علوم رایانش و فناوری اطلاعات
نشریه علمی انجمن کامپیوتر ایران
مجلد ۱۶، شماره ۱، ۱۳۹۷
صفحات ۳۶- ۴۶
مقاله عادی

ارائه یک سیستم کنترلِ دسترسیِ ثبت‌نامِ یک‌باره مبتنی بر کربروس برای فدراسیون ابری

محمد بهارلو[۱] مهدی افشارمنش[۲] ثارالله کشاورز للکامی[۳]

[۱]دانشکده مهندسی برق و کامپیوتر، دانشگاه تهران، تهران، ایران
[۲]دانشکده مهندسی کامپیوتر، موسسه آموزش عالی پویش، قم، ایران
[۳]دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد قزوین، قزوین، ایران

چکیده

رایانش ابری از دیرباز برای تحولی بنیادی در راه مدیریت منابع و سرویس‌ها پیش‌بینی شده است. این فناوری، به‌عنوان یک پدیده تکنولوژیکی با مزایای زیادی برای کسب‌وکار و مصرف‌کنندگان پدید آمده است. رایانش ابری یک الگوی امیدوارکننده برای ارائه رایانش همگانی (مثل خدمات آب و برق و ...) به‌عنوان خدمات است. فراهم‌کنندگان رایانش ابری مقدار زیادی منابع توزیع شده در سراسر دنیا دارند، اما گاهی اوقات این منابع برای کسب رضایت مشتریان کافی نیستند به همین دلیل مفهومی به نام فدراسیون ابری که اخیراً توجه جامعه پژوهش را به خود جلب کرده است، برای گسترش این فناوری، مطرح شده است. فدراسیون ابری به فراهم‌کنندگان اجازه به اشتراک‌گذاری منابع‌شان را برای کمک به انجام تقاضاهای مشتریانی که یک ابر منفرد نمی‌تواند آن تقاضاها را به‌تنهایی برآورده نماید را می‌دهد. یکی از موضوعات مهمی که در یک محیط فدراسیونی وجود دارد و باید به آن‌ها پرداخته شود، موضوع نگرانی از بابت مدیریت کاربران و احراز هویت آن‌ها در فدراسیون ابری است.

در این مقاله روی مبحث کنترل دسترسی به منابعِ فراهم شده در یک فدراسیون ابری متمرکز شده‌ایم. راه‌حل پیشنهادی مبتنی بر ثبت‌نام یکباره، پروتکل احراز هویت کربروس، لیست‌های کنترل دسترسی و بلیت‌های مجوز برای پیاده‌سازی کنترل دسترسی است. ارزیابی عملکرد طرح، با استفاده از شبیه‌ساز کلودسیم نشان می‌دهد که طرح پیشنهادی سودمند است و زمان دسترسی به منابع مشترک در سناریوهای مختلف قابل قبول است. ارزیابی‌ها همچنین نشان می‌دهند که کشسانی (ارتجاع) منابع ابر، اثر قابل توجهی روی زمان دسترسی ندارد. از این‌رو سربار ناشی از مکانیسم امنیتی پیاده‌سازی شده در فدراسیون می‌تواند قابل تحمل باشد.

کلمات کلیدی: رایانش ابری، فدراسیون ابری، کنترل دسترسی، کربروس، ثبت‌نام یکباره.

۱- مقدمه

رایانش ابری[۱] یک الگوی موفق و توسعه‌یافته برای محاسبات توزیع‌شده و یک فناوری در حال رشد می‌باشد که امروزه به‌عنوان یکی از مهم‌ترین موضوعات در دنیای کامپیوتر و ارتباطات معرفی شده است و دسترسی به مخازن بزرگی از منابع را فراهم می‌سازد. ابرها به‌تنهایی توانایی پاسخگویی به درخواست‌های کاربران را ندارند و ازاین‌رو برای آنکه سودمند[۲] باشند باید با یکدیگر (سایر ابرها) همکاری و تعامل داشته باشند و در نتیجه فدراسیون ابری[۳] را به وجود می‌آورند. مزایایی چون افزایش حافظه، افزایش منابع، افزایش انعطاف‌پذیری و کاهش هزینه باعث استقبال روزافزون سازمان‌ها و کاربران از فدراسیون‌های ابری شده است. فدراسیون‌های ابری علاوه بر مزایای یاد شده، دارای چالش‌هایی نیز می‌باشند. حفظ حریم خصوصی و محرمانگی یا به عبارتی «کنترل دسترسی» ازجمله چالش‌ها و مشکلاتی هستند که فدراسیون‌های ابری با آن مواجه هستند. رویکردهای

گوناگونی برای کنترل دسترسی در فدراسیون ابری پیشنهاد و اعمال شده‌اند که هر یک خصوصیات و کاربردهای خاص خود را دارند.

مسئله اصلی در این پژوهش ارائه یک سیستم کنترل دسترسی برای فدراسیون ابری، جهت کاهش چالش‌های مدیریتی و امنیتی براساس بررسی مدل‌های موجود می‌باشد.

۱-۱- تعریف رایانش

رایانش ابری موج بعدی انقلاب فناوری اطلاعات است. به گفته نیکولاس در کتاب «تحول عظیم»، او رایانش ابری را در عصر اطلاعات با برق در عصر صنعت مقایسه می‌کند، جایی که شرکت‌ها، تولید برق خودشان را متوقف کردند و به شبکه برق جدید متصل شدند. تحولی مشابه در منابع محاسباتی نیز در حال اتفاق افتادن است. شرکت‌ها درحال حرکت به سمت مدل‌های محاسباتی مبتنی بر صنایع همگانی هستند. در کل رایانش ابری توجه شایان‌ذکری در جامعه علمی به دست آورده است، تعریفی که بیشترین پذیرش را کسب کرده توسط موسسه ملی استاندارد و فناوری[۴] ارائه شده است. رایانش ابری مدلی است برای فراهم کردن دسترسی آسان براساس تقاضای کاربر، از طریق شبکه، به مجموعه‌هایی از منابع محاسباتی قابل تغییر و پیکربندی مانند شبکه‌ها، سرورها، منابع ذخیره‌سازی، برنامه‌های کاربردی و خدماتی که این دسترسی بتواند با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت مستقیم ارائه‌دهنده خدمات به‌سرعت فراهم شده یا آزاد (رها) گردد [۲].

۱-۱-۱- سرویس‌های رایانش ابری و مدل‌های استقرار ابر

سرویس‌های متنوعی در رایانش ابری عرضه می‌شوند که عبارتند از زیرساخت به‌عنوان سرویس[۵]، بستر به‌عنوان سرویس[۶] و نرم‌افزار به‌عنوان سرویس[۷]. موسسه ملی استاندارد و فناوری[۸] چهار مدل توسعه را برای محاسبات ابری تعریف می‌نماید که عبارتند از [۳-۵]: ابر عمومی، ابر خصوصی، ابر ترکیبی، ابر انجمنی.

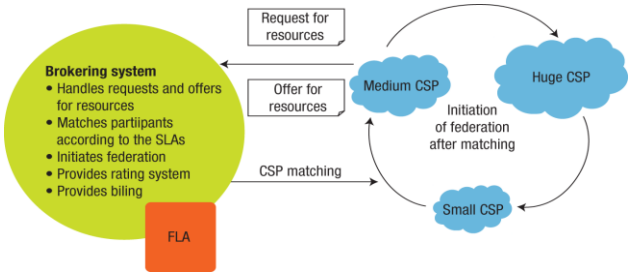
۲- فدراسیون ابری[۹]

برای برآوردن تقاضا با استفاده از ابرهای به‌هم‌پیوسته و مشترک، دانشگاه و صنعت می‌خواهند ابرهای ناهمگن (نامتجانس) را به شکل یک سیستم فدرال متصل کنند. این رویکرد امیدوارکننده است اما با چالش‌های قابل توجهی مواجه است. رایانش ابری به کاربران اجازه‌ی دسترسی به منابع و سرویس‌های محاسباتی مورد تقاضا و بدون نیاز به خرید زیرساخت‌هایشان و پرداخت فقط برای آنچه آن‌ها استفاده می‌کنند را می‌دهد. بسیاری از شرکت‌های ابری مثل آمازون و گوگل، پلت فرم‌های خودشان که شامل واسط‌های اختصاصی می‌باشد را دارند که تا زمانی که یک ارائه‌دهنده واحد می‌تواند به‌صورت کامل نیازمندی‌های مشتریان خود را برآورده کند، مشکلی ندارد. با این حال عدم‌وجود یا فقدان استانداردهایی برای تعامل و اتصال پلتفرم‌ها، باعث سخت شدن آن برای مشتریانی که نیاز به سرویس‌های ترکیب شده یا منابع فراهم‌کنندگان متعدد دارند، می‌شود. این اغلب به خاطر کاربرانی است که در پلتفرم‌ها و ارائه‌دهندگان خاص قفل شده‌اند[۱۰] [۶، ۷]. این موضوع منجر به ایده اتصال ابرها که تحت عنوان بین_ابر[۱۱] نیز شناخته می‌شود، می‌گردد [۶، ۸]. بین ـ ابر به محدودیت‌های رویکرد یک ارائه‌دهنده واحد مثل فقدان قابلیت همکاری بین پلتفرم‌ها، محدود بودن منابع و رو به اتمام بودن آن‌ها در زمان اوج تقاضای مشتری، وقفه‌های سرویس و تخریب کیفیت سرویس[۱۲]، اشاره دارد.

بین - ابر: یک بین - ابر، ابری از ابرهاست. در اصل آن ابری بزرگ، متشکل از بسیاری از ابرهای کوچک‌تر است که هر یک ویژگی‌ها و نیازهای خدماتی خاص خودشان را دارند.

یک ابر پیاده‌سازی کننده‌ی بین - ابر، شامل هر کدام یا ترکیبی از این گزینه‌ها است: ابر ترکیبی[۱۳]، محاسبات فلکی[۱۴]، مسابقه چند ابری[۱۵]، فدراسیون ابری. معماری فدراسیون ابری باید استانداردهایی را برای واسط کاربری[۱۶] به کار بگیرد. یک بروکر سرویس، ترجمه‌های بین رابط‌های کاربری را انجام می‌دهد و به‌روزرسانی‌های روی سرویس‌های ارائه شده را و تغییرات وضعیت کاربران و یا ترکیبی از این دو را ارائه می‌دهد [۷، ۹].

فدراسیون‌های ابری اغلب از کارگزاری‌ها یا بروکری‌ها[۱۷] استفاده می‌کنند. معماری بروکر درخواست موضوع (اشیا) مشترک (CORBA[۱۸]) و میان‌افزار بروکر درخواست موضوع (ORB[۱۹]) در ابتدا محبوب‌ترین رویکردها بودند [۱۰]. با این حال ظهور فنّاوری‌های مبتنی بر xml مثل SOAP توانایی استفاده از زبان یکسان در تشریح همه سرویس‌ها و درنتیجه، عدم‌نیاز به ترجمه را فراهم کرده است.



شکل ۱- معماری فدراسیون [۱]

شکل بالا یک معماری فدراسیون ابری که بروکر در آن نقش اصلی را ایفا می‌کند و ارائه‌دهنده‌های سرویس ابری در لبه‌ها عمدتاً از طریق بروکر (کارگزار) ارتباط دارند. سیستم کارگزاری ابر، منابع در دسترس فدراسیون را با تقاضای کاربر، با در نظر گرفتن توافقنامه‌های سطح سرویس شرکت‌کنندگان منطبق می‌کند. برای دست یافتن به این مطلب بروکر باید شیوه‌های مختلفی که هرکدام از ابرها، منابع قابل دسترس خود را توصیف و تشریح می‌کند را، درک کند و بفهمد. مطابق شکل بالا، کاربران درخواست‌هایشان را برای منابع و سرویس‌های ابری به ارائه‌دهندگان سرویس ابری ارسال می‌کنند، سپس پاسخ‌هایشان به بروکر ارسال می‌شود که کاربران را با ارائه‌دهندگان، براساس صدور صورتحساب، رتبه‌بندی و توافقات سطح سرویس منطبق می‌کند. این نتایج در یک فدراسیون توسط یک توافقنامه سطح فدراسیون (FLA) مدیریت و کنترل می‌شود.

برای اینکه فدراسیون، عملکرد درستی داشته باشد، همه اشخاص علاقه‌مند باید ثبت شوند و توافقنامه سطح فدراسیون که قوانین تعاملات خاص و مسئولیت‌ها و رفتارهای مجاز هریک از شرکت‌کنندگان، همراه با قوانین مالی و اداری و برخی جریمه و مجازات برای نقض قوانین و مقررات را توصیف می‌کند. طرفین، مادامی‌که از توافقات سطح فدراسیون پیروی می‌کنند می‌توانند هر زمانی که خواستند، فدراسیون را ترک کنند [۶، ۷].

۲-۱- مدل‌های ارتباطی بین فراهم‌کنندگان در فدراسیون ابری

ممکن است که یک ابر به‌منظور انجام خدمات مهاجرت، تهیه نسخه پشتیبان و ارائه خدمات مبتنی بر ابر به مشتریان خود، نیاز به خرید منابع از ابرهای دیگر داشته باشد. یک ابر زمانی که متوجه شود مرکز داده‌هایش در زمان‌های معینی

تحت استفاده نمی‌باشد، می‌تواند تصمیم به ارائه منابع به دیگر ابرها بگیرد. فرآیند تشکیل همکاری فدراسیون در سه مرحله کشف، تطبیق‌سازی و احراز هویت انجام می‌گردد که وظیفه کشف، پیدا کردن ابرهاست، تطبیق‌سازی عمل گزینش و انتخاب ابرها را براساس نیاز انجام می‌دهد و احراز هویت به‌وسیله ابرهای انتخاب‌شده یک زمینه اعتماد ایجاد می‌کند.

فازهای کشف و تطبیق‌سازی که برای ایجاد یک فدراسیون موردنیاز است را بروکر[۲۰] یا واسطه‌گر یا کارگذار می‌نامیم. چهار طرح برای ایجاد فدراسیون که ممکن است در کارگزارها اتفاق بیفتد، به قرار زیر هستند [۱۱]:

۱- متمرکز: این طرح یک کارگزار مشترک برای تمام ابرهای مسئول ایجاد فدراسیون است. در طرح متمرکز کارگزار یک شخص ثالث می‌باشد که اجازه می‌دهد یک ابر در فدراسیون طبق نیازهایش به دیگر ابرهای موجود در فدراسیون توجه کنند. این طرح یک رابط دارد که وظیفه‌اش مطابق‌سازی نیازهای فدراسیون ابری است.

۲- سلسله مراتبی: این طرح شامل تعدادی از کارگزاها می‌باشد که برای ایجاد فدراسیون باهم تعامل دارند.

۳- غیرمتمرکز: در این طرح یک تابع کارگزار وجود دارد که در داخل ابرها جاسازی شده است و برای انجام کارهای مربوط به آن به هیچ شخص ثالثی نیاز نیست. در این طرح ابرها با همدیگر برای همکاری گفتگو می‌کنند. اگرچه این طرح، یکی از انعطاف‌پذیرترین طرح‌ها می‌باشد، اما در مقابل نیز یکی از سخت‌ترین طرح‌ها برای پیاده‌سازی می‌باشد.

۴- ترکیبی: این طرح ترکیبی از طرح‌های سلسله مراتبی و غیرمتمرکز می‌باشد.

۲-۲- تهدیدهای امنیتی[۲۱] در رایانش ابری

به‌طور کلی، کنترل‌های امنیتی در ابر مشابه کنترل‌های امنیتی در هر محیط فناوری اطلاعات[۲۲] دیگر هستند. با این وجود به‌دلیل مدل‌های عملیاتی و فنّاوری‌های استفاده‌شده برای فراهم کردن خدمات ابری، ممکن است ریسک‌های را معرفی کند که مختص خود محیط‌های ابری باشند. موارد زیر به‌عنوان مهم‌ترین تهدیدات امنیتی خاص محاسبات ابری عنوان شده‌اند [۱۲-۱۴]:

سرقت اطلاعات[۲۳]، از دست دادن اطلاعات، دزدی حساب[۲۴] و یا ترافیک سرویس، واسطهای کاربردی[۲۵] ناامن، حمله انکار سرویس[۲۶]، بداندیشان داخلی، سوءاستفاده و استفاده نابهنجار از محاسبات ابری، کم بودن درجه دیجیتالی شدن، مسائل مربوط به فناوری به اشتراک گذاشته‌شده، چند مستأجری[۲۷]، انتقال اطلاعات[۲۸]، سازمانی، ریسک فنی[۲۹]، امنیت فیزیکی[۳۰]، تفکیک داده‌ها[۳۱]، بازیابی داده‌ها[۳۲] (بازیافت داده‌ها)، کنترل دسترسی[۳۳]، امنیت داده و حریم خصوصی[۳۴].

۳- کارهای گذشته

در ابتدا شرح مختصری درباره کنترل دسترسی[۳۵] بیان می‌نماییم، سپس کارهای انجام شده در این زمینه را مرور می‌کنیم.

یکی از خطیرترین وظایف امنیت، کنترل دسترسی به منابع است. کنترل دسترسی به مجموعه اقدامات و سیاست‌ها و روش‌های مربوط به اعطا یا رد مجوز دسترسی یک کاربر (مشتری) خاص به منابع و یا محدود کردن دسترسی به منابع سیستم‌های اطلاعاتی گفته می‌شود. وظیفه اصلی کنترل دسترسی، کنترل کردن دسترسی کاربران به سیستم و منابع آن به طریقی است که فقط دسترسی مجاز امکان‌پذیر باشد، این تنظیمات کنترل دسترسی بر پایه سیاست‌های کنترل دسترسی سیستم می‌باشد و توسط مکانیزم‌های کنترل دسترسی اجرا می‌گردد. در اصل کنترل دسترسی کاربرانی را که وارد شبکه می‌شوند اعتبارسنجی نموده و تعیین می‌نماید که به چه داده‌هایی می‌توانند دسترسی پیدا کنند و چه اقداماتی را نیز می‌توانند انجام دهند [۱۵، ۱۶].

۳-۱- عناصر اصلی

- **عامل[۳۶]:** یک عنصر فعال که باعث به جریان انداختن اطلاعات میان اشیاء و یا تغییر حالت سیستم شود. هر آنچه یا هر کس، اعم از انسان، ماشین، فرآیند و ... که متقاضی دسترسی است.
- **شیء یا منبع[۳۷]:** موجودیتی که حاوی اطلاعاتی باشد که نیاز به محافظت (تعیین سطح دسترسی) دارند. دسترسی به یک شیء، دسترسی به اطلاعات موجود در آن را نشان می‌دهد. نمونه‌هایی از اشیاء، بلوک، صفحات، فایل‌ها، دایرکتوری‌ها، برنامه، نمایش ویدئو، صفحه‌کلید، ساعت، پرینتر و ... می‌باشند.
- **عمل[۳۸]:** عملی که توسط عامل بر روی شیء یا منبع انجام می‌شود؛ که نمونه‌های آن شامل خواندن، نوشتن، چاپ، حذف و ... است.
- **اعتبار یا مجوز[۳۹]:** به امکان انجام یک عمل خاص بر روی یک شی خاص گفته می‌شود. اصطلاح مجوز در ادبیات امنیت کامپیوتر، به ترکیبی از شیء و عملیات اشاره دارد.

کنترل دسترسی در مورد ارتباط بین اشیا و عوامل می‌باشد. انتقال اطلاعات از یک شی به یک عامل را دسترسی می‌گویند. دسترسی فقط یک موضوع فنی و منطقی نیست، قسمت‌های فیزیکی مسئله را نباید فراموش کنید که به‌راحتی می‌تواند باعث افشای اطلاعات و یا ایجاد مشکلات عدیده شود. قانون اصلی کنترل دسترسی این است که دسترسی به منابع همیشه و به‌صورت معمول و پیش‌فرض باید در وضعیت منع[۴۰] شده باشد، مگر اینکه به یک عامل خاص اجازه دسترسی داده شده باشد [۱۷، ۱۸].

۳-۲- کارهای انجام شده در زمینه فدراسیون ابری

کارهای اصلی مربوط به فدراسیون‌های ابری توسط Buyya در [۱۹] ارائه شده است که در آن یک فدراسیون از ابرها ، به‌عنوان یک مدل از چندین ارائه‌دهنده‌ی در حال تعامل، برای جستجو منابع است، تشریح شده است. این جستجو به‌صورت مستقیم در بین ارائه‌دهندگان اتفاق می‌افتد یعنی پشتیبانی سرتاسری برای آن وجود ندارد. کاربران ابر با یک ارائه‌دهنده، که مسئول انجام تقاضاهای کاربر است در ارتباط هستند. رویکردهای مشابهی در [۲۰-۲۳] پیدا می‌شود. بعضی تجارب دیگر در مورد فدراسیون‌های ابری در [۲۴-۲۶] ارائه شده است. این‌ها از رویکرد پشتیبانی سرتاسری، برای تعیین محل کردن منابع ارائه شده، استفاده می‌کنند. با این‌حال در این مدل‌ها با یک زیرساخت کنترل متمرکز، هنوز هم ارائه‌دهنده ابر مسئولیت مدیریت هویت را بر عهده دارد، برای مثال ویژگی‌های کاربر توسط ارائه‌دهندگان ابر به‌صورت محلی ذخیره می‌شوند. در حقیقت کاملاً روشن نیست که چگونه مدیریت هویت در اغلب رویکردهای ذکر شده اجرا شده است.

این طرح‌های پیشنهادی در اغلب موارد مبتنی بر راه‌حل‌های سنتی مدیریت هویت هستند، زمانیکه فدراسیون‌های ابری با این کنترل‌های هویت محلی تعریف شده است (تشکیل شده است) مسائل خاصی پدید می‌آید. با احراز هویت محلی و تهیه منابع در سطح ارائه‌دهنده، تعیین مقدار استفاده از منابع (برای انجام حسابرسی) در سطح فدراسیون دشوار است.

رویکردی که در [۲۰] ارائه شده یک استثنا است که در آن نویسندگان فدراسیونی از ابرهای مبتنی بر ارتباطات فراهم‌کننده - فراهم‌کننده را پیشنهاد می‌کنند. این طرح پیشنهادی مدیریت هویت فدراسیونی را در نظر می‌گیرد.

بنابراین احراز هویت کاربر در همه ارائه‌دهندگان فدراسیونی معتبر است، با تضمین اینکه منابع ارائه شده توسط ابرهای دیگر در فدراسیون می‌تواند توسط کاربر بدون نیاز به احراز هویت دوباره به کار گرفته شود. به هر حال هزینه‌های نگهداری ویژگی‌های کاربر محلی است.

در [۲۷] یک مدل کنترل دسترسی برای ابرهای فدرال (فدراسیون ابری) پیشنهاد و ارائه شده است. این مدل کنترل دسترسی مبتنی بر ویژگی[۴۱] است که ویژگی‌های کاربر، شیء و سیستم را با همدیگر به‌وسیله‌ی یک مجموعه از قوانین دسترسی برای تعیین اینکه آیا دسترسی به یک منبع معین را مجاز می‌داند یا نه، ترکیب می‌کنند.

V.Echevarna و همکارانش [۲۸] رویکردی به نام مجوز به‌عنوان سرویس[۴۲] (PaaS) توسعه دادند که یک سرویس کنترل دسترسی مجزا از خدمات ابری دیگر را ارائه می‌دهد. مجوزها از طریق رمزگشایی کلیدهای مبتنی بر ویژگی‌های کاربرانی که به آن‌ها دسترسی اهدا شده است، مدیریت می‌شوند.

در کاری که اخیراً توسط Dongwan Shin [۲۹] انجام شده کنترل دسترسی‌های مبتنی بر نقش دقیق و خوبی به IaaS با معرفی یک دامنه قابل اعتماد برای کاربران، نقش‌ها و مجوز (اجازه)های دسترسی استفاده می‌شود، اضافه می‌شود؛ اما تمام کاربران و نقش‌ها و مجوزها در این دامنه به‌صورت مرکزی مدیریت می‌شوند بنابراین دسترسی فدرال را فراهم نمی‌کند و اجازه می‌دهد که نقش‌ها و ویژگی‌ها توسط مقامات خارجی معینی، تعیین شوند یا تخصیص داده شوند.

پروژه Contrail [۲۵] چارچوبی برای ساخت یک فدراسیون ابری می‌باشد. این بر اساس مجموعه‌ای از مؤلفه‌های اصلی ساخته شده است: پلتفرم اجرای مجازی[۴۳] (VEP)، XtreemFS و فدراسیون ابری Contrail. یک پروژه بزرگ است که توسط اتحادیه اروپا تأمین می‌شود و تحت توسعه فعال می‌باشد. همچنین از مدیریت هویت فدرال استفاده می‌کند و از مجوزِ زبان نشانه‌گذاری کنترل دسترسی قابل توسعه (XACML) و مدل کنترل دسترسیِ کنترل مصرف[۴۴] (UCON) حمایت و پشتیبانی می‌کند.

یک طرحِ کاربنیادی برای بین ـ ابر در [۳۰، ۳۱] ارائه شده است. در این آثار مجموعه‌ای از ابرها براساس یک معماری شامل یک ریشه بین ـ ابر، یک مسئول برای نام‌گذاری و اعتماد در نظر گرفته شده است. دروازه‌های[۴۵] بین ـ ابر، برقراری ارتباط بین پروتکل‌ها و استانداردها و نهایتاً ابرها. این آثار نشان می‌دهند که اعتماد توسط ریشه بین ـ ابر در این پیکربندی که شبیه به یک فدراسیون هویت است، مدیریت می‌شود.

بعضی از چالش‌های کنترل دسترسی در محیط‌های با توزیع‌شدگی بالا (بسیار توزیع‌شده) در [۳۲] که مدل‌های کنترل دسترسی مبتنی بر ویژگی (ABAC)، کنترل مصرف، و کنترل دسترسی منطبق با ریسک (RAdAC) را با هم مقایسه می‌کند.

ایده استفاده از کنترل دسترسی مبتنی بر ریسک در رایانش ابری در [۳۳] ارائه شده است که در آن نویسندگان ادعا می‌کنند که این مدل برای حل مشکلات ایجاد شده به واسطه چند مستأجری و همچنین اینکه یک محیط پویا نیاز به یک مدل کنترل دسترسی پویا دارد، مناسب است. اینائر، سناریویی را ارائه می‌دهد که کنترل دسترسی منطبق با ریسک (RAdAC) برای اجرای کنترل دسترسی بین مستأجران یک ابر، با توجه به خطرات ناشی از دسترسی غیرقانونی به اطلاعات کاربران توسط مستأجران دیگر یا توسط مدیران استفاده می‌شود و به کار می‌رود.

Arias و همکاران [۳۴] مجموعه‌ای از معیارهای ارائه شده در یک طبقه‌بندی را پیشنهاد می‌دهد که برای ایجاد فدراسیون‌های هویت در ابر و برای رسیدگی به درخواست‌های دسترسی استفاده می‌گردد. نویسندگان ادعا می‌کنند که مدل مدیریت هویت فدرال توسط مدل‌های اعتماد اساسی مهار می‌شود و از اجرای آن ممانعت به عمل می‌آید که باید از قبل اجرا شود و استفاده از شاخص‌های ریسک می‌تواند این مشکل را کاهش و تخفیف دهد.

در [۳۵] یک سیستم کنترل دسترسی پویای مبتنی بر ریسک برای فعال‌سازی فدراسیون‌های ابری بدون نیاز به فدراسیون‌های هویت (اما با امکان استفاده از آن‌ها) ارائه شده است. به واسطه حذف فدراسیون‌های هویت طرح پیشنهادی استفاده از فدراسیون‌های ابری را تسهیل می‌کند، چراکه وابسته به استقرار یا ایجاد توافقات و قلمروهای اعتماد نیست، همچنین با اجتناب از تشکیل جزایر هویت[۴۶]، مقیاس‌پذیری را افزایش می‌دهد. سهم اصلی این اثر تعریف یک سیستم کنترل دسترسی مبتنی بر ریسک برای فدراسیون‌های ابری و پیشنهاد استفاده از خط‌مشی (سیاست)های ریسک در قالب فایل‌های xml که اجازه استفاده از معیارهای ریسک مختلف و روش‌های کمیت‌سنجی که لزوماً از پیش تعریف نشده‌اند را می‌دهد، می‌باشد.

در [۳۶] عنوان شده که با رشد تعداد کاربران در فنّاوری رایانش ابری، کنترل دسترسی به منابع، اهمیت بسزایی پیدا می‌کند. این اثر، یک رویکرد مبتنی بر اتوماتای یادگیر[۴۷] برای کنترل دسترسی کاربران به منابع، براساس پارامترهای ریسک، اعتماد و اندازه‌گیری دسترسی ارائه کرده است.

در رویکرد پیشنهادی با حذف مؤلفه مرکزی فدراسیون هویت و عدم‌نیاز به تشکیل حوزه امن، محدودیت مقیاس‌پذیری از بین رفته است و در هر لحظه ابرها می‌توانند با همدیگر بدون نیاز به اقدامات قبلی ارتباط برقرار نمایند در نتیجه یک رویکرد کاملاً پویا می‌باشد. همچنین هر تغییری در رفتار کاربران باعث بروزرسانی همه‌ی پارامترهای محاسبه اعتماد و ریسک می‌شود. از سوی دیگر رویکرد پیشنهادی یک روش انعطاف‌پذیر است زیرا تغییر شرایط کاربر از مجاز به غیرمجاز به واسطه تغییر در رفتار او یا برعکس امکان‌پذیر است. همچنین امکان استفاده از تکنیک‌های تصمیم‌گیری دیگر مانند مدل مخفی مارکوف و درخت تصمیم‌گیری برای توسعه رویکرد پیشنهادی امکان‌پذیر است.

۴- مدل کنترل دسترسی پیشنهاد شده

برخی موقعیت‌های مختلف که منجر به ایجاد فدراسیون ابری و همکاری بین فراهم‌کنندگان ابری می‌شود عبارت‌اند از: فقدان منابع در یک ارائه‌دهنده منفرد برای پشتیبانی از تقاضاهای زیاد، نیاز به خصوصیات یا سرویس‌هایی که توسط یک فراهم‌کننده معین ارائه نشده است و توزیع یک برنامه کاربردی روی ارائه‌دهندگان مختلف برای کمک به بهبود بهره‌وری و قابلیت اعتماد و همکاری بین ارائه‌دهندگان ابری کوچک. به هر حال ایجاد شبکه‌های معتمدی که به محدوده گسترده‌ای از کاربران خدمت‌رسانی و سرویس‌دهی می‌کند، می‌تواند چالش‌های زیادی را در زمینه مکانیسم‌های امنیتیِ احراز هویت و مجوز دهی[۴۸] (اعطای مجوز) مطرح کند. برای عبور از مشکلات احتمالی در برخورد با مسائل امنیتی، مدل‌های مدیریت هویت تبدیل به نقطه کلیدی برای این سیستم‌های بزرگ می‌شود.

۴-۱- شرح مختصری در مورد ثبت‌نام یکباره

ثبت‌نام یکباره (SSO) به عمل وارد شدن کاربر به سایت‌ها و برنامه‌های مختلف تنها با یک نام کاربری و رمز عبور[۴۹] یکسان گفته می‌شود. به این معنی که اطلاعات مربوط به تائید هویت و اعتبارسنجی کاربر یعنی نام کاربری و رمز عبور در یک مکان امن به‌صورت موقت نگهداری می‌شود و پس از آن، این کاربر به‌منظور ورود به سایت‌ها و بخش‌های مختلف (دسترسی به برنامه‌های متعدد) نیازی نیست که مجدداً ورود[۵۰] نماید. در این هنگام در صورت لزوم اطلاعات حساب کاربر با اطلاعات ثبت شده‌ای که مربوط به تعیین سطح دسترسی و حقوق آن کاربر

می‌باشد، مطابقت داده می‌شود و در صورت عدم‌محدودیت، اجازه ورود برای او صادر می‌گردد. به عبارت دیگر SSO فرآیند (پروسه‌ی) احراز هویت یا نشست کاربر می‌باشد که به او اجازه می‌دهد تا برای دستیابی به چندین برنامه نرم‌افزاری مستقل ولی مرتبط از یک نام کاربری و کلمه عبور یکسان استفاده نمایند.

۴-۲- مرور اجمالی عملکرد طرح پیشنهادی

شکل زیر یک نمای اولیه و ابتدایی از طرح پیشنهادی را نشان می‌دهد که ترکیبی از اجزای کاربردی زیر می‌باشد:

شکل ۲- نمای اولیه و خلاصه شده‌ی طرح

- **کاربر**: مشتریانی که قصد استفاده از خدمات ارائه شده در فدراسیون ابری را دارند.

- **ارائه‌دهنده هویت:** که همان‌طور که قبلاً هم بیان شد، نقش آن احراز هویت کاربرانی است که درخواست دسترسی به منابع ارائه شده در فدراسیون ابری را دارند. این سرور ترکیبی از سرور احراز هویت (AS) و سرور اعطای بلیت (TGS) می‌باشد.
- **ارائه‌دهنده سرویس فدرال**[۵۱]: این سرور روند ثبت‌نام کاربران را در سرویس‌های مختلف فدراسیون انجام می‌دهد و اعتبار بلیت‌های فدرال را بررسی و در نهایت، تائید یا رد می‌نماید.
- **منابع و سرویس‌های مشترک:** سرویس‌های مختلفی که توسط ارائه‌دهندگان مختلف شرکت‌کننده در فدراسیون، برای استفاده کاربران عضو فدراسیون به اشتراک گذاشته شده‌اند.

در طرح پیشنهادی از همکاری چند ارائه‌دهنده ابری متفاوت که می‌توانند نامتجانس (ناهمگن) هم باشند، برای تشکیل فدراسیون ابری استفاده نموده‌ایم. همان‌طور که در فصل اول بیان شد سازمان‌های ابری به‌طور داوطلبانه بعد از ثبت یک توافقنامه سطح فدراسیون، در فدراسیون ابری شرکت می‌کنند. کاربران فدراسیون به یک مکانیسمی برای دسترسی مشترک به سرویس‌های قابل دسترس نیاز دارند که ما در اینجا از یک بروکر سرویس که ترجمه‌های لازم برای ارتباط ارائه‌دهندگان فدراسیون را انجام می‌دهد، استفاده نموده‌ایم. همچنین از طرح متمرکز برای ایجاد فدراسیون استفاده کرده‌ایم هر کدام از ارائه‌دهندگان ابری دارای منابع، زیرساخت و سیاست‌های مخصوص به خود هستند.

در این فدراسیون بروکر مرکزی نقش اصلی را ایفا می‌کند و ارائه‌دهندگان خدمات ابری از طریق این بروکر (کارگزار) با همدیگر ارتباط دارند. این سیستم بروکری منابع در دسترس فدراسیون را با تقاضای کاربران منطبق می‌سازد و این تقاضاها را برای اجرا شدن در سرویس‌های فدراسیون به ارائه‌دهندگان مختلف که عضو فدراسیون هستند ارسال می‌نماید و ارائه‌دهندگان ابری پس از انجام وظایف محوله، پاسخ‌های خود را به بروکر برمی‌گردانند. جهت این که فدراسیون به درستی کار کند و منابع آن دردسترس افراد غیرمجاز قرار نگیرد نیاز به یک سیستم کنترل دسترسی ایمن داریم که برای رسیدن به این هدف یک سیستم کنترل دسترسی ثبت‌نام یکباره (SSO) مبتنی بر کربروس را ارائه نمودیم که متعاقباً نحوه کارکرد آن را توضیح می‌دهیم. در شکل صفحه بعد نمای کلی از طرح به تصویر کشیده شده است.

روند انجام کار به این شکل است که کاربر پیام درخواست دسترسی به سرور اهدای بلیت ($TGS^{۵۲}$) را به‌وسیله ارسال اعتبارات خود برای سرور احراز هویت ($AS^{۵۳}$) ارسال می‌نماید. حال سرور احراز هویت، به وسیله ارسال پیامی که توسط کلیدِ مشتق شده از رمز عبور کاربر (K_C) رمز گذاری شده و شامل بلیت هم هست، به کاربر پاسخ می‌دهد. پیام‌های رمزگذاری شده همچنین شامل یک کپی از کلید جلسه $K_{C.TGS}$ هستند که با توجه به اندیس آن‌ها می‌توان دریافت که این یک کلید جلسه، برای کاربر و سرور اهدای بلیت است.

(1) $C \rightarrow AS: \quad ID_C || ID_{TGS} || TS_1$
(2) $AS \rightarrow C: E_{K_C} [K_{C.TGS} || ID_{TGS} || TS_2 || Lifetime_2 || Ticket_{TGS}]$

$Ticket_{TGS} = E_{K_{TGS}}[K_{C.TGS} || ID_C || AD_C || ID_{TGS} || TS_2 || Lifetime_2]$

شکل ۳- مبادله سرویس احراز هویت: جهت به دست آوردن بلیت واگذاری بلیت [۲۰]

(3) $C \rightarrow TGS: \quad ID_{SP} || Ticket_{TGS} || Authenticator_C$
(4) $TGS \rightarrow C: \quad E_{K_{C.TGS}} [K_{C.SP} || ID_{SP} || TS_4 || Ticket_{SP}]$
   a. $Ticket_{TGS} = E_{K_{TGS}} [K_{C.TGS} || ID_C || AD_C || ID_{TGS} || TS_2 || Lifetime_2]$
   b. $Ticket_{SP} = E_{K_{SP}}[K_{C.SP} || ID_C || AD_C || ID_{SP} || TS_4 || Lifetime_4]$
   c. $Authenticator_C = E_{K_{TGS}} [ID_C \| AD_C \| TS_3]$

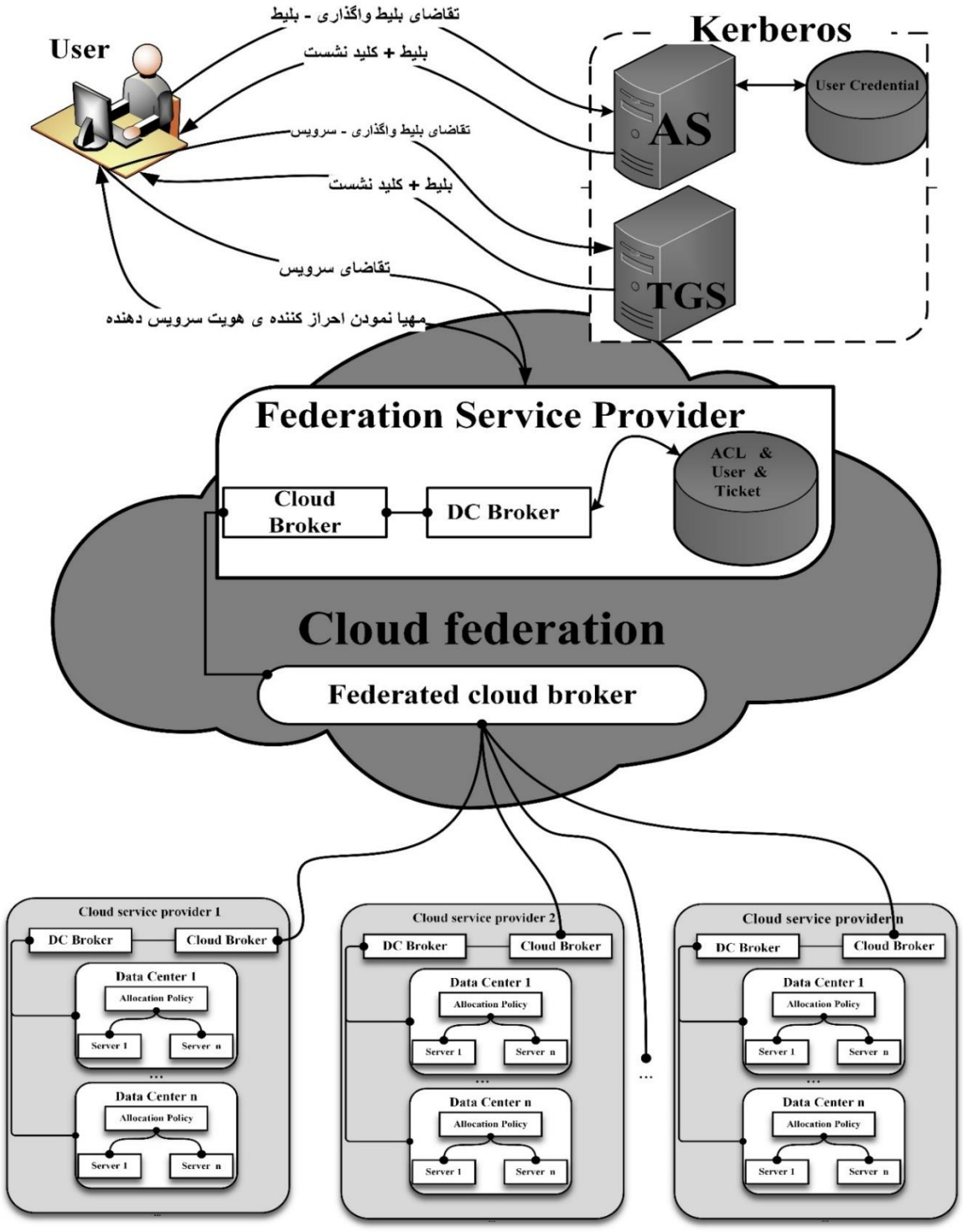
شکل ۴- تبادل سرویس واگذاری بلیت: برای به دست آوردن بلیت سرور ارائه‌دهنده سرویس [۲۰]

(5) $C \rightarrow SP: \quad Ticket_{sp} || Authenticator_C || Service /$
$Ticket_{sp} || Authenticator_C || Federal Ticket$
(6) $SP \rightarrow C: \quad E_{K_{C.SP}} [(TS_6 + 1) || Federal Ticket]$
   a. $Ticket_{SP} = E_{K_{SP}}[K_{C.SP} || ID_C || AD_C || ID_{SP} || TS_4 || Lifetime_4]$
   b. $Authenticator_C = E_{K_{C.SP}}[ID_C \| AD_C \| TS_5$
   c. $Service = E_{K_{C.SP}}[C_i S_j || TS_6]$
   d. $Federal Ticket = E_{K_{C.SP}}[ID_{SP} || ID_T || ID_C || AD_C || TS_8 || C_i S_j P_k]$

شکل ۵- تبادل پیام بین ارائه‌دهنده سرویس فدراسیون و کاربر برای به دست آوردن سرویس [۲۰]

از آنجاکه این کلید جلسه در داخل پیام رمز شده با (K_C) است لذا تنها کاربر سرویس‌گیرنده می‌تواند آنرا بخواند. کلید جلسه مشابه در بلیت گنجانده شده است که فقط می‌تواند توسط سرور اهدای بلیت خوانده شود؛ بنابراین کلید جلسه به شکلی امن به هر دو گیرنده، کاربرو سرور اهدای بلیت، تحویل داده می‌شود. با توجه به بلیت و کلید جلسه حال کاربر برای رسیدن به سرور اهدای بلیت، آماده است. کاربر یک پیام را که شامل بلیت به همراه شناسه درخواست سرور (ID_{SP}) است برای سرور اهدای بلیت ارسال می‌نماید. علاوه بر این، کاربر یک تائیدکننده اعتبار[۵۴] که شامل شناسه، آدرس کاربر و برچسب زمان است را نیز منتقل می‌نماید. برخلاف بلیت که قابل استفاده مجدد است، تائیدکننده هویت تنها برای یک‌بار استفاده در نظر گرفته شده و دارای طول عمر بسیار کوتاهی است.

حال سرور اهدای بلیت می‌تواند بلیت را با کلیدی که با سرور احراز هویت به اشتراک گذاشته، رمزگشایی نماید. این بلیت نشان می‌دهد که کلید جلسه $K_{C.TGS}$ به کاربر داده شده است. همچنین این کلید بیان می‌نماید که آن کس که از $K_{C.TGS}$ استفاده نماید، باید کاربر باشد.



شکل ۶- نمای کلی طرح اصلی و روند انجام کار

حال سرور اهدای بلیت از کلید جلسه برای رمزنگاری استفاده می‌نماید و می‌تواند نام و آدرس تائیدکننده اعتبار را با بلیت و آدرس شبکه پیام ورودی مقایسه نماید. اگر با هم تطابق داشتند آنگاه سرور اهدای بلیت مطمئن خواهد شد که فرستنده بلیت درواقع مالک واقعی بلیت است. توجه داشته باشید که بلیت (البته منظور بلیت فدرال نیست)، بلیت هویت کسی را ثابت نمی‌نماید بلکه تنها راهی برای توزیع امن کلید است. این تائیدکننده هویت است که هویت سرویس گیرنده را اثبات می‌کند.

پاسخ آمده از جانب سرور اهدای بلیت در پیام ۴ مشابه پیام ارسالی از طرف سرور احراز هویت (پیام ۲) می‌باشد. این پیام با کلید جلسه به اشتراک گذاشته شده توسط سرور اهدای بلیت و کاربر رمزگذاری شده و همچنین شامل یک کلید

جلسه که بین کاربر و ارائه‌دهنده سرویسِ فدراسیون ابری مشترک است، شناسه ارائه‌دهنده سرویس (sp[۵۵]) و برچسب زمانی بلیت خواهد بود. خود بلیت شامل یک کلید جلسه مشابه خواهد بود.

سرویس‌های مختلفی از طرف ارائه‌دهندگان شرکت‌کننده در فدراسیون ابری ارائه شده است و در ارائه‌دهنده سرویس مربوط به فدراسیون به اشتراک گذاشته می‌شود. حال کاربر دارای یک بلیت اجازه واگذاری سرویس قابل استفاده مجدد برای ارائه‌دهنده سرویس (sp) خواهد بود.

هنگامی‌که کاربر این بلیت را ارائه می‌دهد، همان‌طور که در پیام ۵ نشان داده شده است، یک تائیدکننده هویت و سرویس‌هایی را که می‌خواهد در آن‌ها ثبت‌نام کند و از آن‌ها استفاده نماید را نیز می‌فرستد. سرویس‌دهنده می‌تواند بلیت را رمزگشایی نموده، کلید جلسه را بازیابی کرده و تائیدکننده هویت را نیز رمزگشایی نماید؛ و پس از تائید هویت کاربر (مشتری)، ارائه‌دهنده سرویس اقدام به ثبت‌نام وی در سرویس‌های درخواستیِ او نموده و یک بلیت فدرال[۵۶] را برای کاربر ثبت می‌نماید. در این بلیت فدرال، شماره شناسایی بلیت، شماره شناسه کاربر، آدرس شبکه کاربر، شماره شناسایی ارائه‌دهنده سرویس و همچنین سرویس‌هایی از سرویس‌دهنده‌های مختلف با مجوزهای دسترسی مختلف برای کاربر ثبت شده، نیز درج شده است.

متعاقباً سرویس‌دهنده جهت احراز هویت متقابل خود به کاربر و همچنین برای اینکه کاربر از ثبت‌نام خود درسرویس‌های مختلف درخواستیِ خود مطمئن گردد، این بلیت فدرال را به او ارسال می‌نماید. شماره این بلیت فدرال، در یک لیست کنترل دسترسی[۵۷] به همراه شماره شناسایی کاربر ثبت می‌گردد و همچنین خودِ بلیت نیز در یک مخزن بلیت، برای انجام عملیات ثبت‌نام یکباره (SSO) نگهداری می‌شود و اطلاعات کاربر نیز در یک مخزن دیگر ثبت می‌گردد. در مجموع از سه مخزن برای انجام عملیات ثبت‌نام یکباره، استفاده شده است. اولین مخزن حاوی لیست‌های کنترل دسترسی است که شامل شماره شناسایی کاربر و شماره بلیت فدرال است، مخزن دوم نیز برای ذخیره‌سازی بلیت فدرال به جهت دسترسی به اطلاعات بلیت و مجوزهای دسترسی (سطوح دسترسی) کاربر به سرویس‌های مختلف در فدراسیون ابری در نظر گرفته شده است، سومین مخزن هم برای ذخیره‌سازی اطلاعات جامع کاربران فدراسیون برای مقاصد مختلف در نظر گرفته شده است. حین صدور بلیت فدرال برای کاربر، بلیت صادر شده برای او در این مخازن برای مراجعات بعدی کاربر ذخیره می‌گردد.

در شکل‌های زیر نمونه‌هایی از لیست کنترل دسترسی، نمونه بلیت فدرال و قالب اطلاعات کاربر که در سمت ارائه‌دهنده سرویسِ فدراسیون ذخیره می‌شوند، نمایش داده شده است.

جدول ۱- نمونه بلیت فدرال

Federal Ticket
ID_T
ID_C
AD_C
ID_{sp}
$C_iS_jP_k$

جدول ۲- نمونه مدخل اطلاعات کاربر

Client / user
ID_C
AD_C

جدول ۳- لیست کنترل دسترسی

ID_C	ID_T
ID_{C1}	ID_{TC1}
ID_{C2}	ID_{TC2}
ID_{C3}	ID_{TC3}
و...	و...

مراجعه کاربر به فدراسیون جهت استفاده از سرویس‌های آن از سه حالت زیر خارج نیست؛ در هر سه حالت کاربر برای دریافت سرویس اول پیام شماره ۵ را برای سرور ارسال می‌نماید و سرور با مراجعه به لیست کنترل دسترسی (ACL)، از بین سه حالت زیر بسته به وضعیت کاربر گزینه مناسب را برای سرویس‌دهی به کاربر اتخاذ می‌نماید:

۱) اگر کاربر از قبل ثبت شده باشد و بلیتی که از طرف سرور اهدای بلیت، برای دسترسی به ارائه‌دهنده سرویس در فدراسیون دریافت کرده بود انقضاء نیافته باشد، به مخزن بلیت فدرال مراجعه می‌شود و با توجه به سطوح دسترسی کاربر به سرویس‌های مختلف، مجوز دسترسی به او اهدا می‌شود.

۲) اگر کاربر از قبل ثبت شده باشد و بلیتی که از طرف سرور اهدای بلیت، برای دسترسی به ارائه‌دهنده سرویس در فدراسیون دریافت کرده بود انقضاء یافته باشد، با پیامی به کاربر اطلاع داده می‌شود که باید از سرور اهدای بلیت، جهت مراجعه به ارائه‌دهنده سرویسِ فدراسیون، بلیت تهیه نمایند.

۳) اگر کاربر از قبل ثبت نشده باشد باید برای او یک بلیت فدرال صادر گردد و این بلیت صادر شده برای کاربر ارسال گردد و همچنین شماره بلیت فدرال در لیست کنترل دسترسی در مقابل شماره شناسایی کاربر درج گردد و محتوای بلیت نیز در مخزن بلیت درج شود و پس از آن مجوز دسترسی برای کاربر صادر شود.

۵- شبیه‌سازی و ارزیابی طرح پیشنهادی

برای انجام شبیه‌سازی طرح پیشنهادی، از کلودسیم[۵۸] به‌عنوان شبیه‌ساز فدراسیون ابری استفاده شده است. مطابق [۳۷، ۳۸] کلودسیم یک چهارچوب تعمیم‌یافته و قابل توسعه است که اجازه مدل‌سازی، شبیه‌سازی و آزمایش زیرساخت‌های ابری و سرویس‌های قابل اعمال را می‌دهد. این یکی از محبوب‌ترین محیط‌های شبیه‌سازی است و به‌طور گسترده توسط انجمن محققان در زمینه رایانش ابری مورد استفاده قرار می‌گیرد. کلودسیم به‌عنوان یک کد منبعِ رایگانِ جاوا[۵۹] در دسترس است. ایندر کلاس (دسته‌بندی)های مدل‌سازی نهادهای ابری مختلف ساخته شده است. متناسب با ویژگی لایه‌ای (لایه‌بندی شده) و همچنین انتزاع معماری رایانش ابری است و انعطاف‌پذیری زیادی را در دست‌کاری نهادها (موجودیت‌ها)ی مختلف نشان می‌دهد. آزمایش‌های انجام شده، بر روی یک کامپیوتر شخصی با مشخصات زیر انجام شده است.

جدول ۴- مشخصات سیستم

CPU	intel(R) Core (TM) i5- 2450CPU@ 2.50 GHz 2.50GHz
RAM	4GB
OS	Windows

۵-۱- پارامترهای شبیه‌سازی طرح پیشنهادی

ما طرح پیشنهادی به‌وسیله شبیه‌سازی ثبت‌نام یکباره که با کربروس به جهت پیاده‌سازی یک راه‌حل ایمنِ احراز هویت و کنترل دسترسی در فدراسیون ابری ادغام‌شده است، پیاده‌سازی شده است. فدراسیون ابری ذکر شده شامل سه ارائه‌دهنده ابری، سه مرکز داده، سه میزبان و ۱۰۰۰ ماشین مجازی و تعداد ۱۰۰۰ وظیفه (تکه ابر) می‌باشد. در طول فاز توسعه بعضی از کلاس‌های کلودسیم تغییر داده شده و بعضی کلاس‌های جدید که درخور نیازمندی‌های طراحی راه‌حل هستند اضافه شده است.

فدراسیون شبیه‌سازی شده شامل سه ارائه‌دهنده ابری است که در هر کدام یک مرکز داده و یک میزبان و تعدادی منابع (سرویس‌های) مشترک قرار داده شده است. ارائه‌دهنده سرویس فدرال (فدراسیون) مدیریت لیست‌های کنترل دسترسی و کلیه‌ی بررسی‌های لازم برای مجوز، طی فرآیند مجوزدهی را پیاده‌سازی می‌نماید. حین شبیه‌سازی تعداد منابع مشترک ارائه شده در هر مرکز داده را به‌منظور تعیین تأثیرشان بر روی زمان دسترسی، مادامی‌که امنیت طرح پیشنهادی را در نظر می‌گیریم، تغییر می‌دهیم.

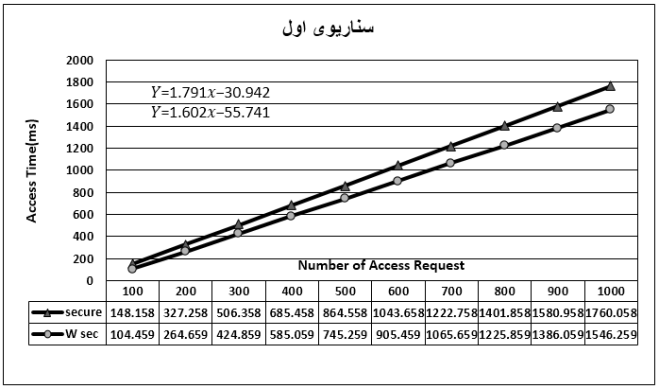
مجموعه داده موردنیاز برای ایجاد بارِکاری لازم جهت اجرای عمل شبیه‌سازی فدراسیون منظوره را از [۳۹] دانلود نموده و پس از ایجاد بارِکاری مناسب، عمل شبیه‌سازی انجام شده است.

سه سناریوی شبیه‌سازی را تعریف شده است: در سناریوی اول از سه ارائه‌دهنده ابری با سه مرکز داده و سه میزبان و سه منبع مشترک، استفاده شده است. در سناریوی دوم تعداد منابع را به ۶ عدد افزایش یافته؛ و در نهایت در سناریوی سوم از سه ارائه‌دهنده ابری، سه مرکز داده، سه میزبان و ۹ منبع مشترک استفاده می‌شود.

سه سناریو ارائه شده در بالا در هر دو حالتِ با و بدون امنیت با استفاده از حداکثر ۱۰۰۰ درخواست دسترسی کاربر، شبیه‌سازی شده‌اند. اشکال زیر یک مقایسه‌ی تنوعِ زمان دسترسی کاربران بین نسخه ایمن و نسخه ناامنِ مدل برای سناریوهای در نظر گرفته شده را نشان می‌دهند.

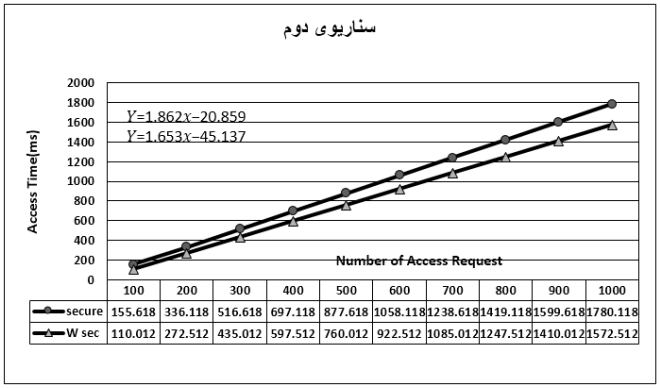
این شکل‌ها مقدارهای میانگین نتایج ۱۰ آزمایش برای هر سناریو را نشان می‌دهند. در نمودارهای نمایش داده شده در بالا ملاحظه می‌کنیم که خط منحنی کنترل دسترسی امن و ناامن شکل یکسانی برای هر سناریو دارد. اندازه‌ها (مقادیر)ی همه سناریوها یک تابع خطی را نشان می‌دهد (Y=Ax+B).

Y_{SECURE} تابع خطیِ نسخه امن و Y_{WS} تابع خطی نسخه ناامن است. سربار[۶۰] سیستم کنترل دسترسی به‌عنوان تفاوت بین نسخه‌های امن و ناامن سیستم، اندازه‌گیری شده و ارائه شده است.



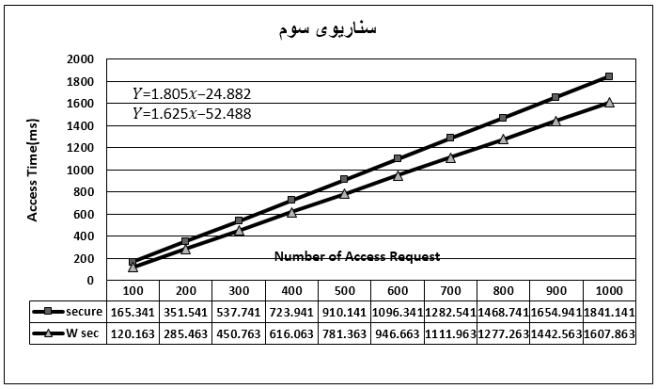
	100	200	300	400	500	600	700	800	900	1000
secure	148.158	327.258	506.358	685.458	864.558	1043.658	1222.758	1401.858	1580.958	1760.058
W sec	104.459	264.659	424.859	585.059	745.259	905.459	1065.659	1225.859	1386.059	1546.259

شکل ۷- زمان دسترسی در مقابل تعداد درخواست‌های دسترسی در سناریوی اول



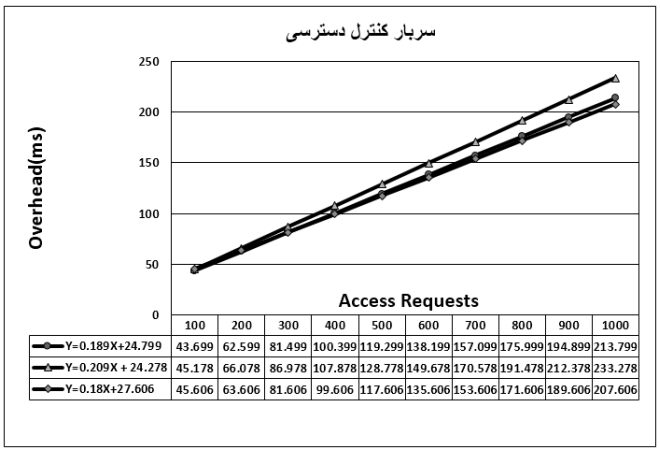
	100	200	300	400	500	600	700	800	900	1000
secure	155.618	336.118	516.618	697.118	877.618	1058.118	1238.618	1419.118	1599.618	1780.118
W sec	110.012	272.512	435.012	597.512	760.012	922.512	1085.012	1247.512	1410.012	1572.512

شکل ۸- زمان دسترسی در مقابل تعداد درخواست‌های دسترسی در سناریوی دوم



	100	200	300	400	500	600	700	800	900	1000
secure	165.341	351.541	537.741	723.941	910.141	1096.341	1282.541	1468.741	1654.941	1841.141
W sec	120.163	285.463	450.763	616.063	781.363	946.663	1111.963	1277.263	1442.563	1607.863

شکل ۹- زمان دسترسی در مقابل تعداد درخواست‌های دسترسی در سناریوی سوم



	100	200	300	400	500	600	700	800	900	1000
Y=0.189X+24.799	43.699	62.599	81.499	100.399	119.299	138.199	157.099	175.999	194.899	213.799
Y=0.209X + 24.278	45.178	66.078	86.978	107.878	128.778	149.678	170.578	191.478	212.378	233.278
Y=0.18X+27.606	45.606	63.606	81.606	99.606	117.606	135.606	153.606	171.606	189.606	207.606

شکل ۱۰- سربار کنترل دسترسی برای سه سناریوی شبیه‌سازی شده

همان‌طور که مشاهده می‌نمایید، در نمودار بالا به ترتیب از بالا به پایین، معادلات نوشته شده مربوط به سناریوی اول، دوم و سوم می‌باشد. در شکل بالا سربار را به‌صورت زیر برای هر سناریو محاسبه می‌کنیم:

$$Overhead=Y_{SECURE_i} - Y_{WS_i} \quad (۱)$$

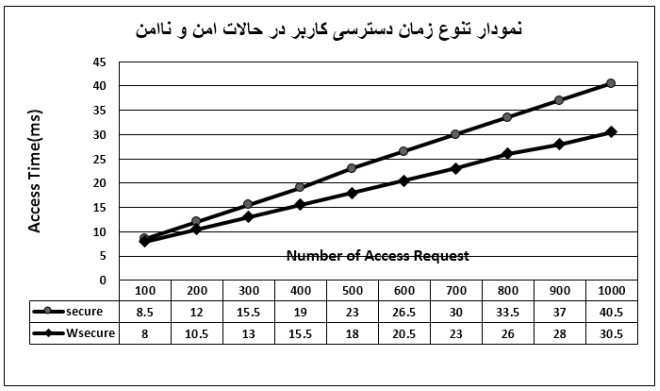
در سناریوی اول برای مثال توجه می‌کنیم که سربار در حدود ۴۳ میلی‌ثانیه برای ۱۰۰ درخواست دسترسی ۱۱۹ میلی‌ثانیه برای ۵۰۰ درخواست دسترسی و ۲۱۳ میلی‌ثانیه برای ۱۰۰۰ درخواست دسترسی می‌باشد. میانگین مقدار سربار

برای ده اندازه ثبت شده ۱۲۸,۷۴۹ میلی‌ثانیه است و این اشاره به این مطلب دارد که سربار راه‌حل امن تأثیر چشمگیر و قابل توجهی به‌واسطه‌ی تعداد درخواست‌های دسترسی (با زیاد شدن تعداد درخواست‌ها) ندارد.

در سناریوی سوم، سربار محاسبه شده حدود ۴۵ میلی‌ثانیه برای ۱۰۰ درخواست دسترسی، ۱۱۷ میلی‌ثانیه برای ۵۰۰ درخواست دسترسی ۲۰۷ میلی‌ثانیه برای ۱۰۰۰ درخواست دسترسی می‌باشد.

درصد نرخ رشد سربار بین سناریوی اول و سناریوی سوم برای ۱۰۰ درخواست برابر ۴,۳۶۳٪ و این در حالی است که این مقدار برای ۱۰۰۰ درخواست دسترسی به ۲,۸۹۶٪ کاهش می‌یابد.

شکل زیر منحنی تنوع زمان دسترسی کاربران، در ۳ سناریوی شبیه‌سازی شده را نشان می‌دهد. برای هر مقدار از دامنه درخواست دسترسی از ۱۰۰ تا ۱۰۰۰، میانگین سربار را محاسبه می‌کنیم.



	100	200	300	400	500	600	700	800	900	1000
secure	8.5	12	15.5	19	23	26.5	30	33.5	37	40.5
Wsecure	8	10.5	13	15.5	18	20.5	23	26	28	30.5

شکل ۱۱- تنوع زمان دسترسی کاربران

این مقدار حدود ۸,۵ میلی‌ثانیه برای صد درخواست و به ۴۰,۵ میلی‌ثانیه برای ۱۰۰۰ درخواست، افزایش می‌یابد. می‌توان این اختلاف را با مقدار زمانی که سیستم برای ایجاد لیست‌های کنترل جدید و بلیت‌های مجوز و انجام عملیات رمزنگاری ضروری، توجیه کرد.

شکل منحنی راه‌حل امن، مقیاس‌پذیری معماری از نظر زمان دسترسی را نشان می‌دهد. افزایش کوچک زمان دسترسی و سربار در طول سناریو در نظر گرفته شده نشان می‌دهد که کشسانی (قابلیت ارتجاع) معماری فدراسیون ابری (اینجا منظور ۳ سناریوی ارائه شده در فدراسیون ابری است) تأثیر چشمگیری روی زمان دسترسی ندارد.

۶- نتیجه‌گیری

پس از تشریح طرح پیشنهادی که یک الگویی برای احراز هویت و مجوزدهی، با استفاده از پروتکل‌های احراز هویت کربروس و ثبت‌نام یکباره برای فدراسیون‌های ابری می‌باشد، ما به انجام آزمایش‌ها، بیان نتایج و تحلیل‌های مربوط به آن‌ها، برای ارزیابی طرح پیشنهاد شده در این پژوهش پرداختیم. نتایج به‌دست آمده بیانگر این موضوع است که طرح پیشنهادی یک راه‌حل عمومی جهت جلوگیری از دسترسی‌های غیرمجاز به منابع فراهم شده در فدراسیون ابری می‌باشد؛ و قابلیت ارتجاع معماری این روش تأثیر قابل توجهی در زمان دسترسی آن ندارد، یعنی با توجه به سناریوهای مختلف که تعداد منابع مشترک و تعداد درخواست‌های دسترسی کاربر در آن‌ها متفاوت است، تأثیر قابل توجهی در زمان دسترسی دیده نمی‌شود؛ و همچنین با به‌کارگیری روش ثبت‌نام یکباره[۶۱] در فدراسیون ابری که با خصوصیات متنوعی که ارائه می‌دهد، نیازمندی‌های کنترل دسترسی فدراسیون ابری را برآورده می‌کند؛ و نیز سربار ناشی از این روش برای کل سیستم در حدی است که کاملاً قابل قبول می‌باشد. برخلاف رویکردهای ارائه شده در بخش کارهای گذشته، در این طرح، یک پشتیبانی سراسری به نام ارائه‌دهنده سرویس فدراسیون برای به دست آوردن منابع (سرویس‌ها) وجود داردکه سرویس‌های ارائه شده از ارائه‌دهندگان متعدد در آن ثبت شده و کاربران و مشتریان برای دریافت سرویس به‌جای مراجعه مستقیم به ارائه‌دهنده سرویس، به ارائه‌دهنده سرویس فدراسیون مراجعه می‌کنند؛ و همچنین مسئولیت مدیریت هویت به یک نهاد منفرد، محول گردیده است و کلیه ویژگی‌های کاربر توسط این نهاد نگهداری می‌گردد و به‌واسطه این کار، بسیاری از هزینه‌های نگهداری که قبلاً ارائه‌دهنده‌ها متحمل آن می‌شدند برداشته می‌شود؛ و اگر بنا بر حسابرسی مشتریان باشد، طرح پیشنهادی برای پیاده‌سازی این کار راحت‌تر است.

مراجع

[1] D. G. Kogias, M. G. Xevgenis, and C. Z. Patrikakis, "Cloud Federation and the Evolution of Cloud Computing," *Computer*, vol. 49, pp. 96-99, 2016.

[2] E. Samlinson, and M. Usha, "User-centric trust based identity as a service for federated cloud environment," in *Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on*, 2013, pp. 1-5.

[3] s. r. pakizeh, "simulation of cloud computing," 2013 ed: pardise danesh, 2013, p. 290.

[4] M. S. J. M. K.Akbari, *cloud computing*: Amirkabir University of Technology, 2011.

[5] E. N. Farrokhi, *cloud computing and simulation methods*: Computer science, 2016.

[6] M. R. Assis, and L. F. Bittencourt, "A survey on cloud federation architectures: Identifying functional and non-functional properties," *Journal of Network and Computer Applications*, vol. 72, pp. 51-71, 2016.

[7] A. N. Toosi, R. N. Calheiros, and R. Buyya, "Interconnected cloud computing environments: Challenges, taxonomy, and survey," *ACM Computing Surveys (CSUR)*, vol. 47, p. 7, 2014.

[8] B. Di Martino, G. Cretella, A. Esposito, A. Willner, A. Alloush, D. Bernstein, D. Vij, and J. Weinman, "Towards an ontology-based intercloud resource catalogue-the ieee p2302 intercloud approach for a semantic resource exchange," in Cloud Engineering (IC2E), 2015 IEEE International Conference on. IEEE, 2015, pp. 458-464.

[9] G. Zangara, D. Terrana, P. P. Corso, M. Ughetti, and G. Montalbano, "A Cloud Federation Architecture," in *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015 10th International Conference on*, 2015, pp. 498-503.

[10] M. Henning, "The rise and fall of CORBA," *Queue*, vol. 4, pp. 28-34, 2006.

"Cloud federation in a layered service model," Journal of Computer and System Sciences, vol. 78, no. 5, pp. 1330-1344, 2012.

[25] M. Coppola, P. Dazzi, A. Lazouski, F. Martinelli, P. Mori, J. Jensen, I. Johnson, and P. Kershaw, "The contrail approach to cloud federations," in The International Symposium on Grids and Clouds (ISGC) 2012, vol. 153, SISSA Medialab, 2012, p. 019.

[26] E. Carlini, M. Coppola, P. Dazzi, L. Ricci, and G. Righetti, "Cloud federations in contrail," in *European Conference on Parallel Processing*, 2011, pp. 159-168.

[27] H. H. d. P. M .Costa, A. P. F. de Araújo, J. J. C. Gondim, M. T. de Holanda, and M. E. M. T. Walter, "Attribute based access control in federated clouds: A case study in bionformatics," in *Information Systems and Technologies (CISTI), 2017 12th Iberian Conference on*, 2017, pp. 1-7.

[28] V. Echeverria, L. M. Liebrock, and D. Shin, "Permission management system: Permission as a service in cloud computing," in *Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual*, 2010, pp. 371-375.

[29] D. Shin and H. Akkan, "Domain-based virtualized resource management in cloud computing," in *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on*, 2010, pp. 1-6.

[30] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the intercloud-protocols and formats for cloud computing interoperability," in *Internet and Web Applications and Services, 2009. ICIW'09. Fourth International Conference on*, 2009, pp. 328-336.

[31] D. Bernstein, and D. Vij, "Intercloud directory and exchange protocol detail using XMPP and RDF," in *Services (SERVICES-1), 2010 6th World Congress on*, 2010, pp. 431-438.

[32] V. Suhendra, "A survey on access control deployment," *Security Technology* , pp. 11-20, 2011.

[33] Q. Wang, and H. Jin, "Quantified risk-adaptive access control for patient privacy protection in health information systems," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, 2011, pp. 406-410.

[34] P. Arias-Cabarcos, F. Almenárez-Mendoza, A. Marín-López, D. Díaz-Sánchez, and R. Sánchez-Guerrero, "A metric-based approach to assess risk for "on cloud" federated identity management," *Journal of Network and Systems Management*, vol. 20, pp. 513-533, 2012.

[35] D. R. dos Santos, C. M. Westphall, and C. B. Westphall, "Risk-based dynamic access control for a highly scalable cloud federation," in *7th International Conference on*

[11] R. Ranjan, and R. Buyya, "Decentralized overlay for federation of enterprise clouds," *Handbook of Research on Scalable Computing Technologies*, vol. 191, 2009.

[12] A. H. Rabia Latif, A. Saïd, and A. Qasim, "Cloud Computing Risk Assessment: A Systematic Literature Review," 2014.

[13] D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire, and P. R. Inácio, "Security issues in cloudenvironments: a survey," *International Journal of Information Security*, vol. 13, pp. 113-170, 2014.

[14] H. Eken, "Security threats and solutions in cloud computing," in *Internet Security (WorldCIS), 2013 World Congress on*, 2013, pp. 139-143.

[15] W. Stallings, *network Security Essentials applications and standards*: Science of iran, 2017.

[16] V. C. Hu, D. Ferraiolo, and D. R. Kuhn, *Assessment of access control systems*: US Department of Commerce, National Institute of Standards and Technology, 2006.

[17] A. R. Khan, "Access control in cloud computing environment," *ARPN Journal of Engineering and Applied Sciences*, vol. 7, pp. 613-615, 2012.

[18] B. Farroha, and D. Farroha, "Challenges of "operationalizing" dynamic system access control: Transitioning from ABAC to RAdAC," in *Systems Conference (SysCon), 2012 IEEE International*, 2012, pp. 1-7.

[19] R. Buyya, R. Ranjan, and R. N. Calheiros, "Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services," in *International Conference on Algorithms and Architectures for Parallel Processing*, 2010, pp. 13-31.

[20] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "Three-phase cross-cloud federation model: The cloud sso authentication," *in Advances in Future Internet (AFIN), 2010 second international conference on*, 2010, pp. 94-101.

[21] B. Rochwerger, D. Breitgand, E. Levy, A. Galis, K. Nagin, I. M. Llorente, R. Montero, Y. Wolfsthal, E. Elmroth, J. Caceres, and et. al., "The reservoir model and architecture for open federated cloud computing," IBM Journal of Research and Development, vol. 53, no. 4, pp. 4-1, 2009.

[22] B. Rochwerger, D. Breitgand, A. Epstein, D. Hadas, I. Loy, K. Nagin, J. Tordsson, C. Ragusa, M. Villari, S. Clayman, and et. al., "Reservoir-when one cloud is not enough," Computer, vol. 44, no. 3, pp. 44-51, 2011.

[23] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How to enhance cloud architectures to enable cross-federation," in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, 2010, pp. 337-345.

[24] D. Villegas, N. Bobroff, I. Rodero, J. Delgado, Y. Liu, A. Devarakonda, L. Fong, S. M. Sadjadi, and M. Parashar,

[1]Cloud Computing
[2]Beneficial
[3]Cloud Federation
[4]NIST
[5]Infrastructure As a Service
[6]Platform As a Service
[7]Software As a Service
[8]NIST
[9]Cloud Federation
[10]Lock-In
[11]Intercloud
[12]Quality of Service
[13]Hybrid Cloud
[14]Sky Computing
[15]Multi-Cloud Tournament
[16]Interface
[17]Brokerage
[18]Common Object Request Broker Architecture
[19]Object Request Broker
[20]Broker
[21]Security Threats
[22]IT
[23]Information Theft
[24]Account
[25]API
[26]Denial of Service
[27]Multi Tenancy
[28]Data Transfer
[29]Technical Risk
[30]Physical Security
[31]Separation of Information
[32]Data Recovery
[33]Access Control
[34]Data Security and Privacy
[35]Access Control
[36]Subject / Factor
[37]Object / Resource
[38]Action
[39]Credential
[40]Deny
[41]Attribute Based Access Control
[42]Permission as a Service
[43]Virtual Execution Platform
[44]Usage Controlaccess Control Model
[45]Gateway
[46]Identity Islands
[47]Learning Automata
[48]Authentication and Authorisation
[49]Username and Password
[50]Log in
[51]Federation Service Provider
[52]Ticket Granting Server
[53]Authentication Server
[54]Authenticator
[55]Service Provider
[56]Federate Ticket
[57]Access Control List
[58]Cloudsim
[59]Java Code-Free Source
[60]Overhead
[61]Single Sing-On

Emerging Security Information Systems and Technologies, 2013, pp. 8-13.

[36] B. S. Taheri, M. G. Arani, and M. Maeen, "ACCFLA: Access Control in Cloud Federation using Learning Automata," *International Journal of Computer Applications*, vol. 107, 2014.

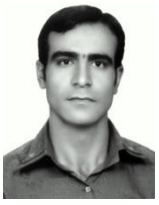
[37] R. Buyya, R. Ranjan, and R. N. Calheiros, "Modeling and simulation ofscalable Cloud computing environments and the CloudSim toolkit: Challenges and opportunities," *in High Performance Computing & Simulation, 2009. HPCS'09. International Conference on*, 2009, pp. 1-11.

[38] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. DeRose, and R. Buyya, "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," *Software: Practice and experience*, vol. 41, pp. 23-50, 2011.

[39] (2017) *http://gwa.ewi.tudelft.nl./*

محمد بهارلو وی دوره کارشناسی رشته کامپیوتر گرایش سخت‌افزار، را دانشگاه شهید باهنر کرمان در سال ۸۵ به اتمام رساند و طی سال‌های ۸۷-۸۵ در دانشگاه صنعتی شریف، در مقطع کارشناسی‌ارشد مشغول به تحصیل شد و هم‌اکنون نیز دانشجوی مقطع دکتری در دانشگاه تهران می‌باشد.

آدرس پست‌الکترونیکی ایشان عبارت است از:
m.baharloo@ut.ac.ir, m.baharloo@ipm.ir



مهدی افشارمنش وی دوره کارشناسی رشته کامپیوتر گرایش فناوری اطلاعات را، در دانشگاه پیام نور ملایر در سال‌های ۸۶-۹۱ گذراند و دوره کارشناسی‌ارشد رشته شبکه‌های کامپیوتری را طی سال‌های ۹۶-۹۴ در دانشگاه صنعتی پویش قم گذرانده است.

آدرس پست‌الکترونیکی ایشان عبارت است از:
e.mehdi.afshar@gmail.com

ثارالله کشاورز للکامی وی دوره کارشناسی رشته کامپیوتر گرایش سخت‌افزار را در دانشگاه شهید باهنر کرمان و دوره کارشناسی‌ارشد رشته معماری کامپیوتر را در دانشگاه آزاد قزوین گذرانده است.

آدرس پست‌الکترونیکی ایشان عبارت است از:
keshavarz458@gmail.com

اطلاعات بررسی مقاله:

تاریخ ارسال: ۱۳۹۶/۰۷/۰۷
تاریخ اصلاح: ۱۳۹۶/۱۱/۲۰
تاریخ قبول شدن: ۱۳۹۷/۰۲/۰۱
نویسنده مرتبط: مهدی افشارمنش، دانشکده مهندسی کامپیوتر، موسسه آموزش عالی پویش، قم، ایران.

The CSI Journal on
Computing Science and
Information Technology
Vol. 16, No. 1, 2018

Single Sign-on Access Control System Based on Kerberos in Cloud Federation

Mohammad Baharloo[1] **Mehdi Aafsharmanesh**[2] **Sarallah Keshavarz Lelkami**[3]

[1]School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran
[2]Faculty of Computer Engineering, Pooyesh Institute of higher education, Qom, Iran
[3]Faculty of Computer Engineering, Qazvin branch, Islamic Azad University, Qazvin, Iran

ABSTRACT

Cloud computing is designed to revolutionize resource and service management. This technology is constantly evolving by providing attractive solutions and services to businesses and consumers. Cloud computing is a promising paradigm for delivering computing as services. Cloud computing providers have a lot of distributed resources around the world, however, sometimes these resources are not enough to satisfy customers, so a concept called the cloud federation has been developed to extend this technology. The cloud federation gives providers the opportunity to share their resources to meet customer demands that a single cloud could not meet those demands on its own. One of the important issues that exist in a federation environment is managing users and authenticating them in the cloud federation. In this article, we focus on controlling access to resources in a cloud federation. The proposed solution is a single sign-on system based on the Kerberos authentication protocol. The evaluations using the cloud sim simulator show that in the proposed method the access time to the shared cloud resources in different scenarios is limited. Also, in the proposed approach, the elasticity of cloud resources has not significantly affected the access time to resources. Hence, the overhead due to the proposed security mechanism in the cloud federation is tolerable.

Keywords: Cloud Computing, Cloud Federation, Access Control, Kerberos, Single Sign-on.