مسائل امنیتی در سطوح مختلف پارادایم رایانش ابری: یک مقاله مروری

چکیده :

رایانش ابری امروزه به یک شعار در صنعت فناوری اطلاعات تبدیل شده است و سازمان ها به سمت این قطب برای توسعه زیر ساخت آن ها به نرخ ارزان تر جذب شده اند. با این حال، با همه انعطاف پذیری ارایه شده توسط ابر، نگرانی هایی در خصوص امنیت، یکپارچگی، صحت و قابلیت دسترسی اطلاعات ارزشمند کاربران ابری وجود دارد. مکانیسم های حفاظت سنتی باید از نظر کارایی و اثر بخشی خود مجددا در نظر گرفته شوند زیرا مدل سرویس ابری به شدت متمایز از سایر مدل های سرویس های مبتنی بر اینترنتی است. اخیرا، تحقیقات زیادی در امنیت ابری انجام شده اند با این حال تلاش های زیادی در این رابطه نیاز است. چون امنیت ابر یک بعد حساسی است که بر پذیرش تجاری آن اثر گذاشته است. این مطالعه به بررسی سطوح مختلف نگرانی های امنیتی در محیط ابری پرداخته و فهرستی از مکانیسم های موجود را برای رسیدگی به آن ها ارایه می کند.

لغات کلیدی: رایانش ابری، مسائل امنیتی، سطوح، مقاله مروری

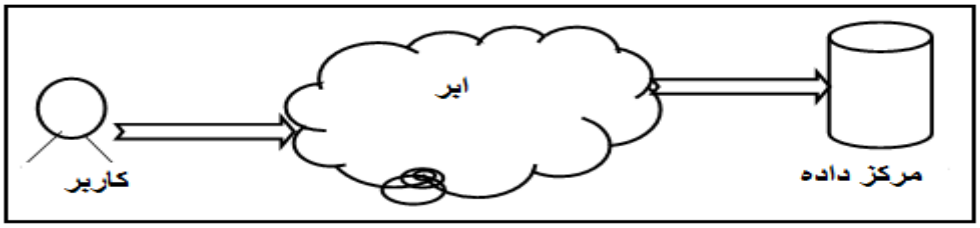
1- مقدمه

زیر ساخت به عنوان خدمات (IaaS)، به خصوص ذخیره داده ها، یکی از خدمات مهم ارایه شده توسط رایانش ابری است (CC). کاربران فردی و سازمان های کسب و کار در حال تغییر ذخیره داده ها در مورد ابر به دلیل قابلیت دسترسی آسان و کاهش هزینه ارایه شده توسط آن(1) می باشد. با این حال، ذخیره سازی داده ها در یک سرور از راه دور همانند دادن پول به یک نفر می باشد زیرا در دوره دیجیتال امروزه، داده ها، ستون اصلی پردازش هستند. از این روی با همه انعطاف پذیری ارایه شده توسط ابر، نگرانی های امنیتی مختلف نیز ایجاد شده اند. مسائل امنیتی امروزه یک مانعی برای سازمان های کسب و کار برای تغییر به ابرهای عمومی می باشند(2). اخیرا، توجه زیادی از طرف جوامع تجاری و پژوهشی به توسعه ابزار های امنیتی مهم برای پارادایم ابری صورت گرفته است. برخی از سازمان ها نظیر اتحادیه امنیتابر (CSA)،آژانسشبکهواطلاعات(ENISA) [3]، اروپا، گروهقابلیتهمکاریرایانش ابریوانجمن چند آژانسی رایانش ابری در حال ارایه کنترل های موثر و کارامد

برای ایجاد امنیت اطلاعات در محیط ابری می باشند. برخی از مسائل امنیتی مهم در این حوزه شامل امنیت داده ها، حریم خصوصی، قابلیت دسترسی به منابع، مدیریت اعتماد و غیره می باشد. با این حال، اخیرا تعداد زیادی از محققان روش هایی را برای بهبود امنیت اطلاعات پیشنهاد کرده اند با این حال یک حوزه تحقیقاتی در این رابطه وجود دارد. این مطالعه به بررسی مسائل امنیتی در محیط ابری پرداخته و راه حل هایی را ارایه می دهد. بخش بعدی در خصوص مسائل امنیتی در سطوح مختلف رایانش ابری می باشد. بخش سوم بر راه حل های موجود برای این مسائل تاکید دارد. در نهایت بخش آخر شامل نتیجه گیری بود و مطالعات آینده را شامل میشود.

2- مسائل امنیتی در سطوح مختلف در رایانش ابری

CC پارادایم خدمات مبتنی بر اینترنتی است که در آن کاربران به سطوح مختلف عرضه کننده خدمات ابری از طریق اینترنت دسترسی دارند. وقتی که کاربر وارد ابر می شود و شروع به دسترسی به خدمات مختلف می کند، تبادل اطلاعات بین کاربر و CSP شروع می شود. شکل 1 در زیر یک محیط رایانشی را نشان می دهد



شکل 1: محیط ابری

تا جایی که امنیت اطلاعات مبادله شده مورد نگرانی است، ذخیره ابری جای نگرانی ندارد. سطوح متعددی وجود دارد که در آن نقض امنیت رخ داده و صحت اطلاعات به خطر می افتد. شکل 2، در زیر سطوح مختلف مسائل امنیتی را در محیط ابری نشان می دهد.

هر سطح در بر گیرنده نقاط کلیدی در سطوح مختلف است. همه سطوح دارای اهمیت خاص خود بوده و نیاز مند توجه برابری برای اطمینان از امنیت قوی در محیط های ابری هستند. شکل 3 در زیر برخی از سطوحی را نشان می دهد که نیاز مند امنیت با مسائل اساسی مربوطه هستند.

شکل 3: امنیت در ابر ها: سطوح و مسائل

امنیت شبکه	• تامین امنیت انتقال داده ها • تسهیم داده ها با کاربران مجاز • شفاف سازی پروتکل های امنیتی
امنیت رابط	• تامین امنیت رابط کاربر • تقویت رابط مدیریتی • تامین امنیت رابط برنامه نویسی برنامه
امنیت ماشین مجازی	• مدیریت ماشین مجازی • مجازی سازی • شناسایی VM
انطباق	• توافق سطح سرویس استاندارد • حسابرسی • مدیریت اعتماد در میان شرکت کننده ها
حریم خصوصی	• حریم خصوصی مکان یابی داده ها • روش های رمزگذاری برای امنیت داده ها • بک اپ های مخفی و اضافی از داده ها

توصیف مسائل امنیتی مختلف به صورت زیر است

2-1 امنیت شبکه

وقتی که اطلاعات در شبکه جران می یابد، آن گاه امنیت شبکه به یک نگرانی تبدیل می شود. عرضه کننده های رایانش ابری باید اطمینان حاصل کنند که پروتکل ارتباطی ایمن و قوی برای اجتناب از حملات به اطلاعات ضمن انتقال در شبکه استفاده می شود.

2-2 امنیت رابط

این مستقیما مربوط به رابط است که توسط عرضه کننده های ابر و سطح امنیت عرضه ارایه می شود. رابط VM بر ویژگی های امنیت ذاتی نظیر IBM Blue Mix تاثیر می گذارد که مورد اخیر یک سرویس ابری مبتنی بر لینوکس است و مایکروسافت ایژر بر اساس سیستم عامل ویندوز است. سیستم عامل لینوکس در مقایسه با ویندوز مایکروسافت ایمن تر است و از این روی امنیت رابط با رابط مبتنی بر لینوکس بهتر است. از این روی رابط ارایه شده توسط CSP باید از سیستم عامل امن استفاده کند.

2-3 امنیت ماشین مجازی

امنیت VM یکی از برجسته ترین نگرانی ها و مسائل در میان همه مشکلات امنیتی است. کاربران از VM برای انجام کار های پردازشی استفاده می کنند. به علاوه، یک ابر می تواند از روش چند اجاره ای استفاده کند یعنی منابع و ,VM های یکسان توسط کاربران مختلف در نقاط زمانی متعدد برای بهبود مصرف منابع و کاهش هزینه استفاده می شوند. با این حال این موضوع باعث افزایش احتمال نقض امنیت می شود. کاربران مختلف ماشین های مجازی باید تفکیک شوند به طوری که محرمانگی فرد را می توان حفظ کرد.

2-4 انطباق

انطباق بر اجرای توافق نامه سطح خدماتی(SLA) تاکید دارد. SLA یک سند حقوقی بین کاربر و عرضه کننده کاربر است که بیان گر نیاز های خدماتی کاربر و استاندارد های خدماتی ارایه شده توسط ارایه کننده است. با این حال، یک استاندارد سازی کلی از SLA وجود ندارد که برای امن کردن این مدل کسب و کار مفید باشد. پیاده سازی ضعیف استاندارد های خدماتی توسط عرضه کننده می تواند منجر به مشکلات امنیتی شود.

2-5 محرمانگی/حریم خصوصی

محرمانگی بر پیشیگیری از افشای اطلاعات خصوصی به کاربران غیر مجاز تاکید دارد. در رایانش ابری، همه داده ها به طور مجزا ذخیره شده و از این روی موجب حفظ محرمانگی داده ها می شود. استفاده از الگوریتم های رمز نگاری مختلف(5) یک راه حل می باشد. تقسیم داده ها(6) یک روش قوی برای اطمینان از امنیت داده ها می باشد. در این روش، داده ها در میزبان ها و هاست های غیر متعامل مختلف ذخیره می کنند. با این حال، هر دو روش فوق دارای مشکلات خاص خود هستند.

همه مشکلات امنیتی فوق اهمیت زیادی در سطوح مختلف ارتباطی با ابر دارند.CSP باید از امنیت در همه سطوح اطمینان حاصل کند. بخش بعدی به تحلیل راه حل های موجود برای مسائل امنیتی فوق می پردازد.

3- مکانیسم های امنیتی موجود در منابع

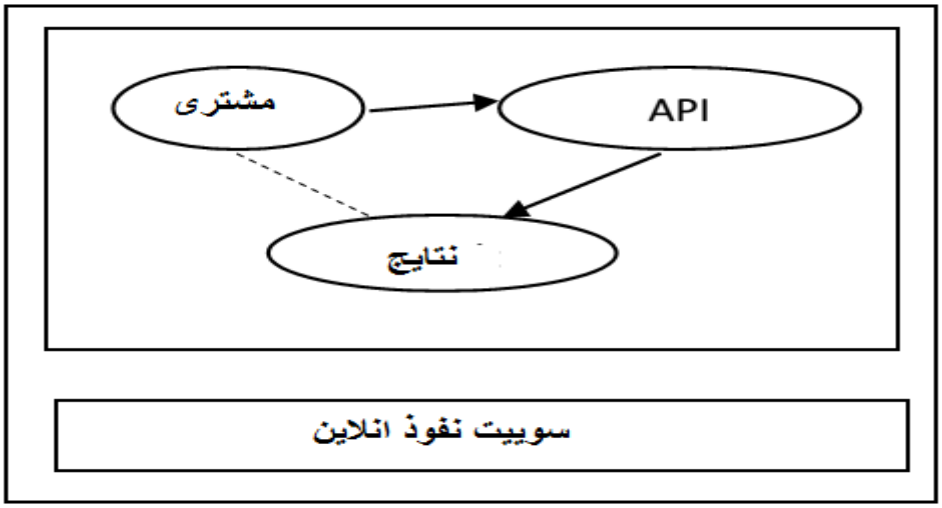
3-1 به سمت امنیت شبکه

ارفین و همکاران(7) بر آگاهی شبکه و بهینه سازی پایدار راهبرد های تخصیص منابع تاکید کردند و بر مسائل تحقیقاتی غالب در این رشته متمرکز شده اند. محققان تاکید کرده اند که تلاش های بیشتری برای بهبود پیش بینی مدل های عملکرد و افزایش حساسیت آن ها لازم است. سافیرا(8) یک پروتکل مدیریت هویت کاربر(UIDM) را در پارادایم ابری ارایه کرده اند. این خود در بر گیرنده همه ذی نفعان می باشد کاربران نهایی و عرضه کننده ها. این مدل شامل احراز هویت، رمز گذاری و مکانیسم مدیریت کلیدی است. آن ها دارای هویت کاربر ضعیف، قوی و بسیار قوی هستند و در موارد IDM ضعیف با شکست مواجه شده اند. زن و همکاران(9) یک سیستم نمونه امنیتی مشارکتی مورد استفاده در مرکز داده های چند جزیی ارایه کرده اند. آن ها از طرح مشارکتی متمرکز با بازرسی بسته در سطوح مختلف امنیت استفاده کرده اند . این مدل از مرکز داده ها از همه حملات احتمالی شبکه استفاده کرده است. این مرکز امنیت متمرکز از قواعد امنیتی استفاده کرده و داده های شبکه را جمع اوری می کند. با این حال نمونه پیشنهادی قادر به تشخیص نقض سیاست شبکه نیست.

3-2 به سمت امنیت رابط

فیلیپ و همکاران(10) یک پلتفرمی را ارایه کرده اند که موجب حصول اطمینان از امنیت یکپارچه و بهبود پردازش داده های موسوم به ناکس مجازیفورت می شود. این محصول برای شرکت های کوچک و متوسط مناسب است. این امنیت فیزیکی نظیر کنترل دسترسی، حفاظت در برابر ورود سرور فیزیکی و نیز حفاظت در برابر خرابی مدیریت را تضمین میکند.

3-3 به سمت امنیت ماشین مجازی



شکل 4: جستجوگرمعماری آپدیت

رولاند و همکاران(11) یک معماری را ارایه می کند که موجب افزایش امنیت ماشین مجازی می شود. معماری به دو بخش تقسیم می شود که یکی معماری جست و جو گر آپدیت بوده و دیگری معماری سویت نفوذ انلاین می باشد که در شکل 4 نشان داده شده است. جست و جو گر آپدیت، اطلاعات قدیمی نصب شده ب روی ماشین مجازی را شناسایی می کند. دومین مورد همه ماشین های مجازی را اسکن کرده و در صورتی که به آن نیاز باشد، آن را بوت می کند. به علاوه، تولید کننده گزارش دیگر مولفه ای است که بعد از جمع اوری همه گزارش ها از اسکنر، نتایج خطا را در اختیار می گذارد. با کمک این گزارش، خطا را می توان به آسانی تشخیص داده و حذف کرد. با این حال هردوی این معماری ها تنها به محیط لینوکس مربوط می باشند. با این حال نیاز به یک معماری کلی وجود دارد که در هر محیط کار کند.

اسپونتازکیس و همکاران(12) یک مکانیسمی را ارایه کرده اند که ماشین های مجازی را به طور خودکار تعیین می کند. طرح پیشنهادی مانع از نقض امنیت می شود با این حال امکان به روز رسانی همه بسته های ماشین های نرم افزاری را نمی دهد

3-4 به سمت انطباق

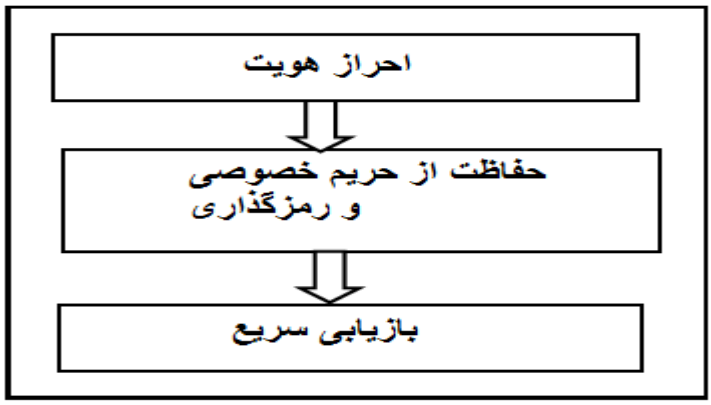
گیان و همکاران(13) یک معماری ذخیره داده ابر را ارایه کرده اند که یک مکانیسم ابری قابل حسابرسی عمومی را ارایه می کند و این به بررسی قابلیت و مهارت مالک داده ها برای ارزیابی ریسک برون سپاریدداده ها با کمک گروه حسابرسی خارجی کمک زیادی خواهد کرد. معماری پیشنهادی شامل چهار مولفه است: مالک داده، کاربر، سرور ابری و حسابرس شخص ثالث(TPA). این یک مکانیسمی را ارایه می کند که در آن مالک داده TPA را به حسابرسی سرور ابری به شکل موثر و مقرون به صرفه برای کاربران نهایی نسبت می دهد. وقتی که پای امنیت در میان باشد، امنیت آن کامل نیست زیرا حسابرسی به طور کامل به TPA و مالک داده ها متکی است. از این روی سوالی که مطرح می شود این است که اگر مالک و TPA یک گزارش صحیح به کاربر ارایه نکند ، آنکاه چه کسی مسئول آن خواهد بود؟ فانمیلاد و همکاران(14) یک جست و چو گر مبتنی بر داده های دینامیک را پیشنهاد کرده اند که قادر به کاهش نقض SLA با آزاد سازی منابع است. در معماری پیشنهادی، محققان بر آزاد سازی منابع تاکید داشته اند تا توجه به امنیت. اتحادیه امنیت ابری یک سازمان غیر انتفاعی است که در دسامبر 2008 تاسیس شده است. در این اتحادیه همه راهبرد های دولتی کنترل شده و سیاست های تضمین امنیت کالا در ایانش ابری حسابرسی می شود. به این ترتیب سیاست هایی با کمک موسسه ملی استاندارد و فناوری و انجمن کنترل و حسابرسی سیستم های اطلاعاتی آزاد خواهد شد.

3-4 به سمت حریم خصوصی

یوفا و همکاران(16) مطالعه ای را در خصوص نیاز امنیتی در رایانش ابری انجام داده اند. امروزه، بیشتر آژانس ها بر روی معماری سیستم فایل توزیع یافته هادوپ کار می کنند که بر مبنای گره کارفرما-کارگر است. گره کارفرما به صورت گره اسم و کره کارگر موسوم به گره داده ها است. بر طبق این مطالعه، همه گره های کنترل دسترسی داده ها توسط یک نقطه مدیریت می شود، گره نام یک عامل شکست و خرابی است. آن ها

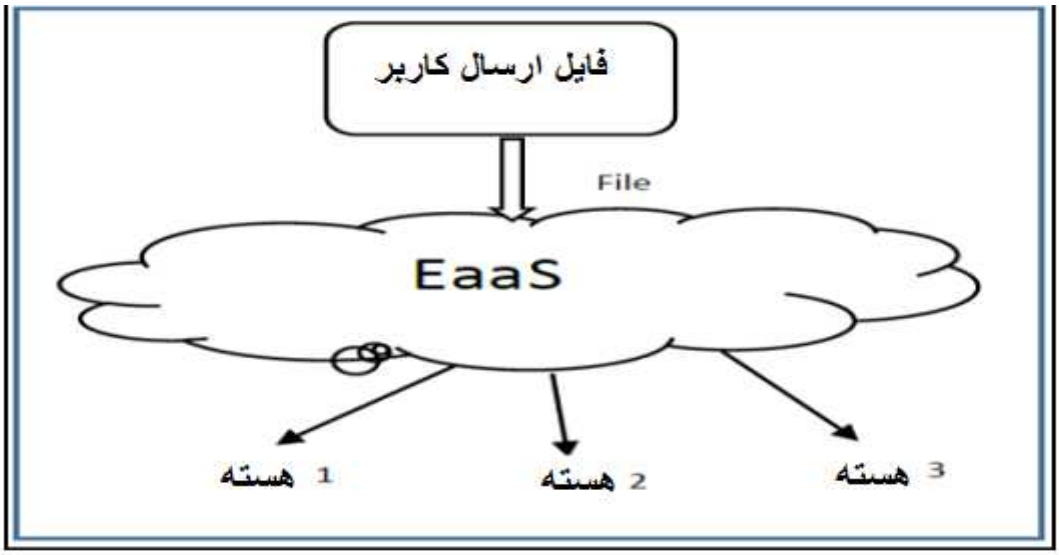
مدلی را با سه خط دفاعی ارایه کرده اند که در شکل 5 دیده می شود. این ها امنیت احراز هویت در سطح اول،رمزگذاریوحفاظتازحریمخصوصیدرسطحدوموبازیابیسریعدرسطحسوم می باشد. لایه احراز هویت برای تایید کاربران با کمک امضای دیجیتال استفاده می شود والکوریتم رمز گشایی در لایه دوم استفاده می شود. این لایه از الگوریتم ریکاوری سریع برای بازیابی داده ها استفاده می کند.

هیکویی و همکاران(17) روش آشفتگی فضای تصادفی و نزدیک ترین همسایه را ارایه کرده اند که به چهار داده کلیدی محرمانه بودن، حفظ حریم خصوصی پرس و جو، پردازش کارآمد پرس و جو و هزینه پردازش پایین رسیدگی می کند. محققان ازمایشی را تحت مدل تهدید انجام داده و پی بردند که نتایج کارایی بهتری با هزینه پایین دارند. با این حال این روش از کمبود داده ها و نیز حریم خصوصی ضعیف پرس و جو رنج می برند.



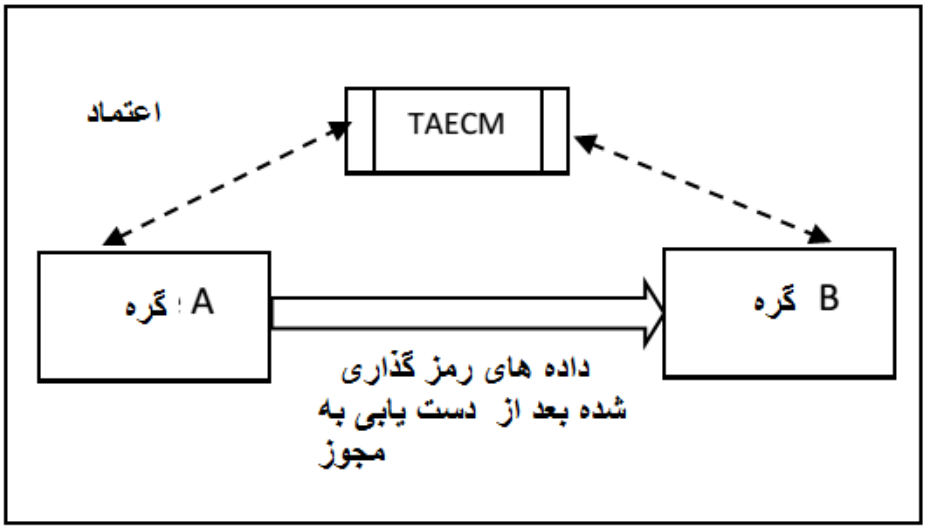
شکل 5: مدل امنیت داده ها برای رایانش ابری(16)

حسین و همکاران(18) رمزگذاری را به صورت یک سرویس برای اطمینان از امنیت در CSP ارایه کرده اند. در این روش، یک ابر خصوصی با استفاده از کد احراز هویت پیام از نظر صحت ایجاد می شود. هر تک رشته به طور معادل بر روی یک منطقه موازی ایجاد شده و تولید گروهی از رشته ها بعد از رمزگذاری می کنند. با این حال، این مکانیسم در صورتی به طور موفق عمل می کند که تنها اگر برنامه به سبک چند رشته ای نوشته شود در غیر این صورت عملکرد کاهش می یابد. توصیف این مدل در شکل 6 نشان داده شده است.



شکل 6: رمز گذاری به صورت یک سرویس(18)

زو و همکاران یک مدل اعتماد مبتنی بر عامل را ارایه کرده اند که اطمینان پذیری و اعتبار بالایی دارد. محققان یک تراشه اجرایی عامل مطمئن را ارایه کرده اند که موجب افزایش اطمینان شده و بر روی گره سنسور با استفاده از فناوری عامل کار می کند. قبل از ارسال داده ها از گره A به B، این داده ها را با استفاده از TAEC رمز گذاری می کند. اول گره A، یک مجوز اعتماد را از تولید کننده TAEC دریافت می کند که شامل کلید عمومی، راهبرد امنیت و نوع TAEC می باشد. بعد از تایید امضای دیجیتال، داده ها به گره B انتقال می یابند. به دلیل ترکیب عوامل، مدل پیشنهادی به یک مدل مستقل از پلاتفرم تبدیل می شود با این حال کاربرد امضای دیجیتال موجب کاهش کارایی مدل می شود. معماری در شکل 7 نشان داده شده است.



شکل 7: اجرای عامل معتمد(19)

وانگ و همکاران(20) یک مکانیسم حسابرسی را در محیط ابری ارایه کرده اند که موسوم به حسابرسی عمومی برای داده های مشترک با لغو کاربر کارامد است. هدف فسخ کاربر، این است که اگر یک کاربر به ابر نزدیک شود، کلید خصوصی تولید شده و داده ها با کلید خصوصی تعیین می شود. به دلیل این رایانش، زمان افزایش و کارایی کاهش یابد.

بخش فوق نشان می دهد که تحقیقات محدود در مسائل امنیتی مختلف در CC وجود دارد. هنوز مطالعات زیادی در این بعد در حال انجام است. بخش بعدی شامل نتیجه گیری است.

4- نتیجه گیری و مطالعات آینده

امنیت، یکی از ابعاد اصلی رایانش ابری به دلیل پذیرش تجاری بالای آن است. این مطالعه به خلاصه سازی مسائل امینتی در سطوح مختلف رایانش ابری می پردازد. با این حال، بر اساس این مقاله مروری می توان کفت که کم و بیش، رویکرد های امنیتی مشابه برای رایانش ابری همانند سایر روش های رایانش مبتنی بر اینترنت پیشنهاد میشود. با در نظر گرفتن ویژگی های مجزای کاربرد های ابری، نظیر شارش داده های کاربر، و چند محلی بودن زیر ساخت، تقاضای واقعی برای مکانیسم های امنیتی خاص می تواند یک اعتماد ضمن همکاری با ابر ارایه کند. انطباق SLA باید به طور جدی توسط سازمان های دولتی در نظر گرفته شود کار های آینده بر توسعه مکانیسم های مطمئن، ایمن و معتمد برای محیط ابری متمرکز خواهند بود.