مشابه خدمات ابر وجود داشته باشند.

تعریف رایانش ابری NIST سه طبقه‌بندی مجزای مدل‌های خدمات ابر را شناسایی کرده است: نرم‌افزار به عنوان یک خدمت، پلتفروم به عنوان یک خدمت، و زیرساخت به عنوان یک خدمت. در حال حاضر، مصرف‌کنندگان باید به دنبال درک خدمات ابری از طریق دیدگاه سفارشی ارائه شده توسط هر ارائه‌دهنده خدمات باشند. به علاوه، درحالیکه بسیاری فروشندگان به دنبال ایجاد طبقه‌بندی‌های جدید از خدمات هستند، که موقیت بازارشان را بهبود ببخشد، مشخص نیست که هر یک از طبقه‌بندی‌های پیشنهادی منحصر به فرد است و در سه خدمت اولیه موجود قرار ندارد. نمونه‌های مواداضافه شده پیشنهادی شامل داده به عنوان یک خدمت، شبکه به عنوان یک خدمت، خدمت به عنوان یک خدمت، و غیره است. نتیجه آن چشم‌انداز گیج‌کننده ای از خدمات ابری بالقوه است [۱، ۲].

در اواخر سال ۲۰۱۰، تیم پروژه معماری مرجع رایانش ابری NIST، ۱۱ مدل مرجع رایانش ابری موجود پیشنهادی سازمان‌های ابر، فروشندگان، و سازمان‌های اتحادی (فدرال) را بررسی کرد تا ببیند که آیا توافق صنعتی مشخصی بین آن‌ها وجود دارد. تحلیل نشانه اختلاف گسترده ای بود. مشتریان به یک مدل بی‌طرف مورد درک عموم نیاز دارند تا همواره و مشخصا درک کنند که چگونه خدمات ابری مقایسه می‌شوند (برای مثال اپل با اپل). در نوامبر ۲۰۱۰، گروه کاری عمومی به میزبانی NIST شروع به بررسی معماری‌های مرجع نمود و همه توصیه‌های پیشنهاد را بررسی کرد. گروه این کار را از طریق اتفاق‌نظر تلفیق به پیش برد تا معماری مرجع بی‌طرف را تعریف کند. معماری مرجع اولیه و طبقه‌بندی بر "کدام" در مقابل "چگونگی" پیاده‌سازی و اجرا تمرکز دارد، و محدود به اجرا و پیاده‌سازی یک فروشنده خاص نیست. اگرچه شرکت‌کنندگان صنعتی این مدل را با طرح‌ریزی آن در خدمات ابری شان، تایید نموده اند، تا برای USG و سایر مصرف‌کنندگان مفید باشد، تایید و مشارکت گسترده‌تر ذینفعان مورد نیاز است [۵، ۶].

۴. معماری رایانش ابری

معماری نرم افزار و سخت افزار بکار رفته در تحویل سرویس های ابری می تواند بطور بسزایی در میان ایجادگرهای ابری عمومی برای هر مدل خاصی از سرویس متفاوت باشد . موقعیت فیزیکی زیر ساختار توسط ایجادگر ابری تعیین می شود ، همانطور که آن زیر ساختار، طرح و پیاده سازی قابلیت اتکاء ادغام منابع ، مقایس پذیری و سایر منطق مورد نیاز در چهار چوب پشتیبان است . برنامه های کاربردی بر مبنای واسطه های برنامه نویسی سرویس های اینترنت دسترس پذیر شکل می گیرند که عمدتاً اجزای ابری چندگانه را با یکدیگر در پیرامون برنامه های کاربردی برنامه ریز واسطه ها درگیر می کنند. ماشین های مجازی اصولاً بعنوان واحد انتزاعی دخل و تصرف برای ابرهای IaaS بکار می رود و بصورت نا هماهنگی با معماری ذخیره ابری جفت و جور می شود . ایجادگر ابری همچنین سایر کیفیات انتزاعی محاسباتی در عوض فناوری ماشین مجازی به منظور تدارک سرویس ها برای هر مدل سرویسی دیگر می تواند، استفاده شود [۷].

برای پیاده سازی سمت سرور معادله ، برنامه های ابر محور به سمت مشتری معادله نیاز دارند تا سرویس ها را راه اندازی و کسب کنند . درحالیکه مرورگرهای شبکه اغلب بعنوان مشتری خدمت می کنند ، سایر احتمالات حذف می شود . علاوه بر آن زیر ساختار ارتباطات شبکه امن و دقیق باید در مکان مناسب قرار گیرند ، بسیاری از واسطه های ساده سازی شده و کیفیات انتزاعی سرویس در مورد مشتری سرور و شبکه مبتنی بر پیچیدگی ذاتی است که بر قضیه حریم خصوصی و امنیت تأثیر می گذارد . بنابراین حائز اهمیت است که تکنولوژیهای ایجادگر ابری استفاده می کند تا سرویس ها را تدارک بینند ، به درستی درک شوند و کنترل های تکنیکی مربوطه ، دلالت هایی بر امنیت و حریم خصوصی سیستم در سراسر چرخه عمرش دارند . با چنین اطلاعاتی معماری سیستمی بنیادین ابر می تواند تجزیه شود و بصورت چارچوبی از کنترل های امنیتی و حریم خصوصی که در ارزیابی و مدیریت بحران بکار می رود ، طراحی شوند [۷].

معماری مرجع (CCRA)، یک طرح تخصصی برای سیستم‌هایی که با دیدگاهی مناسب تعریف شده‌اند، ارائه می‌کند و همچنین نیازها را تأمین و تصمیمات معماری رو محقق می‌سازد. این مدل برای پروژه‌های پیشرفته دو مقوله سازگاری و کیفیت را ارائه و تضمین می‌کند .معماری مرجع رایانش ابری IBM طرحی برای خدمات ابری است که منابع و استفاده از نیروی کار را بهینه‌سازی نموده و طی عملیاتی به مقیاس اقتصادی دست می‌یابد. معماری مرجع رایانش ابری IBM مبتنی بر ورودی حقیقی مبتنی بر راه‌اندازی‌های ابری درون IBM است. این معماری اجزای بنیادی را تعریفت کرده و راهنمایی‌هایی برای ساخت محیط ابری ارائه و پشتیبانی می‌کند. معماری IBM از سه نقش اصلی تشکیل‌شده است که شامل مشتری (مصرف‌کننده) سرویس ابری، تأمین‌کننده سرویس ابری و سازنده سرویس ابری است. هر نقش می‌تواند توسط یک نفر یا گروهی از افراد یا توسط یک یا چند سازمان تحقق یابد [۱، ۷، ۸].

مشتری خدمات ابری یا یک سازمان، عامل انسانی یا سیستم IT است که مواردی از خدمات ارائه‌شده توسط تأمین‌کننده سرویس ابری خاص را مصرف می‌کند. علاوه بر این قابلیت‌ها و توانایی‌های IT به سبک غیر ابری سنتی مدیریت‌شده است. عملکرد ابزارهای تلفیق سرویس ابری برای یکپارچه‌سازی IT خانگی موجود با توجه به سرویس‌های ابری مصرف‌شده از تأمین‌کننده سرویس ابری موردنیاز است [۱، ۷، ۸].

تأمین‌کننده سرویس ابری مسئولیت ارائه خدمات ابری برای مشتریان این خدمات را دارا است. آن خدمات توسط سکوی مشترک مدیریت ابری [۲] چه با اجرای زیرساخت CCMP یا مصرف یک مورد به‌عنوان سرویس ارائه می‌گردند. سرویس‌های ابری هر نوعی از قابلیت IT تأمین‌شده توسط تأمین‌کننده سرویس ابری برای مشتریان خدمات ابری را نمایش می‌دهند. این خدمات خصوصیات ابری شامل سرویس مبتنی بر تقاضا، دسترسی شبکه‌ای گسترده، جمع‌آوری منابع، انعطاف سریع و سرویس اندازه‌گیری شده را در برمی‌گیرد [۸].

[۲] CCMP

لایه‌های IaaS، PaaS و SaaS توسط NIST تعریف‌شده است و BPaaS توسط IBM منتشرشده است. ازاین‌رو، خدمات فرایند کسب‌وکار هرگونه فرایند شغلی ارائه‌شده از طریق مدل سرویس ابری است [۸].

سکوی مشترک مدیریت ابری مجموعه‌ای از خدمات پشتیبان عملیاتی و خدمات پشتیبان کسب‌وکار را به معرض نمایش می‌گذارد. همچنین شامل سطوح کاربری است که سه نقش اصلی تعریف‌شده در مرجع رایانش ابری را ایفا می‌کند. این سه نقش اصلی شامل موارد ذیل است [۷، ۸]:

- پورتال مشتری خدمات که به‌وسیله مشتریان خدمات ابری برای ارائه سرویس و مدیریت مورداستفاده قرار می‌گیرد.
- پورتال تأمین‌کننده سرویس که در جهت منافع مدیران تأمین‌کننده عمل می‌کند تا حامی عملیات تولید باشد و پورتال پیشبردی بکار رفته توسط سازندگان سرویس ابری.
- خدمات پشتیبانی عملیاتی مجموعه‌ای از مدیریت عملیاتی و سرویس‌های مرتبط تخصصی نمایش داده‌شده توسط CCMP را بیان می‌کند. ازاین‌رو موردنیاز سازندگان خدمات ابری به‌منظور راه‌اندازی سرویس ابری است.

۱،۴. ساختارهای امنیتی رایانش ابری

ساختار و مکانیزم‌های امنیتی، از ویژگی‌های کلیدی در رایانش ابری است. این مفاهیم در راستای تحقق رسیدن به یک سرویس امن در رایانش ابری، کمک بلقوه‌ای خواهند کرد. شش عنصر کلیدی برای مدیران و سازمان‌های فناوری اطلاعات برای ساخت یک اکوسیستم ابر قابل اعتماد کمک می‌کند.سازمان‌ها باید این اکوسیستم رو درک کرده و ویژگی‌های یک اکوسیستم ابر قابل اعتماد را درک کنند و دستورالعمل‌های سازمان‌ها بر پایه این مدل باید ارائه شود. ساختن اعتماد در ابر نیاز به این دارد که به محیط ابری خودتان را ایجاد کنید. شکل ۲ این اکوسیستم را نشان داده است [۳، ۹].

شکل ۲ - اکوسیستم ابر قابل اعتماد [۹]

مباحث امنیتی رایانش ابری در ۸ بخش می‌تواند تقسیم‌بندی شود. این ۸ بخش شامل مفاهیم ذیل است. جدول ۲ به بررسی این ۸ فاکتور پرداخته است [۳].

- ذخیره‌سازی داده و محاسبه مسائل امنیتی
- مجازی‌سازی مسائل امنیتی
- اینترنت و خدمات مرتبط با مسائل امنیتی
- مسائل امنیتی شبکه
- مسائل کنترل دسترسی

- مسائل امنیت نرم‌افزاری
- مسائل مدیریت اعتماد و جنبه‌های انطباق و قانونی

جدول ۲ –بررسی مباحث امنیتی در رایانش ابری

نوع	توضیحات
ذخیره‌سازی داده و محاسبه مسائل امنیتی	موضوع ذخیره‌سازی داده، محاسبه غیر اعتماد، دسترسی داده و سرویس، رمزنگاری، بازیافت داده ابری و بدافزار
مجازی‌سازی مسائل امنیتی	مدیریت پشتیبانی ماشین مجازی، ناظر ماشین مجازی، مجازی‌سازی شبکه، سیار بودن، مسائل مربوط به ماشین مجازی و بدافزار
اینترنت و خدمات مرتبط با مسائل امنیتی	تهدیدات پیشرفته مکرر و خطرناک، پروتکل‌های اینترنت، سرویس‌های وب، تکنولوژی‌های وب و دسترسی سرویس
مسائل امنیتی شبکه	سکوهای موبایل و امنیت محیط
مسائل کنترل دسترسی	دسترسی فیزیکی، اعتبارنامه‌های کاربر، تصدیق سازمان، مجوز، مدیریت هویت کاربر و ناشناس شدن
مسائل امنیت نرم‌افزاری	سکو و چارچوب‌ها و پیشروی کاربر
مسائل مدیریت اعتماد	ابر نسبت به اعتماد ابر، جنبه انسانی، شهرت، اعتماد طبق گزارش‌های ممیزی و ناشناس شدن
جنبه‌های انطباق و قانونی	علوم قوانین مهم، قوانین، مسائل قانونی، سنجش مصرف نادرست و هدایت

همچنین، مهم‌ترین مسائل مهم امنیت و حریم خصوصی در جدول ۳ بررسی‌شده است. جدول ۳ خلاصه‌ای از آن مقولات و توصیه‌های مرتبط برای سازمان‌ها را ارائه می‌دهد تا در زمان طرح‌ریزی، مرور ، مذاکره یا آغاز مناسبات برون دادی سرویس ابری عمومی رعایت کند [۹].

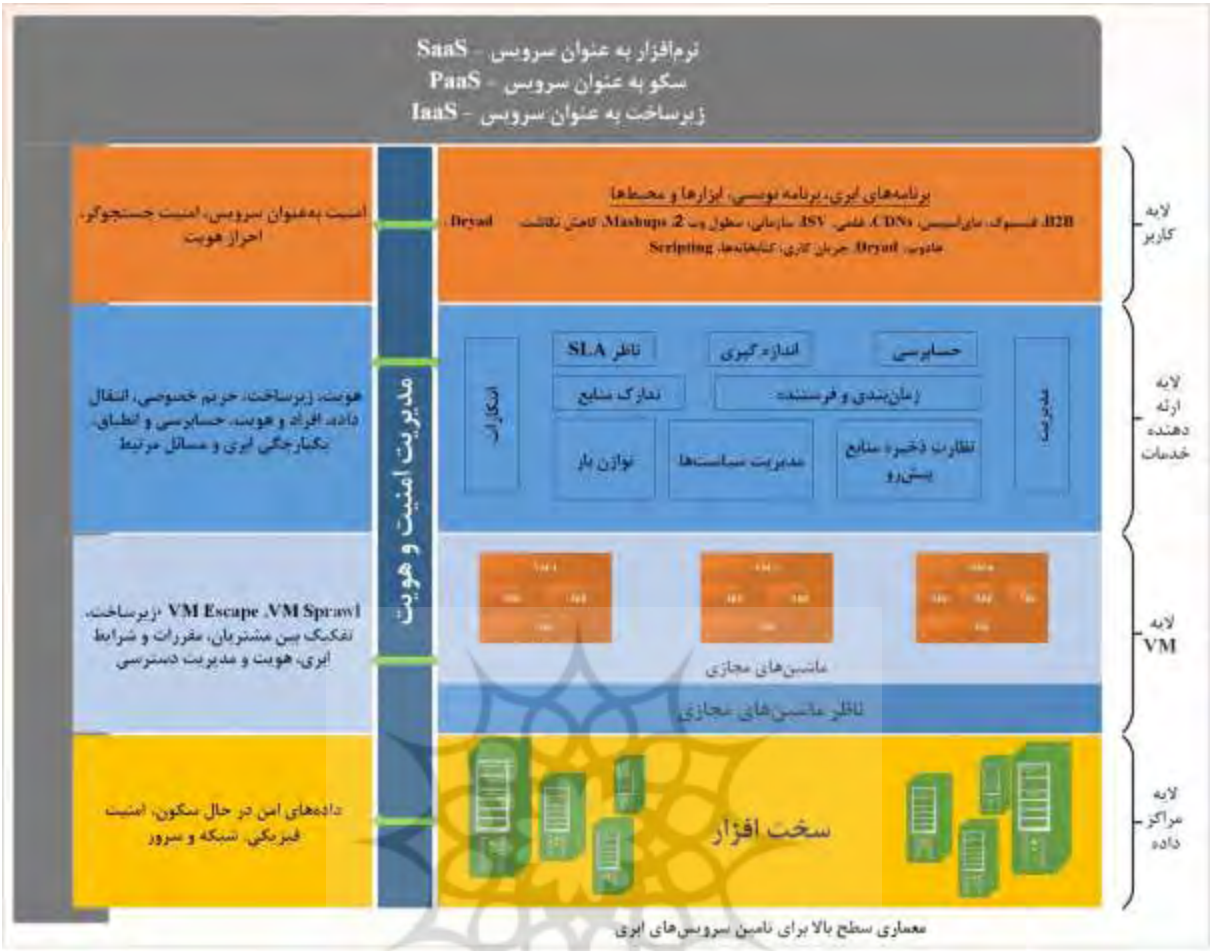
جدول ۳ - بررسی مسائل امنیتی و حریم خصوصی

نواحی	توصیات
دولت	گسترش دادن امورات سازمانی مربوط به خط مشی ها و روندهای اجرایی و استانداردهای بکار رفته برای توسعه برنامه کاربردی و تدارک سرویس در ابر ، همچنین ، طراحی ، پیاده سازی ، آزمون ، کاربری ، و نظارت سرویس های مورد استفاده یا مربوطه . بکارگیری مناسب ابزارها و مکانیزم بازرسی برای تضمین امورات سازمانی در سراسر چرخه عمر سیستم.
پذیرش	درک انواع مختلفی از قوانین و مقرراتی که الزامات امنیت و حریم خصوصی را در سازمان اعمال می کند وبطور بالقوه اقدامات محاسبات ابری ، بالاخص آنهایی که مربوط به موقعیت مکانی داده ، کنترل های امنیتی و حریم خصوصی ، مدیریت سوابق ، و الزامات کشف الکترونیک را تحت تأثیر قرار می دهند .

	مرور و ارزیابی راهنمایی ها و پیشنهاد های ایجادگر ابری با توجه به الزامات سازمانی برای انجام آنها و تضمین اینکه مفاد قرارداد بطور دقیق آن الزامات را تأمین می کند .
اعتماد	تضمین اینکه مناسبات سرویس از ابزاری مکفی برای صدور اجازه قابلیت رؤیت در داخل پروسه ها و کنترل های امنیتی و حریم خصوصی که توسط ایجادگر ابری بکار می رود، و اجرای آنها در طی زمان برخوردارند. تأسیس حقوق مالکیت انحصاری و بی ابهام بر روی داده نهادینه سازی برنامه مدیریت بحران که به حد کافی انعطاف پذیر برای سازگاری دائمی با ظهور و تغییر جهت چشم انداز بحران در چرخه عمر سیستم باشد. نظارت همیشگی و پیوسته حالت امنیت سیستم برای پشتیبانی از تصمیمات پیشرفته مدیریت بحران
معماری	درک فناوریهای تحت امری که ایجادگر ابری از آنها استفاده می کند تا سرویس ها را تدارک بیند ، که شامل دلالتهایی بر کنترل های تکنیکی مربوطه در امنیت و حریم خصوصی سیستم ، کل چرخهٔ عمر سیستم و سراسر اجزای سیستم می شود.
هویت و دسترسی	تضمین اینکه حراست های کافی در موقعیت مناسب حضور داشته باشند تا اعتبار سنجی ، سندیت و سایر عملکردهای مدیریت هویت و دسترسی را امن نمایند ،و متناسب با آن سازمان باشند.
جداسازی نرم افزاری	درک مجازی سازی و سایر فناوری های منطقی جدا سازی که ایجادگر ابری در معماری نرم افزار چند مستأجری اش بکار می گیرد ، و ارزیابی مخاطرات و بحران ها مربوطه به سازمان
پشتیبانی داده	ارزیابی تناسب راه حل های مدیریت بحران ایجادگر ابری با داده سازمانی مربوطه و توانایی کنترل دسترسی به داده ، به منظور حفاظت از داده در مرحله انتقال و مصرف ، و به منظور پاکسازی داده در نظر گیری خطر تلفیق داده سازمانی با داده های سایر سازمان هایی که احتمال تهاجم به پروفایل هایشان بسیار بالاست یا داده هایشان بصورت انباشتی ارزش متمرکز قابل ملاحظه ای را ارائه می دهند . درک کامل وسنجش مخاطرات مربوطه به مدیریت کلیدی کد نویسی با تسهیلات در دسترس محیط ابری و پروسه های احراز شده توسط ایجادگر ابری
دسترس پذیری	درک رویه های اجرایی و تدارکات قراردادی برای دسترس پذیری ، روگرفت داده و بازیابی ، و بازیابی حادثه ، و تضمین اینکه آنها الزامات طرح ریزی احتیاطی و مداومت عملیات سازمان را تأمین می کند . تضمین اینکه طی اختلال طولانی یا متوسط یا فاجعه جدی ، عملیات های بحرانی فوراً ادامه یابند واینکه تمام عملیات در نهایت به روشی سازمان یافته و به هنگام دوباره برقرار گردد .
پاسخ گویی به یک اتفاق	درک رویه های اجرایی و تدارکات قراردادی برای پاسخ گویی به اتفاقی یا تضمین اینکه آنها الزامات سازمان را تأمین می کنند تضمین اینکه ایجادگرابری پروسه پاسخگویی شفاف و مناسب ، و مکانیزم های کارا برای اشتراک اطلاعات در طی و بعد از حادثه داشته باشد. تضمین اینکه سازمان به اتفاقات به روشی هماهنگ با ایجادگر ابری برطبق نقش ها ومسئولیت های مربوطه شان برای محیط ابری پاسخ گو باشد.

۵. بررسی و ارائه راهکار معماری امنیتی رایانش ابری

دیدگاه معماری از مسائل امنیتی به‌منظور بررسی در محیط رایانش ابری و به‌منظور تامین امنیت مشتری است. در این رابطه، ۴ لایه مبتنی بر دسته بندی رایانش ابری شناسایی شده است. دسته بندی رایانش ابری مبنی بر سرویسهایی بصورت نرم‌افزار بعنوان سرویس، سکو بعنوان سرویس و زیرساخت بعنوان سرویس صورت پذیرفته است. این بخش ۴ لایه مشخص در شکل ۳ طراحی مسائل امنیتی متفاوت در هر لایه را شفاف سازی می نماید [۱۰، ۱۱].



شکل ۳ –معماری امنیتی رایانش ابری [۱۰]

با توجه به مسائل بیان شده در زمینه معماری رایانش ابری و بررسی ساختارهای امنیتی در این حوزه، در ادامه به بررسی کارهای پژوهشگران در زمینه معماری امنیتی رایانش ابری پرداخته شده است. همچنین، جدول ۴ به بررسی کامل معماری-های امنیتی رایانش ابری و ارائه راهکارهایی برای بهبود در حوزه دفاعی پرداخته است.

رایانش ابری (ابر) به طور گسترده‌ای برای ذخیره و پردازش داده‌های بزرگ (کلان داده[۳]) مورد استفاده قرار می‌گیرد. بسیاری از محققان در تلاش برای محافظت و بهبود داده‌های بزرگ در محیط رایانش ابری هستند. مکانیزم‌های سنتی امنیتی با استفاده از رمزنگاری به منظور محافظت داده‌های بزرگ در ابرها، ناکارآمد و نامناسب هستند. در این مقاله، ابتدا درباره چالش‌ها و راه‌حل‌های بالقوه برای محافظت از داده‌های بزرگ در رایانش ابری بحث شده است. دوم؛ این مقاله یک معماری امنیتی مبتنی بر رایانش ابری به نام معماری MetaCloudDataStorage برای محافظت از داده‌های بزرگ پیشنهاد داده است. این معماری بر پایه‌ی یک چارچوب جهت پردازش کارآمد داده های بزرگ در محیط رایانش ابری را تضمین می‌کند. از-این‌رو، سازمان‌ها و ارائه دهندگان خدمات ابری در زمینه کسب و کار توسعه بیشتری را به دست می‌آورند [۱۲].

همچنین در این مقاله از چارچوب Map Reduce برای پیدا کردن تعداد کاربرانی که به مرکز داده ابری وارد شده‌اند، استفاده شده است. چارچوب پیشنهادی با استفاده از رابط MetaCloudDataStorage به هر ارائه‌دهنده ابری، نگاشتی از

[۳] Big Data

عناصر داده‌های مختلف را نشان داده و محافظت می‌کند. با توجه به نظرات محققین این مقاله، این رویکرد پیشنهادی نیاز به تلاش زیادی در زمینه پیاده سازی دارد، اما اطلاعات ارزشمندی برای رایانش ابری محسوب می‌شود که می‌تواند بر سیستم‌های نسل آینده تاثیر بگذارد. به عنوان یک کار برای آینده این طرح این است که معماری MetaCloudDataStorage از جریان داده‌ها برای پردازش زمان واقعی گسترش پیدا کند [۱۲].

این مقاله یک چارچوب تطبیق‌دهنده رایانش ابری[۴] مبتنی بر امنیت سازگار برای ابرهای کسب‌وکار را ارائه داده است. معماری CCFA از چندین لایه امنیتی براساس توسعه و یکپارچگی ساخته شده است. همچنین از سه تکنولوژی امنیتی: فایروال، مدیریت احرازهویت و رمزنگاری بر اساس توسعه همگام سازی فایل سازمانی و به اشتراک گذاری فناوری‌ها در راستای ایجاد یکپارچگی و توسعه استفاده کرده است. در این مقاله هسته فناوری‌ها به تفصیل توضیح داده شده‌اند و آزمایش‌ها برای نشان دادن استحکام امنیتی چند لایه معماری CCAF طراحی شده‌اند. در آزمایش نفوذ صورت گرفته در این مقاله، امنیت چند لایه CCAF می‌تواند ۹۹,۹۵٪ ویروس‌ها و تروجان‌ها را شناسایی و مسدود سازد. تشخیص و مسدود کردن زمان شناسایی ویرویس ها و بدست آوردن زمان برای حملات مسدود شده در این آزمایش موفق بوده است. معماری چندلایه CCFA پیشنهادی به طور کامل می‌تواند حملات تزریق SQL را متوقف کرده و داده‌ها را به صورت دقیق و واقعی محافظت کند. همچنین این معماری هیچ پیغام اشتباهی را گزارش نمی‌کند. دقت معماری پیشنهادی این مقاله در آزمایش‌های صورت گرفته، ۹۹,۷۵ درصد است. مکانیسم ترکیبی معماری چندلایه امنیتی CCAF با سیاست، خدمات واقعی و فعالیت‌های تجاری نشان داده شده است. ایده‌های این معماری می‌تواند حجم، سرعت و خدمات کلان داده در ابرها تضمین کند و همچنین برای امنیت رایانش ابری مفید باشد. با توجه به بررسی‌های انجام شده، این مقاله یک رویکرد امنیتی یکپارچه بر اساس معماری پیشنهادی چند لایه امنیتی CCAF را نشان داده است. این پژوهش برای نشان دادن معماری امنیتی چند لایه CCAF به عنوان یک چارچوب کاری برای ابرهای تجاری، آزمایشات و طراحی بررسی شده است. به عنوان کار آینده این مقاله پیشنهاد داده است که یک همکاری بین المللی از طرف خود با شرکای کشورهای مختلف تقویت کنند و اثبات‌های متفاوتی از مفاهیم، نمونه‌های اولیه، خدمات و مشاوره تحقیقاتی را با با همکاران مشابه‌شان ایجاد کنند [۱۳].

چگونگی اطمینان از امنیت شبکه برای ماشین‌های مجازی مدرت مبتنی بر سکوهای رایانش ابری، هنوز هم یک سوال مبهم و بی پاسخ است. جواب دادن به این سوال مهم به توسعه رایانش ابری در سال‌های اخیر و آینده کمک خواهد کرد. اگرچه در سال‌های اخیر راه‌حل‌هایی به صورت ناقص (نادیده گرفتن ویژگی‌های مهم رایانش ابری) ارائه شده است. در این مقاله، یک معماری امنیتی شبکه برای رایانش ابری[۵] مبتنی بر ویژگی‌های آن ارائه شده است. به طور مشخص [۱۴]:

۱) حفاظت از ترافیک داخلی و خارجی را در محاسبات ابری فراهم می‌کند (حفاظت از حملات داخلی و خارجی)

۲) با توجه به بارگذاری مجدد مجازی باعث مقیاس پذیری قابل انعطاف می‌شود (مقایس‌پذیری انعطاف‌پذیر)

۳) بدست آوردن تحمل خطا بین خطاهای موجود در مجازی سازی (قابلیت موثر در تحمل خطا)

نتایج و آزمایش‌ها از نمونه اولیه معماری NetSecCC نشان داده است که این معماری موثر با سربار کاری کم است و می‌توان آن را جهت ارتقاء گسترده‌ای در رایانش ابر پیاده‌سازی کرد. ازاین‌رو، این مقاله یک معماری جهت اطمینان از امنیت شبکه در رایانش ابری را پیشنهاد کرده است. معماری پیشنهادی NetSecCC به طور مشخص سه نقطه ضعف اشاره شده را بهبود داده است. این معماری توانسته یک حفاظت و امنیت جامعتری را برای رایانش ابری فراهم می‌کند. ازاین‌رو در آینده می‌توان تحقیقاتی امنیتی تحت شبکه رایانش ابری انجام داد [۱۴].

امنیت یک نگرانی اساسی در رایانش ابری است. تعدادی از ارائه دهندگان خدمات ابری، برای توصیف سطح امنیتی خدمات خود، معماری مرجع امنیتی (SRAs) را پیشنهاد کرده‌اند. معماری SRA یک معماری انتزاعی بدون جزئیات اجرایی است که

---

[۴] CCAF

[۵] NetSecCC

یک مدل مفهومی امنیت برای سیستم ابری را نشان می‌دهد. به طور کلی، معماری ارجاع (RAs) در حال تبدیل شدن به ابزار مفیدی برای درک و ساخت سیستم‌های پیچیده است. این مقاله یک معماری مرجع امنیتی (SRA) ارائه کرده است که با استفاده از مدل‌ها و الگوهای UML تعریف شده است. همچنین، یک رویکرد خاص برای ساختن سیستم‌های ایمن را در برمی‌گیرد. این مقاله یک مدل افزوده و یک الگوی قابل اجرا را ارئه کرده است که این رویکرد را مفهومی کرده‌اند. برخی از کاربردهای SRA شامل ارزش‌های SLA، گواهی خدمات و نظارت و ارزیابی امنیتی است که این مقاله این جزئیات را نشان داده است. به‌همین‌دلیل برای ساخت یک معماری مرجع امنیتی قوانین و جزئیاتی نیاز است. که این حزئیات میتواند باعث کاهش هزینه و توسعه سیستم‌های ابری شود [۱۵]:

- یک راه برای درک یک سیستم پیچیده مانند یک ابر امن
- نمای کلی امنیتی
- راهی برای متحد کردن اصطلاحات ابر
- انتخاب ارائه دهندگان ابر بر اساس الزامات امنیتی
- توافقنامه سطح خدمات (SLA)
- گواهی خدمات
- ارزیابی امنیتی
- مدیریت امنیت
- واسط ابری
- یکپارچگی انواع دستگاه‌ها
- فدراسیونی از چندین ابر

این مقاله معتقد است که SRA بسیار مهم هستند و برای بهبود امنیت رایانش ابری باید مورد تحقیق قرار گیرند. تهیه مراجع خوب برای الگوهای امنیتی بسیار مهم است که به طراحان و معماران کمک می‌کند تا از معماری مرجع برای اضافه کردن امنیت و ارزیابی امنیت رایانش ابری و نیز ساختن SLA استفاده کنند [۱۵].

جدول ۴ – بررسی و ارائه راهکارهایی جهت بهبود معماری امنیتی رایانش ابری در حوزه دفاعی

مرجع	معماری پیشنهادی	نقاط قوت و ضعف	راه کارهای توسعه پیشنهادی
[۱۲]	یک معماری امنیتی مبتنی بر رایانش ابری به نام معماری MetaCloudDataStorage بر پایه‌ی چارچوب Map Reduce.	محافظت از داده‌های بزرگ. پردازش کارآمد داده های بزرگ. پیدا کردن تعداد کاربرانی که به مرکز داده ابری وارد شده‌اند.	از جریان داده‌ها برای پردازش زمان واقعی گسترش پیدا کند.
[۱۳]	یک چارچوب تطبیق‌دهنده رایانش ابری (CCAF) مبتنی بر امنیت سازگار برای ابرهای کسب‌وکار. همچنین از سه تکنولوژی امنیتی: فایروال، مدیریت احرازهویت و رمزنگاری استفاده کرده است.	شناسایی و مسدود ۹۹,۹۵٪ ویروس‌ها و تروجان‌ها. تشخیص و مسدود کردن زمان شناسایی ویرویس ها و بدست آوردن زمان برای حملات مسدود شده در این آزمایش موفق بوده است.	تقویت یک همکاری بین المللی از طرف خود با شرکای کشورهای مختلف و ایجاد اثبات‌های متفاوتی از مفاهیم، نمونه‌های اولیه، خدمات و مشاوره تحقیقاتی.
[۱۴]	یک معماری امنیتی شبکه برای رایانش ابری (NetSecCC) با	حفاظت از حملات داخلی و خارجی .	تحقیقاتی امنیتی تحت شبکه رایانش ابری.

	توجه به ویژگی‌های رایانش ابری.	مقایس‌پذیری انعطاف‌پذیر. قابلیت موثر در تحمل خطا.	
[۱۵]	یک معماری انتزاعی به نام SRA بدون جزئیات اجرایی که یک مدل مفهومی امنیت برای سیستم ابری را نشان می‌دهد.	کاهش هزینه و توسعه سیستم‌های ابری. متحد کردن اصطلاحات ابر. یکپارچگی انواع دستگاه‌ها.	تهیه مراجع خوب برای الگوهای امنیتی
[۱۶]	نرم‌افزار را بصورت یک سرویس ابری سازمانی (SaaS) تحلیل نموده و موقعیت تحقیقی از مشکلات امنیتی را در محیط رایانش ابری معرفی می‌کند.	پشتیبانی از تحقیقات بعدی نسل سیار از راه‌حل‌ها. هدایت بکارگیری سیاست‌های امنیتی سرویس‌های ابری سازمانی SaaS.	سرویسهای رایانش ابری سازمان بیشتر به امنیت اطلاعاتی ارائه شده توسط کاربران توجه دارند، از ایم رو باید بر مقوله مقیاس پذیری بیشتر توجه شود.
[۱۷]	یک معماری مبتنی بر سکو به عنوان سرویس (PaaS) مورد اعتماد جهت توسعه امنیت.	بهبود امنیت داده و تهدیدات حریم خصوصی. قابل اعتماد برای پایگاه داده های شخصی.	این مدل باید با پروتکل های امنیتی مختلف بررسی شود و همچنین با سیاست های کنترل دسترسی یکپارچه شود.
[۱۸]	یک طرح مبتنی بر رمزنگاری کارآمد، قابل‌دسترس و قابل‌انعطاف.	در قبال تغییرات در اطلاعات و ناامنی در اطلاعات به‌خوبی عمل می‌کند. این طرح مقیاس‌پذیر و انعطاف‌پذیر است.	استفاده از رمزنگاری مبتنی بر مفاهیم کوانتومی برای بهبود امنیت.
[۱۹]	این مقاله به‌عنوان یک چارچوب معماری امنیتی سعی در حل تقسیم مسئولیت‌ها بر اساس الزامات امنیتی در معماری رایانش ابری را دارد.	تقسیم بندی مسئولیت ها و انعطاف پذیری در راستای سیاست های امنیتی سازمان	از نیازهای ضروری این طرح برای آینده کاهش هزینه‌ها و پردازش-های اضافی محاسبات است
[۲۰]	یک سرور سخت‌افزار افزایشی برای کمک جهت حفاظت از کدها و داده.	از بین بردن نیاز به یک‌لایه مجازی‌سازی در طول زمان اجرا مجازی ماشین. بهبود سخت‌افزار. مدیریت پویا منابع سرور. افزایش اعتماد صحت معماری‌های سخت افزاری و نرم‌افزاری و تسهیل ارتقاء طراحی به سخت‌افزار.	بهبود مقوله‌هایی همانند بسیاری از سیستم‌های اصلی وقفه، بهبود سرعت و زمان سیستم، بهبود دستورالعمل‌های محرمانه و بهبود واسط برای سخت‌افزارهای مجازی. توسعه پارامترهایی نظیر اتوماتیک کردن تائید امنیتی، گسترش این مقوله در برابر انواع حملات و ترکیب پروتکل‌ها.
[۲۱]	یک معماری سیستم ابری جدید به نام CypherDB، برای حفاظت از محرمانه بودن پردازش برون‌سپاری	می‌تواند توسط یکپارچگی با SQLite، یک برنامه کاربردی پایگاه داده کاربردی قابل‌اعتماد	پژوهش در مقوله‌هایی همانند معماری چندهسته‌ای، برنامه کاربردی هدف یافته، پشتیبانی از

	پایگاه داده	باشد. مقرون‌به‌صرفه و دارای عملکرد (کارایی) بالا.	کامپایلرها، سوئیچ کردن مبتنی بر متن و حفاظت از حملات تزریق کد در بهبود امنیت رایانش ابری.

۶. نتیجه‌گیری

رایانش ابری سرویس بروی اینترنت با منابع مقیاس پذیر دینامیک ارائه می‌دهد. تهیه‌کنندگان سرویس رایانش ابری، مزایایی برای کاربران از نظر هزینه و برنامه‌های مهمی برای محیط‌های ابری مشترک و عمومی تامین می‌کند. محیط‌های ابری، مقیاس پذیری بالایی برای پردازش داده و نیازهای ذخیره سازی دارند. محیط رایانش ابری مزایا و معایب متعددی از لحاظ امنیت داده‌ای کاربران سرویس دارد. به همین دلیل اصول امنیت ابر طبق معماری رایانش ابری طبقه بندی می گردد. به هیمن دلیل، این مقاله در راستای بهبود معماری سازمان‌های امنیتی، به بررسی و ارائه‌ی راهکارهایی جهت توسعه معماری امنیتی رایانش ابری پرداخته است.

مراجع

۱. Mell, P., & Grance, T. (۲۱۱۱). The NIST definition of cloud computing.

۲. Erl, T., Puttini, R., & Mahmood, Z. (۲۱۱۳). *Cloud computing: concepts, technology & architecture*. Pearson Education.

۳. Carlin, S., & Curran, K. (۲۱۱۳). Cloud computing security. In Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments (pp. ۱۲-۱۷). IGI Global.

٤. Zhang, H., Han, W., Lai, X., Lin, D., Ma, J., & Li, J. (۲۱۱٥). Survey on cyberspace security. Science China Information Sciences, ٥٨(۱۱), ۱-٤۳.

٥. Badger, L., Bernstein, D., Bohn, R., De Vaulx, F., Hogan, M., Iorga, M., ... & Sokol, A. (۲۱۱٤). US government cloud computing technology roadmap. US Department of Commerce, National Institute of Standards and Technology.

٦. Zhao, W., Peng, Y., Xie, F., & Dai, Z. (۲۱۱۲, November). Modeling and simulation of cloud computing: A review. In ۲۱۱۲ IEEE Asia Pacific cloud computing congress (APCloudCC) (pp. ۲۰-۲٤). IEEE.

۷. Jadeja, Y., & Modi, K. (۲۱۱۲, March). Cloud computing-concepts, architecture and challenges. In ۲۱۱۲ International Conference on Computing, Electronics and Electrical Technologies (ICCEET) (pp. ۸۷۷-۸۸۰). IEEE.

۸. Stifani, R. A. F. F. A. E. L. E., Pappe, S. T. E. F. A. N., Breiter, G. E. R. D., & Behrendt, M. I. C. H. A. E. L. (۲۱۱۲). Ibm cloud computing reference architecture. IBM Academy of Technology, ۳(۱), ۱-۱٦.

۹. Popović, K., & Hocenski, Ž. (۲۰۰۰, May). Cloud computing security issues and challenges. In The ۳۳rd International Convention MIPRO (pp. ۳٤٤-۳٤۹). IEEE.

۰۰. Okuhara, M., Shiozaki, T., & Suzuki, T. (۲۰۰۰). Security architecture for cloud computing. Fujitsu Sci. Tech. J, ٤٦(٤), ۳۹۷-٤۰۲.

۱۱. Chen, J., Wang, Y., & Wang, X. (۲۱۱۲). On-demand security architecture for cloud computing. Computer, ٤٥(۷), ۷۳-۷۸.

۱۲. Manogaran, G., Thota, C., & Kumar, M. V. (۲۱۱٦). MetaCloudDataStorage architecture for big data security in cloud computing. Procedia Computer Science, ۸۷, ۱۲۸-۱۳۳.

۱۳. Chang, V., Kuo, Y. H., & Ramachandran, M. (۲۱۱٦). Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, ٥۷, ۲٤-٤۱.

۱٤. He, J., Dong, M., Ota, K., Fan, M., & Wang, G. (۲۱۱٦). NetSecCC: A scalable and fault-tolerant architecture for cloud computing security. Peer-to-Peer Networking and Applications, ۹(۱), ٦۷-۸۱.
۱٥. Fernandez, E. B., & Monge, R. (۲۱۱٤, April). A security reference architecture for cloud systems. In Proceedings of the WICSA ۲۱۱٤ Companion Volume (p. ۳). ACM.
۱٦. Niu, D. D., Liu, L., Zhang, X., Lü, S., & Li, Z. (۲۱۱٦). Security analysis model, system architecture and relational model of enterprise cloud services. International Journal of Automation and Computing, ٦(۱۳), ٥۷٤-٥٤٤.
۱۷. Niu, D. D., Liu, L., Zhang, X., Lü, S., & Li, Z. (۲۱۱٦). Security analysis model, system architecture and relational model of enterprise cloud services. International Journal of Automation and Computing, ٦(۱۳), ٥۷٤-٥٤٤.
۱۸. Gupta, S. K., Rawat, S., & Kumar, P. (۲۱۱٤, October). A novel based security architecture of cloud computing. In Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), ۲۱۱٤ ۳rd International Conference on (pp. ۱-٦). IEEE.
۱۹. Drozdova, M., Rusnak, S., Segec, P., Uramova, J., & Moravcik, M. (۷۱۱۷, October). Contribution to cloud computing security architecture. In Emerging eLearning Technologies and Applications (ICETA), ۷۱۱۷ ۱٥th International Conference on (pp. ۱-٦). IEEE.
۲۰. Szefer, J. M. (۲۱۱۳). Architectures for secure cloud computing servers (Doctoral dissertation, Princeton University).
۲۱. Chen, H. K. (۲۱۱٦). A novel architecture for secure database processing in cloud computing. HKU Theses Online (HKUTO).