فصلنامه پژوهش در علوم، مهندسی و فناوری
دوره ۹، شماره ۱، بهار ۱۴۰۲
صفحات ۵۳-۵۶
Print ISSN: 2476-5082
www.uctjournals.com

مطالعه‌ای بر روی مسائل امنیتی ذخیره داده‌ها در رایانش ابری

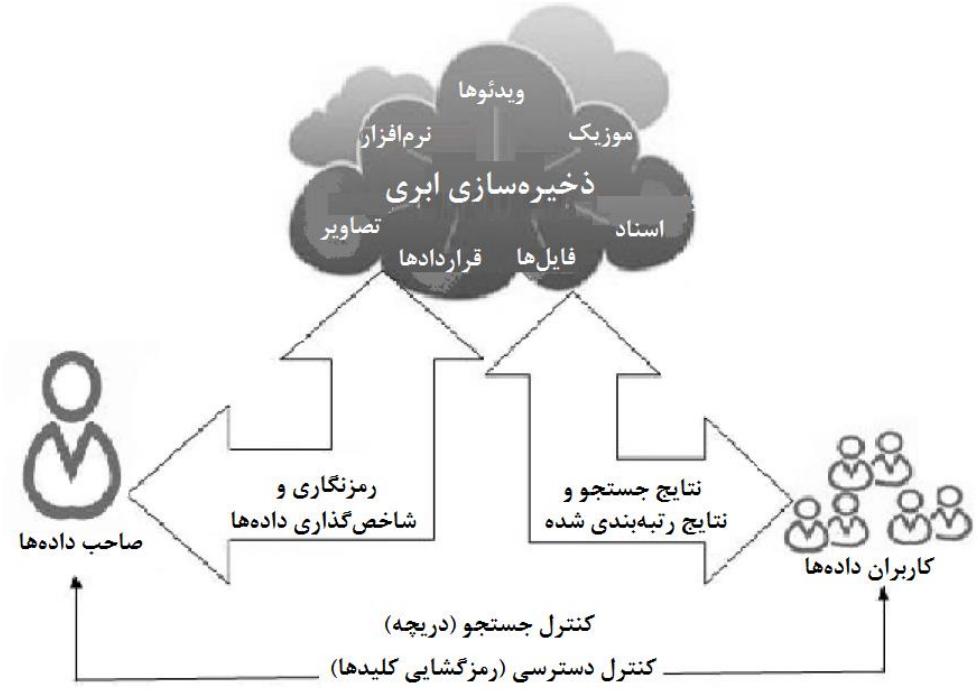
فاطمه دلبری۱* و فاطمه امین صفار۲
۱دانشجو،کارشناسی ارشد،مهندسی کامپیوترنرم افزار،دانشگاه آزاداسلامی واحد سبزوار (نویسنده مسئول)
۲دانشجو، دکتری،مدیریت تکنولوژی، دانشگاه مالک اشتر تهران

چکیده
رایانش ابری یک مکانیزم انقلابی است که در حال تغییر مسیر سرمایه‌گذاری در زمینه‌ی طراحی و تدارکات سخت‌افزاری و نرم‌افزاری می‌باشد. فراهم‌کننده‌ی سرویس ابری (CSP) باید صحت، در دسترس بودن، حریم خصوصی و محرمانگی داده‌ها را تضمین نماید ولی CSP سرویس‌های داده‌ی قابل اعتماد به مشتری و جهت ذخیره‌سازی داده‌های مشتری ارائه نمی‌دهد. این مطالعه، مسائل مرتبط با ذخیره‌سازی داده‌های ابری از قبیل نقض داده‌ها، سرقت داده‌ها، و عدم دسترسی به داده‌های ابری را شناسایی می‌کند. در نهایت، ما راه‌حل‌های ممکن به مسائل مربوطه را در ابر ارائه می‌دهیم.

واژه‌های کلیدی: فراهم‌کننده‌ی سرویس ابری (CSP)، ذخیره‌سازی داده‌های ابری، مسائل امنیتی، سیاست‌ها و پروتکل‌ها

۱- مقدمه

رایانش ابری یک روش انقلابی است که مسیر سرمایه‌گذاری در طراحی و تولید سخت‌افزار و نرم‌افزار راه تغییر داده است. محاسبات ابری برای مشتریان ابری مزایای ارزشمندی را از قبیل سرویس‌های بدون هزینه، انعطاف‌پذیری منابع، دسترسی آسان از طریق اینترنت، و غیره فراهم می‌کند. از شرکت‌های کوچک تا بزرگ، همگی به سمت استفاده از رایانش ابری حرکت کرده‌اند تا تجارت و پیوندهای خود را با دیگر شرکت‌ها افزایش دهند [۱]. حتی اگر رایانش ابری مزایابی بسیار زیادی داشته باشد، کاربران ابری تمایلی به قرار دادن داده‌های محرمانه یا حساس خود ندارند، که این داده‌ها شامل پرونده‌های سلامت شخصی، ایمیل‌ها و فایل‌های حساس دولتی می‌شوند. فرض کنید هنگامی که داده‌ها در مرکزداده‌ی ابری قرار می‌گیرند؛ کاربر ابری کنترل مستقیم خود را بر روی منابع داده‌های خود از دست می‌دهد. فراهم‌کننده‌ی سرویس ابری[1](CSP) قول می‌دهد که امنیت داده‌ها را برای داده‌های ذخیره شده‌ی کاربران ابری با استفاده از روش‌هایی مانند دیواره‌های آتش و مجازی‌سازی تضمین کند. این روش‌ها حفاظت کامل از داده‌ها را فراهم نخواهند کرد چرا که آسیب‌پذیری‌های آنها بر روی شبکه و فراهم‌کنندگان سرویس، بر برنامه‌های کاربردی، سخت‌افزار و داده‌های کاربر فرمان و کنترل کامل دارند. رمزگذاری داده‌های حساس پیش از قرار دادن آنها بر روی ابر می‌تواند از نظر حفظ حریم خصوصی داده‌ها و محرمانگی در برابر فراهم‌کنندگان سرویس روش مناسبی باشد. ولی یک مشکل معمول برای استفاده از روش رمزگذاری داده‌ها این است که به علت مقدار بسیار زیاد سربارهای ارتباطی بر روی الگوهای دسترسی ابر، اجرای روش رمزگذاری غیرعملی می‌باشد. بنابراین، ابر برای حفاظت از حریم خصوصی و محرمانگی داده‌ها نیاز به روش‌های امنی جهت ذخیره‌سازی و مدیریت آنها دارد [۲][۵]. این مقاله به طور عمده بر روی آسیب‌پذیری‌ها و مسائل امنیتی بر روی محرمانگی و حریم خصوصی در داده‌های کاربر تمرکز دارد.



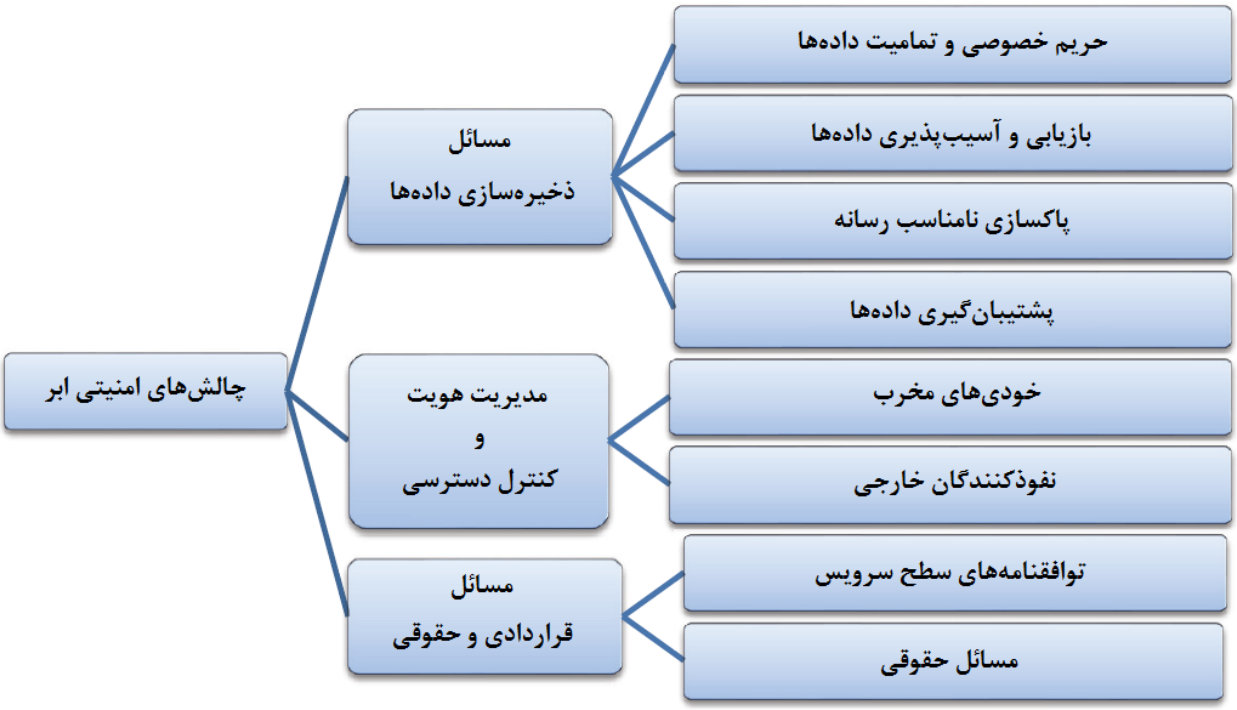
شکل ۱. مدل ذخیره‌سازی داده‌ی ابری

۲- چالش‌ها و مسائل ذخیره‌سازی داده‌های ابری

رایانش ابری کنترلی را بر روی داده‌های ذخیره شده در مراکز داده‌ی ابری فراهم نمی‌کند. فراهم‌کنندگان سرویس ابری کنترل کاملی بر روی داده‌ها دارند، آنها می‌توانند هر وظیفه‌ی خطرناک و مخربی از قبیل کپی، از بین بردن، تغییر، و غیره را بر روی داده‌ها انجام دهند. رایانش ابری سطح خاصی از کنترل را بر روی ماشین‌های مجازی تضمین می‌کند. این فقدان کنترل بر روی

1 Cloud Service Provider (CSP)

داده‌ها به مسائل امنیتی بزرگتری منجر می‌شود که این مسائل بزرگتر از مدل عمومی محاسبات ابری نشان داده شده در شکل ۱ هستند. رمزنگاری کنترل کاملی را بر روی داده‌های ذخیره شده ارائه نمی‌دهد ولی تا حدودی بهتر از داده‌های آشکار و بدون رمز است. همچنین مجازی‌سازی و چند مستأجری که از ویژگی‌های رایانش ابری هستند، نیز در برابر حملات احتمالی مختلفی نسبت به مدل عمومی ابر قرار دارند. شکل ۲ مسائل مختلفی را نشان می‌دهد که به وضوح در ادامه بحث شده‌اند.



شکل ۲. چالش‌های امنیتی ابر

۲-۱. مسائل ذخیره‌سازی ابری

۲-۱-۱. تمامیت و حریم خصوصی داده‌ها

اگر چه رایانش ابری هزینه‌ی کمتر و مدیریت کمتری از منابع را فراهم می‌کند، ولی از طرف دیگر در برابر برخی از تهدیدات امنیتی قرار دارد. همانطور که پیش از این بحث نمودیم، رایانش ابری باید تمامیت، محرمانگی، حریم خصوصی و دسترس‌پذیری داده‌ها را در مدل عمومی رایانش ابری تضمین کند ولی مدل رایانش ابری در برابر تهدیدات امنیتی از نظر شرایط بالا آسیب‌پذیر است. به دلیل سادگی مدل آن، کاربران ابری به صورت نمایی در حال افزایش بوده و برنامه‌های کاربردی بسیار زیادی در ابر میزبانی می‌شوند. این شرایط منجر به تهدیدات امنیتی بزرگتری بر روی کاربران ابری می‌شود. هر گونه حمله‌ی موفقی بر روی موجودیت داده‌ای منجر به نقض داده خواهد شد و یک دسترسی غیرمجاز به داده‌های تمام کاربران ابری صورت خواهد گرفت. به علت این نقض تمامیت، داده‌های ابری ماهیت چند مستاجری خود را از دست می‌دهند. به ویژه اینکه فراهم‌کنندگان SaaS ممکن است داده‌های فنی خود را از دست دهند و آنها متوجه خطر بزرگی بر روی ذخیره‌سازی داده‌ها هستند. به غیر از این خطرات، پردازش داده‌ها نیز با خطر بزرگی مواجه است چرا که داده‌ها در میان مستاجران متعددی در حال تبادل هستند. از آنجا که مجازی‌سازی چندین منبع فیزیکی در میان کاربران به اشتراک گذاشته می‌شود، این امر به راه‌اندازی حملات توسط کاربران داخلی CSP و/یا سازمان منجر می‌شود. این شرایط ممکن است به افراد مخرب اجاز دهد که هنگام پردازش داده‌های خود، حملاتی را بر روی داده‌های ذخیره شده‌ی دیگر مشتریان انجام دهند. خطر عمده‌ی دیگر وقتی است که داده‌ها توسط CSP به یک ذخیره‌کننده‌ی شخص ثالثی واگذار می‌شوند [۵]. تولید و مدیریت کلید در رمزنگاری به خوبی برای رایانش ابری استاندارد نشده است. نبود استاندارد و مدیریت مخفی کلید برای ابر، به الگوریتم‌های

استاندارد رمزنگاری اجازه نمی‌دهد که در مدل عمومی رایانش ابری به خوبی اجرا شوند. حال آنکه رمزنگاری ممکن است رایانش ابری را از خطرات بالقوه مراقبت کند.

۲-۱-۲. قابلیت بازیافت و آسیب‌پذیری داده‌ها

با توجه به مشخصات ائتلاف[2] و کشسانی منابع، ابر می‌تواند پویایی و بر حسب تقاضا فراهم شدن منابع را به کاربران تضمین نماید. منابعی که به یک کاربر خاص تخصیص داده شده‌اند، ممکن است در مدت زمان بعدی به کاربر دیگری اختصاص داده شوند. در مورد حافظه و منابع ذخیره‌سازی، یک کاربر مخرب می‌تواند از روش‌های بازیابی داده‌ها برای به دست آوردن داده‌های کاربران قبلی استفاده کند [۱۳]. نویسندگان در مرجع [۱۳] قادر به بازیابی فایل‌های تصاویر ماشین در ۹۸٪ از موارد تکرار آزمایش شده‌اند. آسیب‌پذیری بازیابی داده‌ها می‌تواند تهدیدات عمده‌ای را بر روی داده‌های حساس کاربران داشته باشد.

۲-۱-۳. پاکسازی نامناسب رسانه

ذخیره‌سازی رسانه‌ها ممکن است بنا به یکی از دلایل زیر پاکسازی شوند (i) دیسک ممکن است نیاز به جایگزینی با دیسک دیگری داشته باشد ، (ii) نیازی به نگهدای دیسک نباشد یا بیش از این دیگر نیازی به نگهداری فایل نباشد، (iii) تخریب سرویس‌ها. پاکسازی نامناسب می‌تواند خطر بزرگی را بر روی داده‌های ذخیره شده تضمین نماید. در ابری با ویژگی چند مستأجری امکان پاکسازی وجود ندارد و علت آن نیز مستاجر قبلی می‌باشد.

۲-۱-۴. پشتیبان‌گیری از داده‌ها

به علت احتمال بروز فجایع تصادفی و/یا عمدی، پشتیبان‌گیری از داده‌ها مهم است. CSP باید پشتیبان‌گیری منظمی را از داده‌های ذخیره شده انجام دهند تا دسترس‌پذیری داده‌ها را تضمین نماید. در واقع، پشتیبان‌گیری از داده‌ها باید به همراه حفظ دستورالعمل‌های امنیتی باشد تا از فعالیت‌های مخرب از قبیل دستکاری و دسترسی غیرمجاز جلوگیری نماید.

۲-۲. مدیریت هویت و کنترل دسترسی

تمامیت و محرمانگی داده‌ها و سرویس‌ها با کنترل دسترسی و مدیریت هویت در ارتباط است. نگهداری سابقه برای هویت کاربر جهت پیشگیری از دسترسی غیرمجاز به داده‌های ذخیره شده بسیار مهم است. کنترل هویت و دسترسی در رایانش ابری وظایف پیچیده‌ای هستند، چرا که صاحبان داده‌ها و داده‌های ذخیره شده در بسترهای اجرایی متفاوتی قرار دارند. در محیط ابر، سازمان‌های مختلف از دستور کارهای متنوعی برای احراز هویت و بررسی مجوز استفاده می‌کنند. استفاده از رویکردهای مختلف برای احراز هویت و بررسی مجوز، یک وضعیت ترکیبی را در طی یک دوره‌ی زمانی ارائه می‌دهد. منابع ابری پویا هستند و برای کاربر ابری به صورت کشسان می‌باشند، و در مدل پرداخت به ازای مصرف، هر گاه سرویس‌ها آغاز یا آغاز مجدد می‌شوند آنگاه در هر بار آدرس‌های IP به طور مداوم تغییر می‌یابند. این امر به کاربران ابری اجازه می‌دهد تا هر گاه که نیاز داشته باشند، ویژگی‌ها را به منابع ابری خود پیوند دهند یا کنار بگذارند، مانند سیاست دسترسی بر حسب تقاضا. تمام این ویژگی‌ها نیاز به کنترل دسترسی و مدیریت هویت موثر و کارآمدی دارند. ابر باید سرعت به‌روزرسانی‌ها را حفظ کند و مدیریت هویت را برای پیوستن و ترک کردن کاربران به منابع ابری مدیریت کند. مسائل زیادی در کنترل دسترسی و مدیریت هویت وجود دارد، برای مثال گواهینامه‌های ضعیف ممکن است به راحتی تنظیم مجدد (ریست) شوند، حمله انکار سرویس جهت قفل کردن حساب برای یک دوره‌ی زمانی رخ دهد، ضعف در ثبت ورود و نظارت بر توانایی‌ها، و حملات پنهان‌سازی XML بر روی صفحات وب.

۲-۲-۱. خودی‌های مخرب

یک تهدید داخلی در یک سازمان می‌تواند از جانب کارکنان، پیمانکاران/یا شرکای تجاری شخص ثالث ایجاد شود. در محیط ابری به عنوان مثال حملات در سمت فراهم‌کننده‌ی سرویس ابری (CSP) منجر به از دست رفتن تمامیت، محرمانگی، و امنیت اطلاعات کاربر می‌شود. این امر منجر به از دست رفتن یا شکاف در داده‌های هر دو محیط می‌شود. این حمله بسیار محبوب بوده و در اکثر سازمان‌ها به خوبی شناخته شده است [۷]. حمله‌هایی با الگوهای متنوع وجود دارد که توسط خودی‌ها انجام

2 resource pooling

شده است، علت این تنوع نیز به دلیل پیچیدگی ساختار داخلی در ساختار ذخیره‌سازی داده‌های یک سازمان است. اکثر سازمان‌ها این حمله را نادیده می‌گیرند، زیرا این حمله بسیار سخت دفاع می‌شود و یافتن راه‌حل کامل برای این حمله غیرممکن است. این حمله خطرهای بزرگی را از نظر نقض و رخنه در داده‌ها و از دست رفتن محرمانگی داده‌ها هم در سطح سازمان و هم در سطح ابر قطعی می‌کنند [۸].

۲-۲-۲. نفوذکنندگان خارجی

حملاتی که از مبدأهای خارجی می‌آیند، با نام حملات خارجی نامیده می‌شوند [۳۰]. امنیت داده‌ها یکی از مسائل مهم در رایانش ابری است. از آنجایی که فراهم‌کنندگان سرویس اجازه‌ی دسترسی به سیستم امنیت فیزیکی در مراکز داده را ندارند، آنها باید به زیرساخت فراهم‌کننده برای کسب امنیت کامل داده‌ها تکیه کنند. در یک محیط ابر خصوصی مجازی، فراهم‌کننده‌ی سرویس تنها می‌تواند تنظیمات امنیت را به صورت از راه دور مشخص کند، و ما دقیقا نمی‌دانیم که آنها به طور کامل پیاده‌سازی شده‌اند. در این فرآیند، فراهم‌کننده‌ی زیرساخت باید به اهداف زیر دست یابد: (۱) محرمانگی، برای انتقال و دسترسی امن به داده‌ها، و (۲) قابلیت حسابرسی [۳۱]. چنانکه مهاجمان خارجی نمی‌توانند به داده‌های حساس ذخیره شده در ابر دسترسی داشته باشند.

۲-۳. مسائل قراردادی و حقوقی

پس از حرکت به سمت محیط رایانش ابری، مسائلی در حوزه‌های قضایی جغرافیایی، قانون نظارتی، تضمین عملکرد، اجرای قراردادها و غیره وجود دارد. مسائل ذکر شده در بالا از قوانین، توافقنامه‌های سطح سرویس و مکان داده‌ها در مراکز داده ناشی می‌شوند [۹].

۲-۳-۱. توافقنامه‌های سطح سرویس

توافقنامه سطح سرویس[3](SLA) می‌تواند به صورت یک پروتکل شرح داده شود، این پروتکل مجموعه‌ای از شرایط و اصطلاحات را میان کاربر و فراهم‌کننده سرویس ابری مشخص می‌کند. SLA باید موارد زیر را مشخص کند: اقداماتی که وقتی نقض داده‌ها رخ می‌دهد، CSP انجام خواهد داد، اقدامات اصلاحی و حداقل سطح عملکرد [۵]. کاربر باید دید واضحی از امنیت را برای منابع خود داشته باشد و تمام دیگر نیازها باید در SLA مورد توافق قرار گیرند. اجرای قرارداد نیز تبدیل به یک مسئله شده است، چرا که آمارهای ارائه شده توسط CSP کاملا اثبات نشده هستند. در نهایت، قراردادها غیرقابل مذاکره و از پیش تعریف شده هستند که باید به صورت دوستانه‌ای بین کاربر و CSP ایجاد شوند. قوانین نظارتی از قبیل Sarbanes-Oxley و HIPAA به یک مسئله‌ی باز تبدیل شده‌اند [۱۰].

۲-۳-۲. مسائل حقوقی

مسائل حقوقی به این دلیل به وجود می‌آیند که منابع CSP در حوزه‌های قضایی مختلفی حضور دارند که به لحاظ جغرافیایی ناسازگار و متضاد هستند [۱۱]. اگر کاربر از یک مکان جغرافیایی به مکان دیگری مهاجرت کند، آنگاه مسئله‌ای به دلیل حوزه‌های قضایی مختلف رخ خواهد داد. برای یک حرکت، داده‌ها بر روی مراکزداده‌ی مختلف توزیع شده‌اند، برخی از آنها متعلق به CSP هستند و برخی قوانین و دستورالعمل‌های امنیتی مختلفی دارند. این سناریو ممکن است در رایانش ابری به یک مسئله‌ی جدی تبدیل شود.

۳. راه‌حل‌های موجود

در این بخش، ما راه‌حل‌های تحقیقاتی را شرح داده و در عین حال بحث جامعی را نیز ارائه می‌کنیم. نتایج در جدول‌ها ارائه شده است که به درک راحت‌تر خواننده کمک می‌کند. بحث در طی زیرفصل‌های مختلفی ایجاد شده است.

3 Service Level Agreement (SLA)

۱-۳. راه‌حل‌های مسائل ذخیره‌سازی داده‌ها

SecCloud توسط Wei و همکارانش [۱۲] ارائه شده است، این روش در واقع یک پروتکل امنیتی ذخیره‌سازی را برای داده‌های مشتری ابری فراهم می‌کند و نه تنها داده‌های ذخیره شده را امن می‌کند بلکه امنیت را برای داده‌های محاسباتی نیز ارائه می‌دهد. پروتکل SecCloud از رمزنگاری برای ذخیره‌سازی داده‌ها در حالت امن استفاده می‌کند. گروه‌های ضرب شونده و جفت شدن افزودنی چرخشی جهت تولید کلید برای مشتریان ابری، CSP، و دیگر شرکای تجاری یا شخص ثالث مورد اعتماد مورد استفاده قرار گرفته است. داده‌های رمز شده همراه با امضای قابل اثبات و کلید نشست به مرکزداده‌ی ابری ارسال می‌شود. الگوریتم دفی-هلمن[4]برای تولید کلید نشست در هر دو گروه دوخطی استفاده می‌شود. ابر با دریافت داده‌های رمز شده، به رمزگشایی آنها می‌پردازد، امضای دیجیتال را تایید کرده و داده‌های اصلی را در مکان مشخصی از ابر ذخیره می‌کند. SecCloud بررسی می‌کند که آیا داده‌ها در مکان مشخص ذخیره شده‌اند یا خیر. درخت هش[5]Merkle برای محاسبه‌ی امنیت در پروتکل SecCloud استفاده می‌شود. عامل بررسی‌کننده به بررسی نتایج محاسباتی خواهد پرداخت که با استفاده از درخت هش Merkle ایجاد شده‌اند. پروتکل حذف مطمئن فایل[6](FADE)، یک روش مدیریت کلید را با تمامیت و حریم خصوصی داده‌ها در مرجع [۱۵] ارائه می‌دهد.

مدیریت کلید همراه با تمامیت و حریم خصوصی داده‌ها به وسیله‌ی پروتکل حذف مطمئن فایل (FADE) در مرجع [۱۸] ارائه شده است. به علت سادگی FADE؛ این یک پروتکل کم حجم است و از هر دو رمزنگاری کلید متقارن و نامتقارن برای داده‌ها استفاده می‌کند. روش Shamir از کلیدهای متقارن و نامتقارن برای اعتماد بخشیدن به مدیریت کلید محافظت می‌کند. گروهی از مدیران کلید توسط پروتکل FADE مورد استفاده قرار می‌گیرند، این مدیران به عنوان یک شخص ثالث مورد اعتماد عمل می‌کنند. کلید k به عنوان کلید رمزنگاری برای فایل F مشتری استفاده می‌شود و دیگر کلید نیز برای رمزنگاری داده‌ی کلید (k) مورد استفاده قرار می‌گیرد. فایل سیاست از جزئیاتی نگهداری می‌کند که مشخص می‌کنند کدام یک از فایل‌ها قابل دسترسی هستند. به این صورت که کاربر برای آپلود کردن داده‌ها باید جفت کلید را با ارسال فایل سیاست p از شخص ثالث درخواست کند. مدیر کلید با استفاده از فایل سیاست، کلیدهای عمومی و خصوصی را به کاربر ارسال می‌کند. فایل آپلود شده با k که به صورت تصادفی تولید شده است، رمز می‌شود و k نیز با کلید متقارن رمز می‌شود. فایل رمز شده، با کلید عمومی تولید شده از جفت کلید از رمز خارج می‌شود و MAC نیز برای بررسی تمامیت تولید می‌شود. فرآیند معکوسی نیز توسط گیرنده برای به دست آوردن داده‌های اصلی انجام می‌شود.

Liu و همکارانش [۱۵] روشی ارائه کرده‌اند که یک رمزنگاری مجدد مبتنی بر زمان با الگوریتم ABE دارد تا از به اشتراک‌گذاری امن داده‌ها میان گروه با کنترل دسترسی پشتیبانی کنند. این روش تضمین می‌کند که داده‌های ارسال شده به صورت امنی به کاربران گروه رسیده است و از فسخ کاربر محافظت می‌کند. در این روش، دوره‌ی زمانی به هر کاربر و تاریخ انقضای ابطال وابسته است که به طور خودکار توسط فراهم‌کننده‌ی سرویس ابر (CSP) مشخص می‌شود. این روش رمزنگاری مبتنی بر زمان به کاربران اجازه می‌دهد تا کلیدها را از قبل با CSP به اشتراک بگذارد و CSP کلیدهای رمزنگاری مجدد را با دریافت درخواست از کاربر تولید می‌کند. پروتکل ABE، به جای اینکه هویت را مورد بررسی قرار دهد، یک کنترل دسترسی را با بررسی مجموعه‌ای از ویژگی‌ها تضمین می‌کند. این روش، حریم خصوصی و دسترس‌پذیری داده‌ها را میان افراد گروه تضمین می‌کند ولی بر روی تمامیت داده‌ها تمرکز ندارد.

نمونه‌گیری احتمالی برای کاهش افزونگی محاسبات به جای بازسازی دوباره‌ی کل درخت مورد استفاده قرار می‌گیرد. لیست زیر در واقع توصیه‌های کلیدی ارائه شده توسط ائتلاف امنیت کامپیوتری[7](CSA) [۱۸] برای امنیت داده‌ها و مدیریت

4 Diffie-Hellman
5 hash
6 File Assured Deletion (FADE)
7 Computer Security Alliances (CSA)

کلید هستند. حوزه‌ی کلید باید توسط گروه یا خود فرد نگهداری شود. الگوریتم‌های استاندارد رمزنگاری باید استفاده شده و الگوریتم‌های ضعیف نیز حذف شوند.

بهترین راهنمایی‌ها برای مدیریت کلید و محصولات نرم‌افزاری رمزنگاری باید مورد استفاده قرار گیرند، بهتر است که از فناوری قانونی نرم‌افزار استفاده شود تا امنیت ذخیره‌سازی تضمین شود. مشتری یا سازمان‌ها و/یا شخص ثالث مورد اعتمادی باید از مدیریت موثر و کارآمد کلید محافظت کند. اگر پروتکل حسابرسی نامناسبی طراحی شود، در فرآیند رمزنگاری ممکن است جریان داده در حین حسابرسی توسط اشخاص خارجی کنترل شود. اگر چه رمزنگاری به تنهایی نمی‌تواند از کنترل جریان داده‌ها توسط اشخاص خارجی جلوگیری کند، اما در عوض می‌تواند این کنترل را به کمترین سطح کاهش دهد. اما در حین ذخیره‌سازی داده‌ها، نیاز به محدوده‌ی وسیعی از فرآیندهای مدیریت کلید و سربارهایی برای تولید کلید وجود دارد. اما آشکارسازی کلید رمزنگاری نیز منجر به فاش شدن داده‌ها شده و این مسئله همچنان یک مشکل در محیط ابری است. این مشکل با استفاده از ترکیب احراز هویت‌کننده‌های مشابه به همراه فرآیند پوشش تصادفی رفع شده است [۱۹]. خلاصه‌ای از این موارد در جدول ۱ نشان داده شده است.

جدول ۱. راه‌حل‌های ممکن برای مسائل ذخیره‌سازی داده‌ها

نویسندگان	روش پیشنهادی	سرویس‌ها	حریم خصوصی	تمامیت	دسترس‌پذیری	محرمانگی
L. Wei و H. Zhu [۱۲]	SecCloud، برای امن نمودن داده‌های ابری	- رمزنگاری - جفت‌سازی دوخطی - بررسی امضا - شخص ثالث مورد اعتماد	√	√	×	√
Y. Tang و P.P. Lee و J.C.S. Lui [۱۵]	FADE، پروتکلی برای حریم خصوصی و تمامیت داده‌ها	- رمزنگاری - شخص ثالث مورد اعتماد - حذف مطمئن - اشتراک‌گذاری امن آستانه	√	√	×	√
Q. Liu و G. Wang [۱۶]	TimePRE، روشی برای اشتراک‌گذاری امن داده‌ها در ابر	- رمزنگاری مجدد پروکسی - رمزنگاری مبتنی بر ویژگی	√	×	×	√
Z. Tari [۱۷]	یک روش برای امنیت داده‌ها ساکن در ابر	- تضمین کد صحیح - افزونگی داده‌ها	×	√	√	√

۲-۳. راه‌حل‌های مدیریت هویت و کنترل دسترسی

نویسندگان روش ساده‌ی مدیریت هویت را به همراه حفظ حریم خصوصی برای محیط‌های ابری (SPICE) در مرجع [۲۰] جهت استفاده در سیستم‌های مدیریت هویت ارائه کرده‌اند. SPICE، امضاهای گروهی را برای ارائه‌ی احراز هویت ناشناس، کنترل دسترسی، قابلیت حسابرسی، قابلیت قطع پیوند، و بررسی مجوز دسترسی به صورت کاربر محور تضمین می‌نماید. SPICE، ویژگی‌های ذکر شده در بالا را تنها با یک ثبت‌نام فراهم می‌کند. کاربر پس از ثبت‌نام در یک شخص ثالث مورد اعتماد، گواهینامه‌های منحصربفردی را برای تمام سرویس‌های ارائه شده توسط CSP به دست می‌آورد. با استفاده از گواهینامه‌ها، کاربر گواهینامه‌ی احراز هویت را تولید می‌کند. CSPهای مختلف انتظار ویژگی‌های متنوعی را از احراز هویت دارند و کاربر باید از همان گواهینامه، گواهینامه‌ی احراز هویت موردنیاز CSPها را تولید کند.

کنترل دسترسی چند مستاجری مبتنی بر نقش (RB_MTAC) در مرجع [۲۱] ارائه شده است. RB_MTAC، روش کنترل دسترسی مبتنی بر نقش را به همراه مدیریت هویت ادغام می‌کند. این روش نیاز دارد که کاربر در CSP ثبت‌نام کند و گواهینامه‌ی واحدی را به دست آورد که باید منحصربفرد باشد. کاربر باید هنگام ثبت‌نام در پورتال CSP، رمز عبوری برای خود انتخاب کند. با استفاده از این گواهینامه‌ها و عبور از ماژول هویت که کاربر را به طور منحصربفردی شناسایی می‌کند، کاربر می تواند به محیط ابر وارد شود و سپس به ماژول انتساب نقش هدایت خواهد شد که یک اتصال را به پایگاه‌داده‌ی RB_MTAC ایجاد می‌کند و نقش‌ها را به کاربرهای ثبت‌نام شده بر اساس اطلاعات ثبت‌نامی آنها نسبت می‌دهد.

Dhungana و همکارانش [۲۲] روشی را برای زیرساخت شبکه‌ی ابری به عنوان چارچوب مدیریت هویت ارائه کرده‌اند و این روش توسط پروتکل دسترسی مدیریت کاربر[8](UMA) حفاظت می‌شود. در اینجا CSP به عنوان یک میزبان عمل می‌کند، در حالی که کاربر مجاز به عنوان صاحب سرویس عمل می‌کند. "مدیر بررسی مجوز" به مدیریت سرویس رسیدگی می‌کند و درخواست سرویس از سوی کاربران نیز توسط این مدیر مدیریت می‌شود. این روش، مدیریت هویت و کنترل دسترسی را در میان چندین فراهم‌کننده‌ی ابری با کمک مدیریت مجوز تضمین می‌کند. این موارد در جدول ۲ نشان داده شده است.

جدول ۲. راه‌حل‌های مدیریت هویت و کنترل دسترسی

نویسندگان	روش پیشنهادی	سرویس‌ها	کنترل دسترسی	احراز هویت	مدیریت هویت
S.M.S. Chow و همکارانش [۲۳]	SPICE، چارچوب مدیریت هویت	- ناشناس و قابل واگذاری - کنترل دسترسی - احراز هویت - حسابرسی	√	√	×
Z. Yan و P. Zhang [۲۴]	روش کنترل دسترسی مبتنی بر نقش	کنترل دسترسی	√	√	×
R.D. Dhungana و A. Mohammad [۲۲]	چارچوب مدیریت هویت	- مدیریت هویت - احراز هویت - کنترل دسترسی	√	×	√
S. Ruj و M. Stomenovic [۲۵]	کنترل دسترسی غیرمتمرکز برای ذخیره‌سازی ابری	- رمزنگاری مبتنی بر ویژگی - امضای مبتنی بر ویژگی	×	√	√
Z. Wan و J. Liu [۲۶]	HASBE	- کنترل دسترسی برای - رمزنگاری مجدد حریم خصوصی در ابر	√	√	×

۳-۳. راه‌حل‌های مسائل قراردادی و حقوقی

در محیط رایانش ابری، کاربران به دلیل سادگی محیط از مزایای زیادی برخوردار هستند و از طرفی در صورت نقض توافقنامه‌های سطح سرویس نیز با خطر بزرگی روبرو می‌شوند. نویسندگان در مرجع [۲۷] روشی را پیشنهاد داده‌اند که به منظور کاهش خطرات امنیتی در محیط لغو/ نقض، به نقض‌های رخ داده در توافقنامه‌های سطح سرویس واکنش نشان می‌دهد. این روش بر روی الگوریتمی تمرکز دارد که در صورت آگاهی از خطر، مذاکرات را دوباره انجام می‌دهد. الگوریتم از روش مرجع

[8] User Managed Access (UMA)

[۲۸] استفاده می‌کند تا حداقل خطر سرویس را میان سطوح سرویس جهت اجرای نیازهای کاربران تعیین کند. الگوریتم به بررسی دقیق و مذاکره‌ی مجدد سرویس‌ها در محیط زمان اجرا می‌پردازد تا سرویس‌ها را در صورت لزوم جایگزین یا لغو نماید. در نهایت با توجه به SLA، عوامل خطر را به‌روزرسانی می‌کند.

Rak و همکارانش [۲۹] روش SPECS را ارائه کرده‌اند که این معماری تضمین می‌کند سرویس‌هایی را با نام "امنیت مبتنی بر SLA" به عنوان یک سرویس فراهم کند. معماری ارائه شده به طور عمده بر روی سه جنبه تمرکز دارد یعنی مذاکره، اجرا، و نظارت. SPEC توصیه می‌کند که اجرای عوامل فعال‌کننده به وسیله‌ی نظارت و گزارش‌گیری یا راه‌اندازی سیستم انجام شود.

جدول ۳. راه‌حل‌های ممکن برای مسائل حقوقی و قراردادی

نویسندگان	روش پیشنهادی	سرویس‌ها	مذاکره	اجرا	نظارت
M.L. Hale و R. Gamble [۲۸]	SecAgreement	جاسازی پارامترهای امنیتی در SLA توافقنامه-ws	√	×	×
M. Rak و N. Suri [۲۹]	SPECS, SLA-based	جاسازی تقاضاهای امنیتی	√	√	√

۴. نتیجه‌گیری

معماری رایانش ابری، داده‌ها و نرم‌افزارهای کاربردی را با حداقل تلاش مدیریتی ذخیره کرده و سرویس‌های برحسب تقاضایی را از طریق اینترنت به مشتریان ارائه می‌دهد. با وجود مدیریت ابر، مشتری اعتماد چندانی به تعهدات یا سیاست‌های ارزشمند ندارد. این امر منجر به ایجاد مسائل امنیتی زیادی در رابطه با ذخیره‌سازی داده‌ها از قبیل حریم خصوصی، محرمانگی، تمامیت و دسترس‌پذیری داده‌ها خواهد شد. در این مطالعه، ما بر روی مسائل امنیتی ذخیره‌سازی داده‌ها در رایانش ابری تمرکز نموده و در ابتدا به ارائه‌ی مدل‌های سرویس ابری، مدل‌های استقرار و انواع مسائل امنیتی در ذخیره‌سازی داده‌ها در محیط ابر پرداخته‌ایم. در بخش پایانی نیز، راه‌حل‌های ممکن برای مسائل ذخیره‌سازی داده‌ها را بیان کرده‌ایم که محرمانگی و حریم خصوصی را در محیط ابر فراهم می‌کنند.

۵.ایده ای جهت افزایش امنیت در رایانش ابری(تأمین امنیت به وسیله مجازی سازی)

امروزه مجازی سازی یکی از راه حل هایی است که برای تأمین امنیت در پردازش ابری به کار گرفته می شود . پذیرش و انتشار پردازش توسط مسائل امنیتی تهدید می شود . بنابراین این باعث می شود هم ارائه دندگان ابر هم کاربران ابر تحت تأثیر این مسأله قرار بگیرند. یکی از روشهای مجازی سازی برای تأمین محاسبات ابری، حفظ یکپارچگی ماشین های مجازی مهمان و یزرساخت است. این بدین معنی است که یک سیستم حفاظتی ابر پیشرفته با هدف تضمین امنیتی مضاعف برای منابع ابر پیشنهاد شده است ACPS .را می توان بر چندین راه حل ابری و در حالی که هنوز به طور کامل برای ماشین های مجازی و کاربران ابر نارمئی است مستقر کرد که این مسأله می تواند به طور مأثر بر یکپارچگی مهمان و اجزای زیرساخت نظارت کند . ACPSمی تواند به نقض های امنیتی محلی واکنش نشان دهد و همچنین لایه های مدیریتی بالاتر را از چندین رویدادهایی مطلع سازد

۶.مراجع ومنابع

A. Abbas, K. Bilal, L. Zhang, S.U. Khan, A cloud based health insurance plan recommendation system: a ser centered approach, Future Gener. Comput. Syst. (2014)
P. Mell, T. Grance, The NIST definition of cloud computing (draft), NIST Special Publ. 800 (145) (2011) 7.
J. Che, Y. Duan, T. Zhang, J. Fan, Study on the security models and strategies of cloud computing, Proc. Eng. 23 (2011) 586–593.

R. Chandramouli, M. Iorga, S. Chokhani, Cryptographic key management issues and challenges in cloud services, in: Secure Cloud Computing, Springer, New York, 2014, pp. 1–30.
C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, Toward secure and dependable storage services in cloud computing, IEEE Trans. Services Comput. 5 (2)(2012) 220–232.
M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, A security analysis of amazon's elastic compute cloud service, in: Proceedings of the 27th Annual ACM Symposium on Applied Computing, 2012, pp. 1427–1434.
Duncan, Adrian, Sadie Creese, and Michael Goldsmith. "Insider attacks in cloud computing." Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.
Khorshed, Md Tanzim, ABM Shawkat Ali, and Saleh A. Wasimi. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing." Future Generation computer systems 28.6 (2012): 833-851.