دانشکده مهندسی کامپیوتر و فناوری اطلاعات

بهبود برقراری امنیت اطلاعات در رایانش ابری با استفاده از استاندارد SAML

پایان‌نامه کارشناسی ارشد مهندسی فناوری اطلاعات گرایش مدیریت سیستمهای اطلاعاتی

فهرست مطالب

فصل چهارم: ورودتکی با استفاده از زبان نشانه‌گذاری اثبات امنیت

فصل پنجم: بررسی مدل پیشنهادی و نتیجه‌گیری

فهرست شکل‌ها

عنوان **صفحه**

فهرست جداول

عنوان سیزده **صفحه**

چکیده

دنیای اینترنت و کامپیوتر هر روز در حال پیچیده‌تر شدن و تکامل است. یکی از محصولات این تکامل، رایانش ابری است. با توجه به این موضوع، حساسیت داده‌ها و حفظ حریم خصوصی اطلاعات به طور جدی به عنوان یک نگرانی مهم برای سازمان‌ها تبدیل می‌شود. شرکت‌ها برای ارائه خدمات تخصصی مبتنی بر وب، توجه ویژه‌ای به ارائه دهندگان خدمات نرم افزار (ASPها) یا فروشندگان نرم افزار به عنوان سرویس (SaaS) دارند که باعث کاهش هزینه‌ها و ارائه برنامه‌های کاربردی خاص و متمرکز به کاربران می‌شود. این روش پیچیدگی طراحی، نصب، پیکربندی، گسترش و پشتیبانی از سیستم توسط منابع داخلی را حذف می‌کند که منافع زیادی به سازمان‌ها ارائه‌می‌دهد.

سازمان‌ها اخیراً از منابع احراز هویت مرکزی برای برنامه‌های کاربردی داخلی و پورتال‌های مبتنی بر وب برای بیشتر قسمت‌های خود استفاده می‌کنند. احراز هویت ورود تکی، هنگامی‌که به درستی پیکربندی شده‌باشد باعث ایجاد یک امنیت قوی می‌شود به این معنا که کاربران، نیاز به یادداشت و به‌خاطر سپردن کلمات عبور سیستم‌های مختلف ندارند. همچنین باعث سهولت مدیریت و حسابرسی کاربران می‌شود. با استفاده از یک استاندارد برای احراز هویت اطلاعات برای مبادله روی اینترنت می‌توان این مشکل را حل کرد. زبان نشانه‌گذاری اثبات امنیت، یک راه حل مبتنی بر XML و امن برای تبادل اطلاعات کاربر بین ارائه‌دهنده شناسه (سازمان) و ارائه‌دهنده سرویس (ASPها یا SaaSها) فراهم می‌کند. استاندارد زبان نشانه‌گذاری اثبات امنیت، قوانین و دستورات نحوی را برای تبادل اطلاعات تعریف می‌کند، در عین حال انعطاف پذیر است و اجازه انتقال داده‌های سفارشی به ارائه‌دهنده سرویس خارجی را می‌دهد.

در این پایان‌نامه سعی گردیده است که از مزایای رایانش ابری و ورود تکی بهترین استفاده برده شود و از آن برای ارتقا سیستم‌های ورود تکی و به طور خاص برای ورود تکی با استفاده از استاندارد زبان نشانه‌گذاری اثبات امنیت استفاده‌شود. برای این منظور ابتدا مفاهیم و تعاریف اولیه مرتبط از جمله رایانش ابری، زبان نشانه‌گذاری اثبات امنیت، احراز هویت و ورود تکی مورد مطالعه قرارگرفته‌اند. سپس بررسی کوتاهی در مورد روش‌های احراز هویت انجام گردیده‌است تا با استفاده از آن مدلی بهتر، کامل‌تر و متناسب با آنچه مورد نیاز است، ارائه گردد. همچنین تعدادی از مدل‌های ارائه شده برای هر یک از مباحث بالا و ترکیب این مباحث مورد بررسی قرارگرفته است. با ترکیب و جمع‌بندی روش‌ها و اطلاعات بدست‌آمده، مدلی برای ورود تکی مبتنی بر رایانش ابری با استفاده از زبان نشانه‌گذاری اثبات امنیت به منظور کمک به فرایند ورود تکی در احراز هویت کاربران، پیشنهاد و شبیه‌سازی گردیده است. در نهایت پس از بیان مزایای مدل پیشنهادی، مشکلات احتمالی بررسی شده و برای رفع این مشکلات و همچنین مطالعات آینده پیشنهاداتی ارائه گردیده است.

کلید واژه‌ها:

به فارسی:

امنیت اطلاعات در رایانش ابری، زبان نشانه‌گذاری اثبات امنیت در رایانش ابری

به لاتین:

Information security in cloud computing, SAML in cloud computing

فصل اول
مقدمه

۱-۱مقدمه

دنیای فناوری اطلاعات روز به روز در حال گسترش است. از زمانی که رایانه‌ها وارد زندگی بشر شدند، حدود ۷۲ سال می‌گذرد. در طول این سال‌ها عطش پیشرفت باعث به وجود آمدن فناوری‌های جدید شده‌است. همچنین از زمانی که اینترنت در اختیار کاربران قرار گرفته‌است، مدت زیادی نمی‌گذرد. اینترنت تحولی شگرف در تبادل اطلاعات به وجود آورده است. البته در آن زمان کسی به این فکر نمی‌کرد که روزی از اینترنت علاوه بر تبادل اطلاعات بتوان به عنوان یک سیستم پردازشی قوی استفاده کرد. اما امروزه بسیاری از پردازش‌ها توسط سرورها انجام‌می‌شود. مفاهیم ابتدایی محاسبات ابری از دهه‌ی ۱۱۶۲ میلادی گسترش یافت. اما محاسبات ابری به صورتی که در حال حاضر آنرا می‌شناسیم و در اختیار همگان قرارگرفته از سال ۲۲۲۶ توسط سایت آمازون بکار گرفته شده‌است. محاسبات ابری یک ایده‌ی قدیمی از منابع محاسباتی است که به عنوان یک ابزار استفاده‌شده‌است. محاسبات ابری یک محاسبه‌ی مبتنی بر اینترنت است که منابع مشترک، نرم‌افزار و اطلاعات، برای کامپیوترها و وسایل مورد تقاضا ارائه‌می‌دهد. محاسبات ابری به افراد اجازه می‌دهد که منابع و خدمات توزیع‌شده را به اشتراک بگذارند. بنابراین محاسبات ابری از منابع توزیع‌شده در محیط باز استفاده می‌کند. در نتیجه برای اشتراک داده در توسعه‌ی برنامه‌های محاسبات ابری، امنیت و اطمینان فراهم می‌کند.

حساسیت داده‌ها و حفظ حریم خصوصی اطلاعات به‌طور افزایشی به یک ناحیه نگرانی برای سازمان‌ها تبدیل می‌شود. جنبه‌های احراز هویت و اثبات هویت شامل استفاده، نگهداری و حفاظت از اطلاعات جمع‌آوری‌شده برای کاربران می‌باشد. جلوگیری از دسترسی غیرمجاز به منابع اطلاعات در ابر نیز یک عامل مهم است. همان‌طور که خدمات وب شایع‌تر می‌شوند، کسب‌وکار به دنبال ارائه خدمات ترکیبی به مشتریانی که آنها را به اشتراک می‌گذارند می‌باشد. این فرایند برای مشتریانی که باید نام‌های کاربری و کلمه‌های عبور مختلف را به‌خاطر داشته‌باشند و رزروهای مختلف روی بخش‌های مرورگرهای وب مختلف را با واسط‌های کاربری غیرواحد نشان‌دهنده‌ی وضعیت‌های رزرو مختلف نگهداری کنند مسئولیت دشواری است [۱، ۲ و ۳].

زبان نشانه‌گذاری اثبات امنیت[۱] استانداری برای ورود تکی کاربران به وب به صورت امن است که اولین بار در ژانویه سال ۲۰۰۱ توسط سازمان گسترش استانداردهای اطلاعات ساختاریافته معرفی شد و یک چارچوب مبتنی بر زبان نشانه‌گذاری توسعه‌پذیر برای تبادل اطلاعات احراز هویت و تصدیق و امنیت تبادل اطلاعات بکار گرفته شده‌بود. آخرین به‌روزرسانی آن در سال ۲۰۰۵ بوده‌است. زبان نشانه‌گذاری اثبات امنیت در چند نسخه وارد بازار جهانی اینترنت شد. اولین نسخه زبان نشانه‌گذاری اثبات امنیت تحت عنوان SAML1 عرضه شد. سپس نسخه SAML1.1 آن ارائه شد که از نظر کارایی مگر جز تفاوت های کوچک، کاملاً مشابه SAML1 بود. در نهایت آخرین نسخه زبان نشانه‌گذاری اثبات امنیت که SAML2 نام گرفت در سال ۲۰۰۵ عرضه گردید تفاوت های اساسی با نسخه‌های قبلی این استاندارد داشت [۴].

---

[۱] Security Assertion Markup Language

اگرچه هر دو نسخه‌ی این استاندارد بر موارد استفاده یکسانی نظارت می‌کردند، SAML2 با نسخه‌های قبلی خود ناسازگار است. نسخه‌های اولیه زبان نشانه‌گذاری اثبات امنیت هیچ پروتکل خاص دیگری را در پرس‌وجوهای خود پشتیبانی نمی‌کند در حالی که نسخه نهایی زبان نشانه‌گذاری اثبات امنیت (SAML2) از پروتکل‌های زیادی پشتیبانی می‌کند که اکثر پروتکل‌ها کاملاً جدید هستند. هم SAML1 و هم SAML2 از امضاهای دیجیتال (مبتنی بر استاندارد امضای XML) برای احراز هویت و یکپارچگی پیام‌ها استفاده‌می‌کنند. با استفاده از رمزگذاری XML، SAML2 عناصری برای تعیین‌کنندگان هویت‌نام رمزگذاری شده، ویژگی‌های رمزگذاری شده و اثبات‌های رمزگذاری شده (SAML1 قابلیت رمزگذاری ندارد) فراهم‌می‌کند [۵].

مهمترین چیزی که آدرس‌های زبان نشانه‌گذاری اثبات امنیت نیاز دارند، ورود تکی مرورگر وب است. راه حل‌های ورود تکی معمولاً در سطح اینترانت (برای مثال با استفاده از کوکی‌ها) است اما توسعه این راه حل‌ها ورای اینترانت مشکل‌زا می‌شود و منجر به گسترش تکنولوژی‌های اختصاصی غیرقابل همکاری می‌شود. زبان نشانه‌گذاری اثبات امنیت قصد حل این نواقصی را دارد که توسط سازمان گسترش استانداردهای اطلاعات ساختاریافته توسعه یافته است. زبان نشانه‌گذاری اثبات امنیت با ارائه یک چارچوب مبتنی بر زبان نشانه‌گذاری توسعه‌یافته قصد حل مشکل تبادل اطلاعات امن را دارد. مهمترین مزیت زبان نشانه‌گذاری اثبات امنیت، گسترش آن و رشد اختیاری آن در صنعت است. این معمولاً بین سازمان‌ها و مشتریان آنها، شریکان کسب‌وکار و ارائه‌دهندگان ابر استفاده می‌شود. زبان نشانه‌گذاری اثبات امنیت از امنیت سطح اثبات، مقیاس‌پذیری و قابلیت اطمینان در هزاران محصول توسعه‌یافته جهانی برخوردار است.

اثبات‌های زبان نشانه‌گذاری اثبات امنیت در امنیت سرویس‌های وب برای امنیت پیام‌های سرویس‌های وب نیز مورد استفاده قرار می‌گیرند. امنیت سرویس‌های وب با استفاده از اثبات‌های زبان نشانه‌گذاری اثبات امنیت در قالب یک توکن امنیتی با پروفایل توکن زبان نشانه‌گذاری اثبات امنیت امنیت سرویس‌های وب را تعریف می‌کند. سرویس‌های وب امنیتی مجموعه‌ای از مشخصات است که ابزارهایی برای تامین حفاظت از امنیت پیام‌ها تعریف می‌کند. زبان نشانه‌گذاری اثبات امنیت از تعدادی اجزای بلوک ساختمان تشکیل شده‌است که هنگامی‌که به هم متصل می‌شوند، اجازه پشتیبانی تعدادی از موارد استفاده می‌دهد. مشخصات زبان نشانه‌گذاری اثبات امنیت، ساختار و محتوای اثبات‌ها که توضیحاتی در مورد یک اصل اثبات شده توسط یک بخش اثبات می‌دهد را تعریف می‌کند [۴ و ۶].

۲-۱ تعریف مسئله

محاسبات ابری از این ایده استفاده‌می‌کند که کار انجام‌شده در سمت سرویس‌گیرنده می‌تواند به برخی از خوشه‌های نامرئی منابع در اینترنت حرکت کند [۱]. محاسبات ابری، بسترهای مجازی‌سازی با منابع ارتجاعی همراه با ارائه‌ی مبتنی بر تقاضای سخت‌افزار، نرم‌افزار و مجموعه داده را به صورت پویا بکار می‌گیرد [۲، ۳]. محاسبات ابر به هزینه کم آن و سادگی، هم برای ارائه‌دهندگان و هم برای کاربران متکی است [۷، ۸]. اما اینترنت مکانی نیست که ارائه‌دهندگان کنترل کاملی روی آن داشته‌باشند. به دلیل نگرانی‌های امنیتی، محاسبات ابر به برخی از کاربران مربوط نمی‌باشد. به عنوان یک محیط مجازی، محاسبات ابری تهدیدات امنیتی خاص خود را دارد و این تهدیدات کاملا متفاوت از تهدیدات در سیستم‌های فیزیکی است. در این مقاله برخی از نگرانی‌های امنیتی در محاسبات ابری خصوصاً در امنیت داده‌ها بررسی می‌شوند.

بخش بازنگری شده به شرح زیر است: در بخش ۲، مدل‌های سرویس ابر و نگرانی‌های امنیتی آن بررسی می‌شود. بخش ۳ به بررسی مدل‌های امنیت اطلاعات می‌پردازد. سپس در بخش ۴، مدل امنیتی اطلاعات جدیدی برای محاسبات ابر ارائه‌شده است و در نهایت در بخش ۵، کارهای آینده و نتایج مورد بحث قرار گرفته‌است. امروزه محاسبات ابری توجه زیادی را به خود جلب

کرده‌است. رسانه و همچنین تحلیلگران در مورد فرصت‌هایی که محاسبات ابری پیشنهاد می‌دهد بسیار مثبت هستند. در ماه می سال ۲۰۰۸، مریل لینچ[۱]مزایای هزینه‌ای محاسبات ابری را ۳ تا ۵ برابر برنامه‌های‌کاربردی تجاری و بیش از ۵ برابر برنامه‌های‌کاربردی مصرف‌کننده تخمین زده‌است. طبق انتشارات گارتنر[۲] در ماه جون سال ۲۰۰۸، قدرت و نفوذ محاسبات ابری کمتر از تجارت الکترونیکی نیست.

گرایش مثبت به سمت اهمیت و تاثیر محاسبات ابری که نتیجه پیش‌بینی‌های مرتبط به بازار ابری است، خوش‌بین می‌باشد. در اکتبر سال ۲۰۰۸، IDC، پیش‌بینی کرد تا سال ۲۰۱۲ زمان صرف‌شده روی سرویس‌های ابری رشدی تقریبا سه برابر خواهد داشت که نتیجه آن رسیدن به ۴۲ میلیارد دلار می‌باشد. همین شرکت تحلیلگر گزارش داد که سود هزینه مربوط به مدل ابری حتی در رکود اقتصادی جذاب‌تر خواهدشد. چشم‌انداز مثبت بازار نیز با انتظار اینکه محاسبات ابری ممکن‌است رویکرد اساسی‌ای به سوی فناوری‌اطلاعات سبز شود، رانده شده است. با وجود پوشش گسترده محاسبات ابری در مطبوعات تجاری، هنوز هیچ توافق عمومی‌ای در مورد اینکه محاسبات ابری واقعاً چیست و چگونه به محاسبات گرید مربوط می‌گردد وجود ندارد. برای بدست‌آوردن درک درستی از آنچه که محاسبات ابری است، در ابتدا نگاهی به چند تعریف موجود از این اصطلاحات پرداخته‌می‌شود. براساس این تعاریف، مشخصات کلیدی محاسبات ابری شناسایی می‌شود [۹]. سپس معماری رایج و مولفه‌های ابرها به‌طور مفصل بررسی می‌شوند، در مورد فرصت‌ها و چالش‌های محاسبات ابری بحث و یک دسته بندی از ابرها ارائه می‌شود.

۳-۱ تبیین صورت مسئله

با توجه به مطالب ذکر شده در مقدمه، در این پایان‌نامه مباحث مرتبط با محاسبات ابری و انواع آن، چالش‌ها و فرصت‌های محاسبات ابری، امنیت محاسبات ابری، روش‌ها و استانداردهای ورود تکی، زبان نشانه‌گذاری اثبات امنیت و کاربردهای آن در سرویس‌های وب مورد مطالعه قرارگرفته و مزایا و معایب آن مشخص شده‌است. همچنین مدل‌های مختلف مربوط به ورود تکی بررسی شده و از ایده‌های داده‌شده در آنها به منظور بهبود زبان نشانه‌گذاری اثبات امنیت برای ورود تکی امن‌تر استفاده گردید. با توجه به اینکه روش‌های ورود تکی سنتی معایب و مشکلات زیادی از جمله هزینه‌های زیاد، مشکل به‌خاطر سپردن نام‌های‌کاربری و رمز عبور، استفاده از این نام‌های‌کاربری و رمز عبورهای متعدد در هر بار استفاده از خدمات وب و هدر رفتن زمان را به همراه دارد، در این پایان‌نامه تلاش شده‌است مدلی برای بهبود استفاده کاربر از خدمات و سرویس‌های وب مبتنی بر اینترنت با استفاده از زبان نشانه‌گذاری اثبات امنیت در محاسبات ابری ارائه گردد.

٤-۱ ساختار پایان‌نامه

در فصل اول این پایان‌نامه پس از بیان مقدمه‌ای بر موضوع، مسئله‌ای که قرار است روی آن کار شود بیان شده‌است. در فصل دوم به مفاهیم و تعاریف اولیه، مزایا و معایب هر یک از مباحث مرتبط، از جمله محاسبات ابری، انواع آن، مدل‌های آن، چالش‌ها و فرصت‌ها، سطوح دسترسی و میزان اختیارات و عوامل مربوط به احراز هویت و تصدیق پرداخته شده‌است. همچنین استاندارد زبان نشانه‌گذاری اثبات امنیت و اجزای آن، زبان نشانه‌گذاری اثبات امنیت در امنیت سرویس‌های وب و حالت‌های استفاده از آن، استفاده از توکن زبان نشانه‌گذاری اثبات امنیت در سرویس‌های وب به صورت مفصل بیان شده‌اند. همچنین بررسی مختصری در مورد احراز هویت ورود تکی به وب با استفاده از زبان نشانه‌گذاری اثبات امنیت ارائه داد. در فصل سوم چند سیستم ورود کی به‌طور مختصر بیان شده است. همچنین تعدادی از مدل‌های ارائه‌شده برای ورود تکی به همراه مزایا و معایب هر کدام به‌طور

---

[۱] Merrill Lynch

[۲] Gartner

اجمالی ارائه گردیده است. در نهایت پروتکل کربروس و فرایند احراز هویت ورود تکی به وب با استفاده از زبان نشانه‌گذاری اثبات امنیت و مزایا و معایب هر کدام به تفصیل آورده شده است تا بتوان با ترکیب و جمع‌بندی روش‌ها و اطلاعات بدست‌آمده از این مدل‌ها، مدلی برای کمک به ورود تکی کاربران و سرویس‌دهی بهتر به آنها ارائه داد. در فصل چهارم با استفاده از تمام اطلاعات و مطالعات انجام‌شده مدلی برای بهبود ارائه خدمات و سرویس‌های وب مبتنی بر اینترنت با استفاده از زبان نشانه‌گذاری اثبات امنیت در محاسبات ابری به کاربر پیشنهاد و سعی در مدل‌سازی آن شده‌است. در نهایت در فصل پنجم مدل مورد بررسی قرار گرفته‌است. برای ارزیابی و بررسی مدل از پرسشنامه استفاده‌شده‌است که نتایج این پرسشنامه با تحلیل‌های آماری در این فصل آورده شده‌است. همچنین مزایای مدل پیشنهادی بیان و مشکلات احتمالی بررسی شده‌اند و برای آنها و همچنین مطالعات آینده پیشنهاداتی ارائه گردیده و نتیجه‌گیری کلی انجام شده‌است.

فصل دوم
محاسبات ابری، چالش‌ها و راهکارها

۲-۱ مقدمه

محاسبات ابری از ایده‌ی منابع محاسباتی به عنوان یک ابزار استفاده کرده است که هزینه‌های زیاد توسعه را کاهش و سرویس جدیدی در اینترنت گسترش می‌دهد. به‌طور کلی، ابر از مجموعه‌ای از سرویس‌ها، برنامه‌های‌کاربردی، اطلاعات و زیرساخت تشکیل شده است که منابع محاسباتی، شبکه، اطلاعات و منابع ذخیره‌سازی را توصیف می‌کند [۱ و ۲]. محاسبات ابری محاسبات مبتنی بر اینترنت است که منابع مشترک، نرم‌افزار و اطلاعات، برای کامپیوترها و وسایل مورد تقاضا ارائه‌می‌دهد. محاسبات ابری به افراد اجازه می‌دهد که منابع و سرویس توزیع‌شده را به اشتراک بگذارند. بنابراین محاسبات‌ابری از منابع توزیع‌شده در محیط باز استفاده می‌کند. در نتیجه برای اشتراک داده در توسعه‌ی برنامه‌های محاسبات ابری، امنیت و اطمینان فراهم می‌کند. محاسبات ابری باعث افزایش نگرانی‌های امنیت، حفظ حریم خصوصی و اطمینان می‌شود که این نگرانی‌ها عبارتند از:

- چگونه داده‌های صحیح توسط ارائه‌دهندگان ابر ذخیره و بکار گرفته می‌شود؟
- چگونه حفظ حریم خصوصی داده‌ها به‌طور مناسبی مدیریت می‌شود؟
- آیا ارائه‌دهندگان ابر با قوانین و دستورالعمل‌ها موافقت می‌کنند؟
- آیا ارائه‌دهندگان ابر در مقابل حملات به‌طور مناسبی محافظت می‌شوند [۳]؟

کنترل‌های امنیتی در محاسبات ابری، در اکثر موارد، هیچ تفاوتی با کنترل‌های امنیتی محیط IT ندارد. به دلیل اینکه مدل‌های سرویس ابری بکارگرفته شده، از مدل‌های عملیاتی و فناوری‌هایی برای فعال کردن سرویس ابر استفاده می‌کنند، محاسبات ابری ممکن‌است خطرات مختلفی برای یک سازمان نسبت به راه حل‌های سنتی IT ارائه دهد [۱]. با افزایش توسعه‌ی محاسبات ابری، حوادث امنیتی متعددی بوجود می‌آید. کاربران ابر می‌توانند از تمرکز تخصص‌های امنیتی در ارائه‌دهندگان ابر بزرگ بهره‌مند شوند، که بهترین روش امنیتی برای کل اکوسیستم را تضمین می‌کند. از سوی دیگر، یک خرابکار می‌تواند بسیاری از کاربران را مختل کند. برای مثال، فرستندگان اسپم، محاسبات ابر ارتجاعی را خراب می‌کنند و باعث اختلالات یک بخش بزرگی از آدرس‌های IP محاسبات ابر می‌شوند [۱۰]. وضعیت قرارگیری امنیت سازمان با بلوغ، اثربخشی و کامل‌بودن کنترل‌های امنیتیِ تعدیلِ خطر پیاده‌سازی شده مشخص می‌شود. این کنترل‌ها در یک یا چند لایه در محدوده‌ای از امکانات (امنیت فیزیکی)، زیرساخت‌های شبکه (امنیت شبکه)، سیستم‌های فناوری اطلاعات (سیستم‌های امنیتی)، رویکردهای اطلاعات و برنامه‌های‌کاربردی (امنیتی نرم‌افزار) پیاده‌سازی شده است [۱].

۲-۲ تاریخچه‌ی محاسبات ابری

مفاهیم ابتدایی محاسبات ابری به دهه‌ی ۱۹۶۰ میلادی برمی‌گردد. این مفهوم که توسط جان مک کارتی[۱] از بنیان‌گذاران هوش مصنوعی ارائه شد، بعدها مورد بررسی بیشتری قرار گرفت. محاسبات ابری به صورتی که در حال حاضر آن را می‌شناسیم و در

---

[۱] John McCarthy

اختیار همگان قرارگرفته، از سال ۲۰۰۶ توسط سایت آمازون انجام‌شده است. این سایت در سال ۲۰۰۶ امکان دسترسی به سیستم خود را از طریق وب سرویس‌های آمازون بر پایه‌ی محاسبات ابری ارائه کرد. وب سرویس‌های آمازون، زیرساخت‌های فناوری اطلاعات را به صورت سرویس‌های انعطاف پذیر به مشتریان ارائه‌می‌دهد که شامل سرویس‌های پردازشی، ذخیره‌سازی، تحویل محتوا، پایگاه‌داده، تجارت الکترونیک، پرداخت و صورتحساب می‌باشد. یک سال بعد در سال ۲۰۰۷، گوگل و آی‌بی‌ام پروژه‌هایی در مقیاس بزرگ در زمینه‌ی محاسبات ابری آغاز کردند [۱۱].

۲-۳ چند نمونه

در این بخش سه سیستم محاسباتی اولیه ارائه می‌شود که ویژگی‌های مشابهی با آنچه امروزه محاسبات ابری نامیده می‌شوند دارند:

۲-۳-۱ مالتیکس[۱]

یک جنبه قابل توجه آن اصول طراحی امنیت آن بود. مالتیکس ابتدا بیشتر از مکانیزم‌های محافظت مبتنی بر دستور نسبت به مبتنی بر اجرا استفاده می‌کرد. در هر دسترسی به شی، اختیارات فعلی بررسی می‌شد. دوم، مالتیکس یک شکل از رهنمودهای کرخوفسک با نگهداری طراحی باز برای مکانیزم‌ها و رمزهای کلیدی آن را شامل می‌شد. سوم، سیستم همیشه در حداقل امتیاز فعالیت می‌کرد. درنهایت، طراحی، به صراحت اهمیت قابلیت استفاده انسان با ازدیاد حملات مهندسی اجتماعی را به رسمیت می‌شناخت. طراحی امنیتی مالتیکس، اهمیت مدیریت سیستم جلوگیری از تنگناهای تصمیم‌گیری را بیان می‌کند. در غیر این صورت، کاربران خواستار گذشتن از مدیریت از طریق عادت و مکانیزم‌های محافظت از سازش هستند. مالتیکس، برای انجام امنیت، یک حالت مطلق ندارد، بلکه اجازه می‌دهد کاربران زیرسیستم‌های محافظت‌شده بسازند. به‌طور مشابه، کاربران مختلف محاسبات ابر، خواستار نیازهای ایمنی مختلفی هستند که یک طراحی خوب می‌تواند سطوح ایمنی و مکانیزم‌های امنیتی را ارائه دهد. ارائه‌دهندگان ابر اولین گام‌ها را با ارائه‌ی نمونه‌ی ابرهای خصوصی مجازی، با منابع اختصاصی و شبکه‌های خصوصی مجازی که جداسازی را تضمین می‌کند آغاز کرده‌اند [۸ و ۱۰].

۲-۳-۲ ناظران ماشین‌های مجازی اولیه[۲]

کار ناظران ماشین‌های مجازی اولیه زیاد است. استدلالی برای امن‌تر بودن ناظران ماشین مجازی از سیستم‌های کامپیوتری معمولی ارائه‌شده است: اول، سطوح پایین‌تر عملکرد چند برنامه‌ای (مثلاً اجرای همزمان) منجر به سطوح پایین‌تر ریسک‌های شکست‌های امنیتی می‌شود. یک سیستم‌عامل تک برنامه‌ای ریسک امنیتی کمتری از یک سیستم‌عامل که چندین برنامه‌ی همزمان را اجرا می‌کند دارد. در نتیجه، ناظران ماشین‌های مجازی با سطوح عملکرد چند برنامه‌ای پایین، امنیت بیشتری از سیستم‌عامل‌های با سطوح عملکرد چندبرنامه‌ای بالا خواهند داشت. دوم، حتی اگر سطح عملکرد چندبرنامه‌ای یکسان باشد، ناظران ماشین‌های مجازی امن‌تر هستند، زیرا برای اشکال‌زدایی ساده‌تر و راحت‌تر هستند. سوم، یک سیستم‌عامل مهمان که روی یک ناظر ماشین مجازی و در چرخه‌ی اجرا روی فلز سخت اجرا می‌شود، تنها زمانی که هر دو سیستم‌عامل مهمان و ناظر ماشین مجازی به‌طور همزمان شکست بخورد نقض امنیتی رخ می‌دهد. در نتیجه یک ناظر ماشین مجازی که در حال اجرای k سیستم‌عامل مهمان و هر سیستم‌عامل در حال اجرای n برنامه است نسبت به یک سیستم‌عامل که n×k برنامه را اجرا می‌کند، به راحتی شکست می‌خورد. چهارم، شکست هر برنامه مستقل است و از این‌رو احتمال شکست به صورت ضرب است. به‌طور کلی هر برنامه‌ی روی یک ناظر ماشین مجازی در

---

[۱] Multics

[۲] Early Virtual Machine Managements

حال اجرای k سیستم‌عامل مهمان، که هریک از سیستم‌عامل‌ها در حال اجرای n برنامه است بسیار کمتر از برنامه‌ی مشابه روی یک سیستم‌عامل با n×k برنامه شکست می‌خورد. این استدلال، سه فرض مهم ایجاد می‌کند. اول، ناظران ماشین‌های مجازی ساده هستند. دوم، سیستم‌عامل‌های مهمان یک سطح عملکرد چند برنامه‌ای پایین‌تری دارند. سوم، ناظران ماشین‌های‌مجازی و سیستم‌عامل‌های مهمان، شکست‌های مستقل دارند. ناظران ماشین‌های مجازی مدرن همه‌ی این سه فرض را زیر سوال می‌برند. امروزه یک سیستم‌عامل مهمان معمولاً سطح مشابهی از عملکرد چندبرنامه‌ای را به عنوان سیستم‌عامل محلی دارد. کاربران با سیستم‌عامل‌های مهمان به روش مشابهی که می‌توانند با یک سیستم‌عامل محلی رفتار کنند، عمل می‌کنند. که فرض اینکه سیستم‌عامل‌های مهمان سطوح عملکرد پایین‌تری دارند را تضعیف می‌کند [۱۲ و ۱۳].

۲-۳-۳ شرکت CSS ملی

بنیانگذاران شرکت، حرکت روبه جلوی هزینه‌ها به هزینه‌های متغیر را پیش‌بینی کردند و شرکت به دلیل انعطاف‌پذیری افزایش‌یافته موفق شد که قابلیت محاسباتی جدا شده‌ی آماده‌ی خود را ارائه‌دهد [۱۴].

۲-٤ مفاهیم

۲-٤-۱ تعریف محاسبات ابری

اصطلاح محاسبات ابری به روش‌های مختلفی توسط شرکت‌های تحلیلگر، دانشگاهیان، شاغلان صنعت و شرکت‌های فناوری‌اطلاعات تعریف شده است. جدول ۲- ۱ توصیف تعدادی از شرکت‌های تحلیلگر محاسبات ابری را نشان می‌دهد.

جدول ۲-۱: تعاریف محاسبات ابری توسط شرکت‌های تحلیلگر منتخب.

منبع	تعریف
Gartner	"سبکی از محاسبات که در آن انبوه قابلیت‌های مرتبط با فناوری‌اطلاعات "به عنوان یک سرویس" با استفاده از فناوری‌های اینترنت به چندین مشتری خارجی ارائه می‌گردد. ".
IDC	"ظهوری از توسعه فناوری‌اطلاعات، مدل استقرار و تحویل، امکان ارائه تحویل محصول به صورت بی‌درنگ، سرویس‌ها و راه حل‌هایی روی اینترنت (به عنوان مثال، امکان ارائه خدمات ابری)".
NIST	"یک مدل برای دسترسی مناسب شبکه‌ی مورد تقاضا به یک مخزن مشترک از منابع محاسباتی پیکربندی‌شده مانند شبکه‌ها، سرورها، حافظه، برنامه‌های‌کاربردی و سرویس می‌باشدکه می‌تواند به سرعت با حداقل تلاش‌های مدیریت یا تعامل ارائه‌دهنده‌ی سرویس، ارائه و منتشر شود [۲ و ۱۵]."
Merrill Lynch	"ایده تحویل شخصی (مانند پست الکترونیکی، پردازشگر کلمه، ارائه‌ها) و برنامه‌های‌کاربردی تولید تجارت (مانند اتوماسیون قسمت فروش، مشتری، سرویس، جواب‌گویی) از سرورهای متمرکز".
گروه ٤٥١	"مدل سرویسی است که یک اصل سازماندهی کلی را برای تحویل مولفه‌های زیرساخت فناوری‌اطلاعات، یک رویکرد معماری و یک مدل اقتصادی را ترکیب می‌کند. اساساً تلاقی محاسبات گرید، مجازی‌سازی، محاسبات ابزاری، میزبانی و نرم‌افزار به عنوان سرویس (SaaS)" .

تمامی این تعاریف مشخصه مشترکی دارند: تمامی آنها تلاش در توصیف و تعریف محاسبات ابری از دیدگاه و نقطه نظر کاربر نهایی را دارند و تمرکز آنها روی این مسئله است که کاربر نهایی ممکن‌است چگونه آن را تجربه کند. طبق این تعاریف، مشخصه‌ی هسته‌ای محاسبات ابری فراهم‌کردن زیرساخت فناوری‌اطلاعات و برنامه‌های‌کاربردی به عنوان سرویس به صورت مقیاس‌پذیر است. تعریف محاسبات ابری حتی در جامعه علمی هم موضوع بحث شده است. همانند مطبوعات تجاری، نظرات مختلف در مورد اینکه محاسبات ابری چیست و چه مشخصه‌های ویژه‌ای دارد، وجود دارد. در مقایسه با تعاریف مطبوعات تجاری،

تعاریف در ادبیات علمی نه تنها شامل دیدگاه کاربر نهایی بلکه به جنبه‌های معماری نیز می‌پردازد. به عنوان مثال، آزمایشگاه برکلی راد محاسبات ابری را اینگونه تعریف می‌کند:

"محاسبات ابری هم به برنامه‌های‌کاربردی تحویل داده‌شده تحت اینترنت به عنوان سرویس اشاره دارد و هم به سخت‌افزار و نرم‌افزار سیستم‌ها در مراکز داده که این سرویس‌ها را فراهم می‌کنند. مدتهاست که به خود سرویس‌ها به عنوان، نرم‌افزار به عنوان سرویس (SaaS) اشاره می‌شود. سخت‌افزار و نرم‌افزار مرکز داده همان چیزی است که آن را یک ابر می‌نامیم. وقتی که این ابر به روش پرداخت هزینه و استفاده در اختیار عموم قرار گیرد، به آن ابر عمومی گویند. سرویس فروخته‌شده محاسبات ابزاری است. واژه ابر خصوصی به مراکز داده درونی یک تجارت یا دیگر سازمان‌ها اشاره دارد که در اختیار عموم نیست. بنابراین، محاسبات ابری مجموع SaaS و محاسبات ابزاری است اما شامل ابرهای خصوصی نیست. افراد می‌توانند کابران و فراهم‌کنندگان SaaS و یا کاربران و فراهم‌کنندگان محاسبات ابزاری باشند."

این تعریف دیدگاه‌های متفاوت روی کلید را با هم آورده‌است: از دیدگاه فراهم‌کننده، مولفه اصلی ابر، مرکز داده‌است. مرکز داده شامل منابع سخت‌افزاری خام برای محاسبات و ذخیره‌سازی است، که به همراه نرم‌افزار به "صورت پرداخت هزینه و استفاده" ارائه می‌شوند. از دیدگاه هدفشان، ابرها به دو دسته خصوصی و عمومی تقسیم می‌شوند. مستقل از هدف ابرها، مهمترین هدف ابرها یکپارچه‌سازی سخت‌افزار و نرم‌افزارهای سیستم با برنامه‌های‌کاربردی می‌باشد، یعنی یکپارچه‌سازی محاسبات ابزاری و SaaS. همچنین Reese بیان می‌دارد که یک ابر می‌تواند هم نرم‌افزار و هم زیرساخت باشد و چگونگی مصرف سرویس‌های ابری را خاطر نشان کرده‌است: "سرویس وب از طریق مرورگر وب (به‌طور غیر اختصاصی) و یا APIهای وب سرویس‌ها قابل دسترسی است. برای شروع نیاز به هزینه‌ای نیست. در واقع افراد تنها برای آنچه استفاده‌می‌کنند هزینه می‌پردازند." Foster و همکارانش محاسبات ابری را این‌گونه تعریف می‌کنند: "یک نمونه محاسباتی توزیع‌شده در مقیاس بزرگ که از صرفه‌جویی‌های مقیاس نشات گرفته‌است، استخری است از انتزاع، مجازی‌سازی، به صورت پویا مقیاس‌پذیر، نیروی محاسباتی قابل مدیریت، حافظه‌های ذخیره‌سازی، پلت‌فرم‌ها و سرویس‌هایی که از طریق اینترنت براساس تقاضای مشتریان خارجی در اختیار آنها گذاشته می‌شود."

دو ایده مهم که در تعریف Foster و همکارانش اضافه شده است: مجازی‌سازی و مقیاس‌پذیری است. مجردسازی محاسبات ابری از طریق مجازی‌سازی سخت‌افزار و نرم‌افزار سیستم زیرین انجام می‌شود. منابع مجازی از طریق یک واسط مجرد از قبل تعریف‌شده (یک واسط برنامه‌کاربردی API) یا یک سرویس فراهم می‌شوند. بنابراین، در سطح سخت‌افزار خام، منابع می‌توانند طبق درخواست فرستاده‌شده به واسط اضافه و یا خارج گردند، در حالی که واسط کاربر هیچ تغییری نکند. این معماری روی لایه فیزیکی ابر، بدون تاثیر روی واسط به کاربر مقیاس‌پذیر و منعطف است. سرانجام Vaquero و همکارانش، حدود ۲۲ تعریف از محاسبات ابری که همه در سال ۲۰۰۸ ارائه‌شده بودند را تحلیل کردند. براساس آن تحلیل، Vaquero و همکارانش تعریف زیر را ارائه دادند که هدف آن بازتاب درک کنونی از محاسبات ابری است: "ابرها استخر بزرگی از منابعی هستند که قابل استفاده و دسترسی به صورت مجازی و به سادگی (مانند سخت‌افزار، پلت‌فرم‌های توسعه‌یافته و/یا سرویس‌ها) می‌باشند. این منابع می‌توانند به‌طور پویا پیکربندی مجدد شوند تا در مورد یک بار (مقیاس) متغیر و همچنین استفاده بهینه از یک منبع متعادل گردند. این استخر از منابع نوعاً براساس مدل پرداخت به ازای استفاده که در آن تضمین‌ها توسط فراهم‌کننده زیرساخت و توسط SLAها تنظیم‌شده پیشنهاد شده است، ارائه می‌گردد."

به علاوه Vaquero و همکارانش مقیاس‌پذیری، مدل استفاده براساس پرداخت و مجازی‌سازی را به عنوان مجموعه مشخصه‌ای که، مینیمم تعریف ابرها دارند، خلاصه می‌کنند. به هر حال، در حالی که تعریف Vaquero و همکارانش دیگر تعریفات را با توجه به لایه فیزیکی خیلی خوب خلاصه کرده‌است اما به یکپارچه‌سازی سخت‌افزار با نرم‌افزار به عنوان یک سرویس به میزان کافی اشاره نکرده‌است. تمامی تعریفات بیان‌می‌دارند که محاسبات ابری محیطی است که شامل تعدادی جنبه

است و مربوط به نمونه‌ای جدید از فناوری‌اطلاعات (تحویل و توسعه سخت‌افزار و برنامه‌های‌کاربردی) می‌باشد. به‌طور کلی، محاسبات ابری در رابطه با تحویل قابلیت‌های فناوری‌اطلاعات به مشتریان خارجی است و یا از دیدگاه کاربر، شامل تحویل قابلیت‌های فناوری‌اطلاعات از یک فراهم‌کننده خارجی، به عنوان یک سرویس به صورت پرداخت به ازای استفاده و از طریق اینترنت می‌باشد. به علاوه، مقیاس‌پذیری و مجازی‌سازی به عنوان مشخصه‌های کلیدی محاسبات ابری دیده شده‌اند، مقیاس‌پذیری به تعدیل منابع فناوری‌اطلاعات فراهم‌شده به نسبت بار متغیر اشاره دارد. به عنوان نمونه، افزایش و یا کاهش تعداد کاربران، ظرفیت ذخیره‌سازی مورد نیاز یا قدرت پردازش. مجازی‌سازی، که به عنوان اساسی در تمامی معماری‌های محاسبات ابری است، اصولا برای تجرید و کپسوله‌سازی استفاده می‌شود. تجرید اجازه می‌دهد تا محاسبه خام، فضای ذخیره‌سازی و منابع شبکه به عنوان استخری از منابع متحد شوند و پوشش و جای‌گیری منبعی مانند سرویس‌های ذخیره‌سازی داده را روی آنها امکان می‌سازد. سرانجام اینکه کپسوله‌سازی برنامه‌های‌کاربردی امنیت، قابلیت مدیریت و ایزوله‌سازی را بهبود داده‌است. مشخصه مهم دیگر ابرها یکپارچه‌سازی سخت‌افزار و نرم‌افزار سیستم با برنامه‌های‌کاربردی است. هم سخت‌افزار و هم نرم‌افزار سیستم، یا زیرساخت و برنامه‌های‌کاربردی به عنوان سرویس در یک محیط یکپارچه ارائه می‌شوند [۹].

۲-٤-۲ مشخصات اصلی محاسبات ابری

محاسبات ابری چند ویژگی اصلی دارد که ارتباط و تفاوت آنها را از روش‌های محاسبات سنتی نشان می‌دهد:

خدمات سلف سرویس مورد تقاضا[۱]: ارائه‌دهنده محاسبات ابری باید توانایی ارائه منابع محاسباتی در هر زمانی که مشتری به آنها نیاز دارد را داشته‌باشد. در واقع مصرف‌کننده می‌تواند به‌طور یک جانبه قابلیت‌های محاسباتی مانند زمان سرور و حافظه‌ی شبکه مورد نیاز را به صورت خودکار، بدون نیاز به تعامل انسان با یک ارائه‌دهنده سرویس فراهم کند. از نقطه نظر مشتری، منابع محاسباتی، تقریباً در دسترسی نامحدود هستند.

دسترسی به شبکه گسترده: محاسبات ابری از فناوری‌های شبکه‌ی موجود برای ارائه سرویس به مشتریان استفاده و میان سهام‌داران اتصال برقرار می‌کند. همچنین سرویس نرم‌افزاری مبتنی بر ابر را ترویج می‌دهد.

ادغام منابع: هر ارائه‌دهنده‌ی ابر، مشتریان متعددی دارد. مشتریان، منابع محاسباتی را به صورت پویا از یک مخزن منابع گرفته و آنها را به مخازنی که هیچ تقاضایی وجود ندارد منتشر می‌کنند. میزانی از استقلال وجود دارد که مشتری به‌طور کلی هیچ کنترل و یا دانشی از محل دقیق منابع ارائه‌شده ندارد، اما ممکن‌است قادر به تعیین محل در سطح بالاتری از انتزاع (به عنوان مثال کشور، ایالت و یا مرکز داده) باشد. نمونه‌هایی از منابع شامل ذخیره‌سازی، پردازش، حافظه، پهنای باند شبکه و ماشین‌های‌مجازی است.

قابلیت ارتجاعی سریع: براساس توافق‌نامه سطح سرویس خاص، ارائه‌دهنده ابر، منابع ارائه‌شده برای پاسخگویی به نیازهای در حال تغییر مشتری را برآورده می‌سازد که تخصیص منابع را با توجه به خواسته‌های فعلی جمع‌آوری‌شده از کاربران خود برآورده می‌کند و در غیر این صورت احتمالاً غرامت مشخصی برای عدم برآورده‌کردن توافق‌نامه سطح سرویس مربوطه به هر یک از مشتریان پرداخت می‌کند. قابلیت‌ها می‌تواند به سرعت و به صورت ارتجاعی و در برخی موارد به‌طور خودکار با سرعت خارج از مقیاس تأمین و به سرعت در مقیاس داخل منتشر شود. برای مشتری، قابلیت‌های موجود برای تأمین اغلب نامحدود است و می‌تواند در هر مقدار و در هر زمان خریداری شود. تأمین منابع می‌تواند به سرعت رخ دهد، همچنین تقاضا برای منابع ممکن‌است به صورت پویا متفاوت باشد.

پرداخت نسبت به استفاده: یک جنبه‌ی جدید دیگر محاسبات ابر، مدل حسابداری مبتنی بر استفاده از برنامه‌های‌کاربردی است. سیستم‌های ابر به‌طور خودکار استفاده از منابع را با بکارگیری قابلیت اندازه‌گیری در برخی سطوح انتزاع مناسب و بسته به نوع

---

[۱] On Demand Self Service

سرویس (به عنوان مثال ذخیره‌سازی، پردازش، پهنای باند یا حساب‌های کاربری فعال) کنترل و بهینه‌سازی می‌کنند. استفاده از منابع برای انواع مختلف سرویس براساس معیار نوع سرویس اندازه‌گیری می‌شود و مشتری تنها برای استفاده کوتاه مدت از پردازنده‌ها و ذخیره‌سازی هزینه می‌پردازد. به عنوان مثال استفاده می‌تواند در افزایش ساعت یا روز بکار رود، آنچه می‌تواند هزینه‌های سرمایه‌گذاری را به هزینه‌های عملیاتی تبدیل کند [۱، ۲، ۹، ۱۵ و ۱۶].

۲-۵ معماری و مولفه‌های ابر

در این بخش ابتدا یک دیدگاه کلی از ایده‌ها با توجه به ساختار و مولفه‌های ابر ارائه می‌شود. سپس معماری سه لایه ابرها بین خواهدشد.

۲-۵-۱ دیدگاه کلی از ایده‌های موجود برای ساختارهای ابری و مولفه‌های آن

در منابع موجود ساختارهای ابری زیادی را می‌توان یافت که این دسته‌بندی‌ها در نگاه اول متفاوتند اما در نهایت طبقه‌بندی و توصیف پدیده‌ی مشابهی را به اشتراک می‌گذارند. ساختاری با جزئیات کامل با هفت مولفه محاسبات ابری ارائه می‌دهد که شامل برنامه‌کاربردی، کلاینت، زیرساخت، پلت‌فرم، سرویس، فضای ذخیره‌سازی و قدرت محاسباتی می‌شود. به روش‌های متفاوتی که یک شرکت می‌تواند از محاسبات ابری برای توسعه برنامه‌های‌کاربردی تجاری‌اش استفاده کند نگاه می‌اندازد و چهار نوع متفاوت از توسعه سرویس ابری شامل نرم‌افزار به عنوان سرویس، پلت‌فرم به عنوان سرویس، سرویس‌های وب و محاسبات بر مبنای تقاضا را برمی‌شمرد. محاسبات بر مبنای تقاضا آن‌طور که بیان داشته‌است، همان محاسبات ابزاری است. Youseff و همکارانش برای محاسبات ابری پنج لایه قائل شده‌اند: برنامه‌کاربردی ابری، محیط نرم‌افزاری ابری، زیرساخت نرم‌افزاری ابری، کرنل نرم‌افزاری و سخت‌افزار/میان‌افزار.

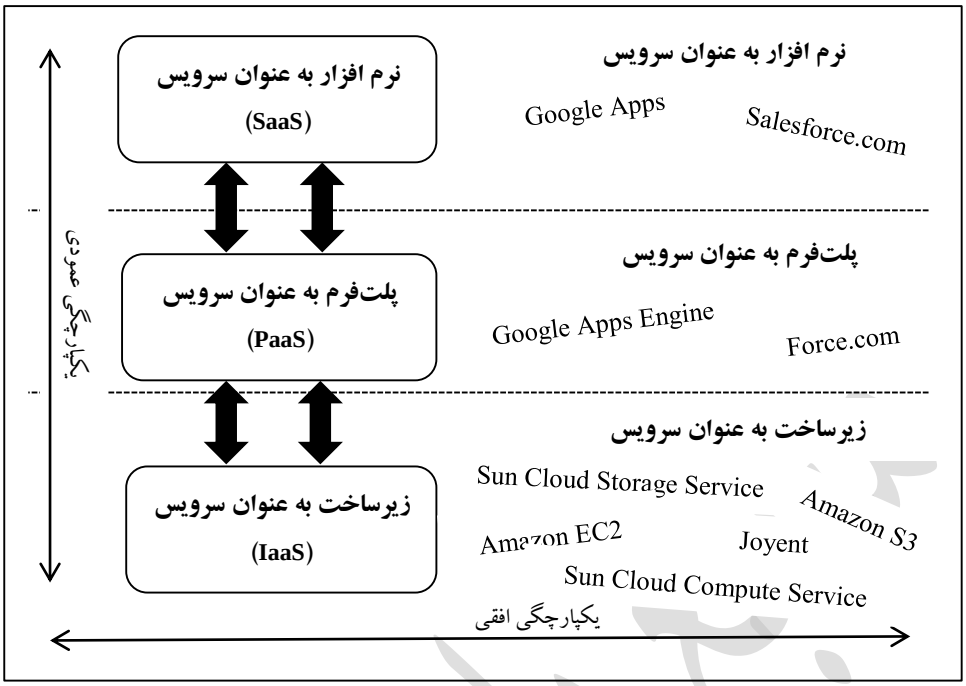
مرکز تحقیقات Forrester مولفه‌های ابرها را به بازارها مربوط کرده است و پنج بازار سرویس ابری را مشخص کرده است. دو مورد از این بازارها، یعنی سرویس‌های مبتنی بر وب و راهنماهای SaaS، به عنوان بازارهایی که از ابر تحویل داده‌می‌شوند، شناخته می‌شوند در حالی که سه زیرساخت بازاری ابری که به عنوان سرویس جدیدی هستند عبارتند از: مولفه‌های برنامه‌های‌کاربردی به عنوان سرویس، پلت‌فرم نرم‌افزار به عنوان سرویس و زیرساخت مجازی به عنوان سرویس. سرانجام Reese، SaaS را به عنوان نرم‌افزاری در ابر مورد ملاحظه قرار داده‌است و چهار مدل زیرساخت ابری به نام‌های پلت‌فرم به عنوان سرویس، زیرساخت به عنوان سرویس، ابرهای خصوصی و مدل چهارم که تمامی جنبه‌های مدل‌های زیرساخت ابری قبلی را ارائه می‌دهد، قائل شده است. ایده‌های بالا توصیف کاملی از یک زیرساخت ابری و مولفه‌هایش ارائه نمی‌کند. ایده‌ای که اغلب برای توصیف یک ساختار نوعی از ابرها و مولفه‌هایش استفاده‌می‌شود ایده‌ی سه لایه‌ای است که در بخش بعدی توضیح داده‌می‌شود [۹ و ۱۷].

۲-۵-۲ مدل‌های سرویس محاسبات ابری

تعاریفی که در بخش (تعاریف ابر) ارائه شد، نشان داد که محاسبات ابری شامل قابلیت‌های متفاوت فناوری اطلاعات شامل زیرساخت، پلت‌فرم‌ها و نرم‌افزار است. می‌توان گفت اشکال، بخش‌ها، قسمت‌ها، استایل‌ها، انواع، سطوح یا لایه‌های متفاوت محاسبات ابری بدون توجه به اصطلاحات بکاررفته، این دسته‌بندی سه لایه برای محاسبات ابری بیشتر رایج است. از آنجایی که تحویل منابع فناوری اطلاعات یا قابلیت‌ها به عنوان سرویس مشخصه مهمی از محاسبات ابری است، سه لایه معماری محاسبات ابری عبارتند از (شکل ۲-۱):

۱) زیرساخت به عنوان سرویس (IaaS)　　۲)پلت‌فرم به عنوان سرویس (PaaS)　　۳)نرم‌افزار به عنوان سرویس (SaaS)

در ادامه سه لایه محاسبات ابری و ارتباط آنها با یکدیگر بیان می‌شود.



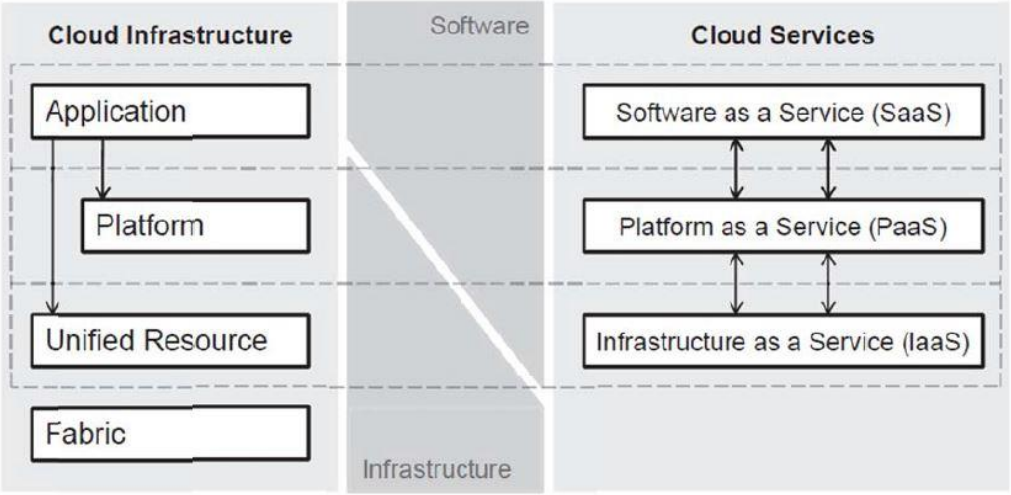
شکل ۲-۱: سه لایه محاسبات ابری: IaaS، PaaS و SaaS [۹].

زیرساخت به عنوان سرویس

قابلیت‌هایی برای ارائه‌ی پردازش، ذخیره‌سازی، شبکه‌ها و سایر منابع محاسباتی اساسی به مشتری ارائه می‌دهد که در آن مشتری می‌تواند یک سیستم‌عامل، برنامه‌ی‌کاربردی یا هر نرم‌افزار منتخب را اجرا و عملیاتی کند. مشتری، زیرساخت‌های اساسی ابر را مدیریت یا کنترل نمی‌کند اما بر سیستم‌عامل، ذخیره‌سازی و گسترش برنامه‌های‌کاربردی‌کنترل دارد و احتمالا کنترل محدودی روی اجزای شبکه انتخابی دارد (به عنوان مثال میزبان فایروال). در واقع چیزی که IaaS ارائه می‌دهد منابع محاسباتی مانند پردازشگر یا فضای ذخیره‌سازی است که می‌تواند به عنوان سرویس استفاده گردد. مثال‌هایی از سرویس‌های وب Amazon با محاسبات قابل ارتجاع ابری (EC2) برای پردازش و سرویس ذخیره‌سازی ساده (S3) برای ذخیره‌سازی و Joyent که زیرساخت مبتنی بر تقاضای مقیاس‌پذیر برای اجرای وب سایت‌ها و برنامه‌های‌کاربردی وب غنی می‌باشد. فراهم‌کنندگان PaaS و SaaS می‌توانند سرویس‌های خود را بر مبنای واسطهای استاندارد شده روی IaaS قرار دارند. به جای فروش زیرساخت سخت‌افزاری خام، فراهم‌کنندگان IaaS نوعاً زیرساخت مجازی‌شده‌ای به عنوان سرویس ارائه می‌دهند. Foster و همکارانش به سطح منابع سخت‌افزاری خام مانند نیروی محاسباتی، فضای ذخیره‌سازی و منابع شبکه لایه fabric می‌گویند. نوعاً با استفاده از مجازی‌سازی، منابع سطح سخت‌افزار مجردسازی و کپسوله می‌شوند و بنابراین می‌توانند در معرض لایه بالاتر و کاربران نهایی از طریق واسطهای استاندارد شده به عنوان منابع یکپارچه‌شده به فرم IaaS قرار می‌گیرند (شکل ۲- ۲).

قبل از ظهور محاسبات ابری، زیرساخت به عنوان سرویس برای مدتی موجود بود که به آن محاسبات ابزاری می گفتند که حتی توسط بعضی از نویسندگان به عنوان لایه زیرساخت محاسبات ابری یاد می‌شود. در مقایسه با چیزی که محاسبات ابزاری ارائه می داد، IaaS سیر تکاملش به سمت حمایت از یکپارچه‌سازی برای تمام سه لایه (IaaS، PaaS و SaaS) در یک ابر است. از ابتدای ارائه محاسبات ابری واضح بود که برای محاسبات ابری فراهم‌کنندگان موفق اند، آنها می‌بایست واسطی آماده می‌کردند که دسترسی، درک، برنامه‌نویسی و استفاده از آن ساده باشد یعنی یک API که یکپاچه‌سازی با زیرساخت برنامه‌های‌کاربردی SaaS

مشتریان و فراهم‌کنندگان بالقوه را فراهم می‌سازد. مراکز داده فراهم‌کنندگان محاسبات ابزاری به میزان کافی استفاده می‌شد اگر تنها توسط توده مهمی از مشتریان و فراهم‌کنندگان SaaS استفاده شوند. به عنوان نتیجه‌ای از شرایط لازم برای دسترسی آسان و مجرد شده به لایه فیزیکی یک ابر، مجازی‌سازی لایه فیزیکی و پلت‌فرم‌های برنامه‌نویسی برای توسعه‌دهندگان به عنوان مشخصه اصلی ابرها محسوب می‌گردد.



شکل ۲- ۲: معماری ابری مربوط به سرویس‌های ابری [۱۵].

پلت‌فرم به عنوان سرویس

پلت‌فرم‌ها لایه‌ای مجرد بین برنامه‌های‌کاربردی نرم‌افزار (SaaS) و زیرساخت مجازی‌شده (IaaS) هستند. ارائه‌دهنده‌ی ابر، سخت‌افزار و قابلیت ایجاد یا خریداری برنامه‌های‌کاربردی مشتری برای گسترش بر روی زیرساخت‌های ابر، با استفاده از زبان‌های برنامه‌نویسی و ابزار پشتیبانی را ارائه‌می‌دهد. مشتری، زیرساخت‌های اساسی ابر مانند شبکه، سرورها، سیستم‌های‌عامل و ذخیره‌سازی را مدیریت یا کنترل نمی‌کند، اما برنامه‌های‌کاربردی گسترش‌یافته و احتمالاً پیکربندی محیط میزبان برنامه‌های‌کاربردی را کنترل می‌کند. ارائه‌دهندگان PaaS، توسعه‌دهندگان نرم‌افزار را هدف قرار داده‌اند. توسعه‌دهندگان کد، برنامه‌کاربردیشان را روی پلت‌فرم بارگذاری می‌کنند که نوعاً وقتی رشد استفاده از برنامه‌های‌کاربردی بالا می‌رود این مساله را به‌طور اتوماتیک مدیریت می‌کنند. ارائه‌دهندگان PaaS می‌توانند تمامی فازهای توسعه نرم‌افزار را پوشش دهند یا ممکن است روی ناحیه مشخص و معینی مثل مدیریت محتوا خاص شده‌باشند. مثال‌ها عبارتند از Google App Engine که اجازه‌ی اجرای برنامه‌های‌کاربردی روی زیرساخت Google را می‌دهد و پلت‌فرم Salesforce.com. لایه PaaS یک ابر بر واسط استاندارد شده لایه IaaS تکیه دارد که دسترسی به منابع موجود را مجازی می سازد و واسط‌های استاندارد شده و یک پلت‌فرم برای لایه SaaS فراهم می‌کند.

نرم‌افزار به عنوان سرویس

قابلیت‌های ارائه‌شده به مشتری برای استفاده از برنامه‌های‌کاربردی ارائه‌دهنده‌ی در حال اجرا بر روی زیرساخت‌های ابر می‌باشد. برنامه‌های‌کاربردی برای دستگاه‌های مختلف مشتریان از طریق یک رابط مشتری نازک مثلاً یک مرورگر وب (به عنوان مثال، ایمیل مبتنی بر شبکه) در دسترس هستند. مشتریان، زیرساخت‌های اساسی ابر از جمله شبکه، سرورها، سیستم‌عامل، ذخیره‌سازی یا حتی قابلیت‌های نرم‌افزاری شخصی را به استثنای پارامترهای برنامه‌کاربردی (مثل تنظیمات پیکربندی برنامه خاص کاربر محدود) مدیریت یا کنترل می‌کنند.

همان‌طور که قبلا بیان شد، SaaS نرم‌افزاری است که تحت مالکیت و مدیریت از راه دور یک یا چند فراهم‌کننده است و براساس استفاده بر مبنای پرداخت هزینه ارائه می‌شود. SaaS مشهودترین لایه محاسبات ابری برای کاربران نهایی است چرا که در ارتباط با برنامه‌های کاربردی نرم‌افزاری واقعی است که مورد دسترسی و استفاده واقع می‌گردد. از نقطه نظر کاربر، داشتن نرم‌افزار به عنوان سرویس اساساً به‌خاطر مدل پرداخت براساس استفاده و به علت مزایای هزینه به آنها انگیزه می‌دهد. مثال‌هایی معروف از ارائه‌دهندگان SaaS، Salesforce.com و Google Apps مانند Google Mail، Google Docs و Spreadsheets هستند. کاربر نوعی یک ارائه‌دهنده SaaS معمولاً نه دانش و نه کنترلی روی زیرساختِ پلت‌فرم نرم‌افزاری که ارائه‌دهنده SaaS بر مبنای آن است (PaaS) و یا زیرساخت سخت‌افزاری واقعی (IaaS) ارائه‌شده به او دارد. به‌طور کلی لایه‌ها خیلی به فراهم‌کننده SaaS مربوط هستند چرا که لازم می‌باشند و می‌توانند به عنوان منبع خارجی باشند. برای مثال، یک برنامه‌کاربردی SaaS می‌تواند روی یک پلت‌فرم موجود توسعه داده‌شود و روی زیرساخت شخص ثالثی اجرا گردد [۱، ۲، ۹ و ۱۵].

٦-۲ دسته‌بندی ابرها

ابرها معمولاً می‌توانند طبق اینکه مالک داده مراکز ابر کیست، دسته بندی شوند. یک محیط ابری هم می‌تواند شامل یک ابر و هم شامل چند ابر باشد. بنابراین بین محیط‌های تک ابری یا چند ابری باید تمایز قائل شد. زیربخش‌های زیر دسته بندی‌ای از محیط‌های تک ابری بر مبنای مالک مرکز داده ابر و دسته بندی بر مبنای محیط‌های چندابری بر مبنای مالک مراکز داده ابری است. صرف نظر از مدل سرویس مورد استفاده، چهار مدل برای گسترش سرویس ابر وجود دارد:

ابرهای عمومی[۱]: زیرساخت‌های ابر ساخته‌شده که در دسترس عموم افراد یا گروه‌های صنعتی بزرگ قرار دارد و متعلق به سازمان فروشنده‌ی سرویس ابر است. سازمان مسئول ممکن‌است انواع مختلفی از سرویس‌های ابر را با استفاده از مدل ابرهای عمومی ارائه دهد.

ابرهای خصوصی[۲]: برای استفاده‌ی انحصاری یکی از مشتریان (یک سازمان واحد) ساخته‌شده، که مالک آن است و به‌طور کامل ابر را کنترل می‌کند، که منابع ممکن‌است در داخل یا خارج از سازمان باشند و به صورت محلی از طریق سازمان یا شخص ثالث اداره شود. این واقعیت که ابر توسط یک مشتری خاص استفاده می‌شود ویژگی متمایز هر ابر خصوصی است.

ابرهای متحدشده[۳]: هنگامی که چندین مشتری (سازمان‌های مختلف) نیازهای مشابه دارند، می‌توانند یک زیرساخت، پیکربندی و مدیریت ابر را به اشتراک بگذارند. این مدیریت ممکن‌است به صورت محلی توسط مشتری (سازمان) یا توسط اشخاص ثالث انجام شود.

ابرهای ترکیبی[۴]: زیرساخت‌های ابر مرکب ابرهای عمومی و خصوصی را به عنوان یک موجودیت واحد و همراه با فناوری‌های استاندارد یا اختصاصی محدود ترکیب می‌کنند و به یک سازمان اجازه می دهند که تعدادی برنامه‌کاربردی را هم روی زیرساخت یک ابر داخلی و هم روی ابرهای عمومی اجرا کند که داده‌ها و قابلیت حمل برنامه‌های کاربردی (به عنوان مثال، انفجار ابر برای تعادل بار بین ابرها) را پشتیبانی می‌کنند [۱، ۲، ۱۵ و ۱۶]. به این ترتیب، شرکت ها می‌توانند از منابع مقیاس‌پذیر فناوری‌اطلاعات ارائه‌شده توسط فراهم‌کنندگان خارجی سود برند، در حالی که برنامه‌های کاربردی خاص و یا داده را دورن دیواره آتش نگه می‌دارند. یک محیط ابری ترکیبی، پیچیدگی را با وجود توزیع برنامه‌های کاربردی در محیط‌های متفاوت، نظارت زیرساخت داخلی و خارجی درگیر، امنیت را افزایش دهد و ممکن‌است در مورد برنامه‌های کاربردی ای که نیاز به پایگاه‌های داده پیچیده و یا همگام‌سازی دارند مناسب نباشند.

ابرهای متحدشده مجموعه‌ای از ابرهای تکی هستند که می‌توانند با یکدیگر کار کنند به عنوان نمونه تبادل داده و منابع محاسباتی از طریق واسط‌های از قبل تعریف شده. طبق اصول کلیدی اتحاد، در اتحاد ابرها تک تک ابرها مستقل می‌مانند اما

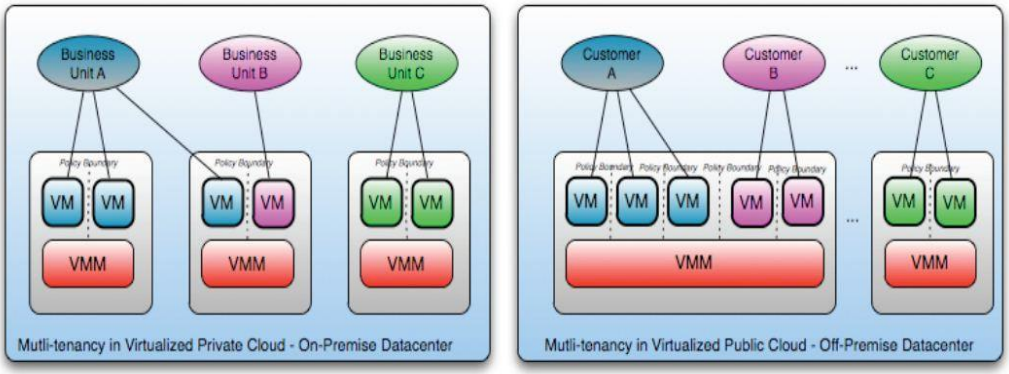
---

۱ Public clouds
۲ Private clouds
۳ Community clouds
۴ Hybrid clouds

می‌توانند با دیگر ابرها در اتحادیه از طریق واسط‌های استاندارد شده با یکدیگر کار کنند. اصطلاح ابرهای اتحادی یا اتحادیه ابرها به همکاری و اتحاد ابرهای عمومی و یا حتی ابرهای خصوصی درگیر اشاره دارد. فراهم‌کنندگان زیرساخت ابری لازم است منابع محاسباتی مقیاس‌پذیر زیادی را فراهم‌کنند. این مسئله به کاربران و فراهم‌کنندگان SaaS ابری اجازه می‌دهد که در مورد زیرساخت محاسباتی مورد نیاز برای اجرای سرویس‌هایشان نگران نباشند. فراهم‌کنندگان زیرساخت ابری ممکن‌است خودشان با مشکل مقیاس‌پذیری رو به رو شوند. یک شرکت میزبان تکی ممکن‌است قادر به فراهم‌کردن زیرساخت محاسباتی ناحدودی که بتواند به تعداد افزایشی‌ای از برنامه‌های‌کاربردی با تعداد زیادی کاربر و دسترسی در هر زمان و در هر کجا سرویس دهد، نباشد. در نتیجه، فراهم‌کنندگان زیرساخت ابری ممکن‌است برای اینکه قادر به خدمت‌رسانی نیازهای فراهم‌کنندگان سرویس ابری باشند، شریک شوند، به عنوان نمونه فراهم‌کردن ابزار محاسباتی نامحدود. بنابراین، ابر ممکن‌است یک اتحادیه از فراهم‌کنندگان زیرساخت یا یک اتحادیه از ابرها باشد.

۲-۷ چند اجاره‌ای[۱]

چنداجاره‌ای در مدل‌های سرویس ابر، نیازهای مربوط به پیاده‌سازی سیاست محور، تقسیم‌بندی، جداسازی، هماهنگی، سطوح سرویس و مدل‌های بازگشت سرمایه/حسابداری برای حوزه‌های مختلف مشتری را نشان می‌دهد. مشتریان ممکن‌است از سرویس ارائه‌شده توسط ارائه‌دهندگان ابرهای عمومی یا سازمان‌های مشابه استفاده‌کنند. از دیدگاه ارائه‌دهنده، چنداجاره‌ای روش معماری و طراحی برای صرفه به مقیاس فعال، دردسترس بودن، مدیریت، تقسیم‌بندی، جداسازی و بازدهی عملیاتی زیرساخت‌های مشترک نفوذی، داده‌ها، فراداده، سرویس و برنامه‌های‌کاربردی در میان مشتریان مختلف را نشان می‌دهد. شکل ۲-۳ مدل چند اجاره‌ای را نشان می‌دهد.



شکل ۲-۳: چنداجاره‌ای [۱].

۲-۸ مجازی‌سازی[۲]

در مدل ابر، آنچه مشتریان واقعاً برای آن پول می‌پردازند و آنچه که آنها به صورت پویا اجاره می‌کنند، ماشین‌های مجازی است. این توانایی به ارائه‌دهنده‌ی سرویس ابر اجازه می‌دهد زیرساخت‌های ابر واقع در مراکز داده را بین مشتریان مختلف به اشتراک بگذارند. مجازی‌سازی به انتزاع منابع کامپیوتر با استفاده از ماشین‌های مجازی اشاره دارد. مجازی‌سازی اجازه می‌دهد تا سیستم‌عامل‌های چندگانه به‌طور همزمان در یک دستگاه فیزیکی مشابه اجرا شوند. مجازی‌سازی و مهاجرت پویای ماشین‌های مجازی در محاسبات ابری باعث استفاده‌ی کارآمدتر از منابع فیزیکی در دسترس موجود می‌شود. مجازی‌سازی با افزودن یک لایه زیرِ سیستم‌عامل (بین سیستم‌عامل و سخت‌افزار) بدست‌آمده‌است. دو گزینه‌ی متفاوت برای این لایه مجازی‌ساز وجود دارد:

---

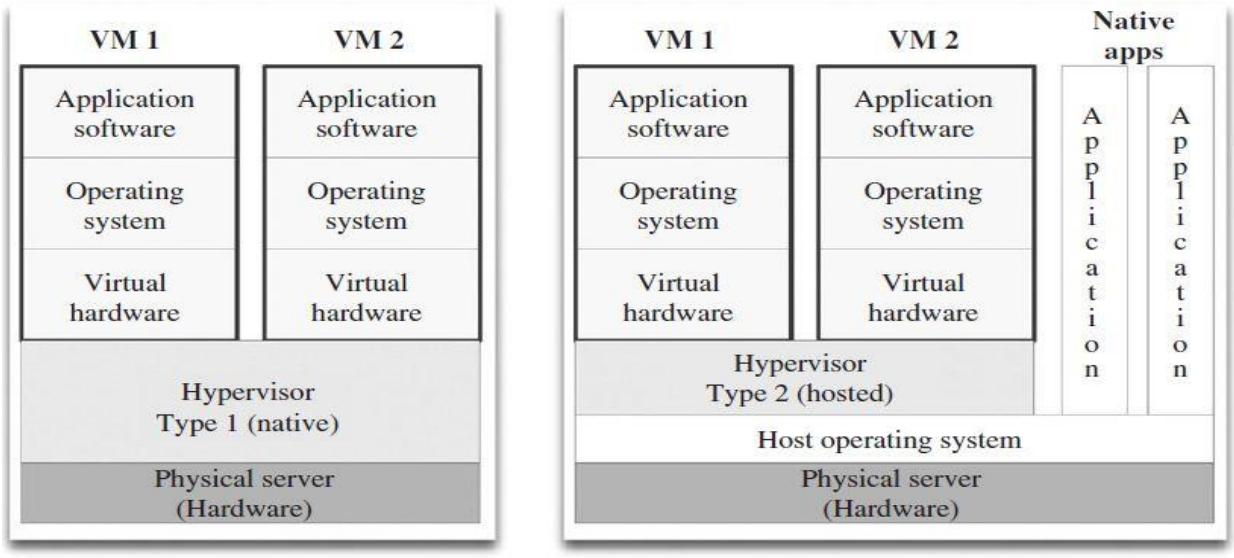
[۱] Multi Tenancy

[۲] Virtualization

نوع یک: این نوع از لایه‌ی مجازی‌سازی، مجازی‌سازی محلی نام دارد و توسط مدیریت ماشین مجازی اجرا می‌شود. به‌طور مستقیم بر روی سیستم نصب‌شده و دسترسی مستقیم به سخت‌افزار دارد. سیستم‌عامل در بالاترین سطح قرار می‌گیرد. به همین دلیل سریع‌ترین، مقیاس‌پذیرترین و قوی‌ترین گزینه است.

نوع دو: مجازی‌سازی میزبان. مدیریت ماشین مجازی به عنوان یک برنامه‌ی کاربردی بر روی سیستم‌عامل میزبان قرار می‌گیرد و ماشین‌های مجازی روی مدیریت ماشین مجازی اجرا می‌شوند.

در هر دو صورت لایه‌ی مجازی‌ساز تمام ماشین‌های مجازی را مدیریت می‌کند. ناظر ماشین مجازی، برای هر یک راه‌اندازی می‌شود. امروزه روش مدیریت ماشین مجازی در همه‌ی مراکز محاسبات ابری استفاده می‌شود و به عنوان کارآمدترین گزینه در شرایط استفاده از سخت‌افزار است (شکل ۲-۴).



شکل ۲-٤: مجازی‌سازی مدیریت ماشین مجازی نوع یک و دو [۱۶ و ۱۸].

۲-۹ شکل‌های ابر

انجمن جریکو به‌طور خلاصه چهار معیار برای شکل‌های مختلف ابر از یکدیگر شناسایی کرده که به مدل مکعب ابر معروف است. این چهار بعد در ادامه توضیح داده شده‌اند:

۲-۹-۱ بعد یک: داخلی/خارجی

این بعد موقعیت فیزیکی داده‌ها را تعریف می‌کند.

شکل‌های ابری که می‌خواهید استفاده کنید کجا هستند. داخل یا خارج از محدوده‌های سازمان هستند.

- اگر درون محدوده‌ی فیزیکی سازمان قرار دارند پس داخلی هستند.
- اگر درون محدوده‌ی فیزیکی سازمان قرار ندارند پس خارجی هستند.

برای مثال، دیسک‌های سخت مجازی در یک مرکز داده‌ی سازمان می‌تواند داخلی باشد، در حالی که آمازن در برخی از موقعیت‌های خارج از سازمان، خارجی است. این فرض که بعد داخلی از بعد خارجی امن‌تر است یک فرض غلط است. استفاده‌ی موثر از هر دو مدل بهترین استفاده‌ی امن را به‌طور احتمالی فراهم می‌کند.

۲-۹-۲ بعد دو: اختصاصی/باز

این بعد حالت مالکیت فناوری، سرویس، واسط‌های ابر و ... را تعریف می‌کند. این بعد درجه‌ای از قابلیت‌های همکاری و نیز محل برنامه و داده‌ها بین سیستم‌ها و شکل‌های ابر دیگر را نشان می‌دهد و توانایی صرف‌نظر کردن داده‌ها از یک شکل ابر یا حرکت آنها به شکل‌های بدون محدودیت دیگر را فراهم می‌کند. همچنین محدودیت‌های روی توانایی اشتراک برنامه‌ها را نشان می‌دهد.

- اختصاصی به این معنی است که سازمان سرویسی فراهم می‌کند که متوسطی از مفاهیم را تحت مالکیتش نگه دارد. به عنوان یک نتیجه، هنگام عملیات در ابرهایی که اختصاصی هستند، بدون تلاش‌های معنی‌دار یا سرمایه، توانایی حرکت به تأمین‌کننده‌ی ابر دیگر ممکن نیست. اغلب، بیشتر پیشرفت‌های فناوری‌های ابداعی در حوزه‌ی اختصاصی رخ می‌دهد.
- ابرهای باز در فناوری‌هایی که اختصاصی نیستند استفاده می‌شود، به این معنی که احتمالا تأمین‌کنندگان بیشتری وجود دارند و شما محدودیتی در توانایی اشتراک داده‌ها و همکاری با بخش‌های انتخاب‌شده برای استفاده از فناوری‌های مشابه ندارید. سرویس باز تمایل به گسترش و مصرف شدن دارند و بیشتر به عنوان یک استاندارد باز منتشر می‌گردند.

۲-۹-۳ بعد سه: محیطی/غیرمحیطی

بعد سوم طرز معماری را ارائه‌می‌دهد—آیا درون محیط IT یا خارج آن عملیات می‌کند؟ غیرمحیطی معمولاً با شکست تدریجی/از بین رفتن/کاهش/فروپاشی محیط IT مبتنی بر انبار ارتباط دارد.

- محیطی به‌طور پیوسته برای عملیاتی کردن داخل محیط IT سازمان بکار می‌رود، اغلب توسط دیوارهای آتش شبکه علامت‌دهی می‌شود. هنگام اجرا در نواحی محیطی، ممکن است به سادگی محیط سازمان در خارج از دامنه‌ی محاسبات ابر با استفاده از یک شبکه خصوصی مجازی یا سرور مجازی عملیاتی در دامنه‌ی پروتکل اینترنت آن، به دلیل استفاده از سرویس دایرکتوری خودتان برای کنترل دسترسی، گسترش داده‌شود.
- غیرمحیطی فرض می‌کند که محیط سیستم از جریان طراحی‌شده‌ی اصول هر فرمان انجمن جریکو و چارچوب معماری همکاری‌گرا ساخته‌شده است.

نواحی غیرمحیطی در مدل مکعب ابر هم در دامنه‌ی داخلی و هم خارجی استفاده می‌شود. همکاری یا اشتراک داده‌ها نباید به عنوان داخلی یا خارجی دیده شود، بلکه باید توسط آن کنترل و محدود به طرفین شود که سازمان‌ها با استفاده از آن انتخاب می‌کنند.

۲-۹-٤ بعد چهار: برون‌سپاری/درون‌سپاری

این بعد به سوال "چه کسی ابر شما را اجرا خواهد کرد؟" پاسخ می‌دهد:

- برون‌سپاری: سرویس توسط یک طرف سومی فراهم شده است.
- درون‌سپاری: سرویس توسط کارمندان شما و تحت کنترل شما فراهم شده است [۱۹].

۲-۱۰ فرصت‌ها و چالش‌های محاسبات ابری

به‌طور کلی، برای تمامی انواع مختلف مشتریان ابری، یک ابر فرصت‌های اصلی را به صورت X به عنوان سرویس ارائه می‌دهد. از دیدگاه کاربر، مدل پرداخت بر مبنای ابزار به عنوان یکی از مزایای اصلی محاسبات ابری در نظر گرفته می‌شود. نیازی به سرمایه‌گذاری در زیرساخت نیست: سرمایه‌گذاری در مجوزهای نرم‌افزار و ریسک پرداخت هزینه مجوز نرم‌افزار و استفاده نکردن از آن و سرمایه‌گذاری در زیرساخت‌های سخت‌افزاری و نگهداری آن و کارکنان. بنابراین، هزینه‌های سرمایه‌گذاری به هزینه‌های عملیاتی تبدیل شده است. کاربران یک سرویس ابری تنها از میزانی از منابع فناوری‌اطلاعات که واقعاً نیاز دارند استفاده می‌کنند و

تنها به میزانی که از منابع فناوری‌اطلاعات واقعاً استفاده کرده‌اند هزینه پرداخت می‌کنند. در عین حال، آنها امکان استفاده از مقیاس‌پذیری و انعطاف پذیری ابر را هم دارند.

با این حال، محاسبات ابری معایبی نیز دارد: ابرها به مشتریان متفاوتی سرویس ارائه می دهند. بنابراین، کاربران یک سرویس ابر از اینکه کار چه شخص دیگری روی همان سروری است که کار آنها می‌باشد، اطلاعی ندارند. یک ابر نوعی در خارج از شرکت و یا فایروال سازمان است. در حالی که این مساله ممکن‌است نقش عمده‌ای برای مصرف‌کنندگان بازی نکند، اما می‌تواند تاثیر قابل توجهی در تصمیم‌گیری‌های شرکت در استفاده از خدمات ابر داشته‌باشد. خطرات عمده‌ی محاسبات ابری عبارتند از: در دسترس بودن، امنیت، کارایی، اطلاعات در قفل، محرمانه بودن و قابلیت بررسی اطلاعات، گلوگاه‌های انتقال داده، سختی یکپارچه‌شدن با فناوری‌اطلاعات محلی و کمبود تطبیق‌پذیری.

کاربر باید به قول فراهم‌کننده ابر با تکیه بر قابلیت اطمینان، کارایی و کیفیت سرویس زیرساخت اعتماد داشته‌باشد. استفاده از ابرها به امنیت بالاتر و ریسک‌های پنهانی مربوط به ذخیره‌سازی و مدیریت داده به دو روش مربوط می‌گردد: اولاً به علت نیاز به انتقال داده به ابر به‌طوری که داده در ابر پردازش شود. ثانیاً چون داده روی یک زیرساخت خارجی ذخیره‌می‌شود و مالک داده به بیمه فراهم‌کننده داده اعتماد دارند مبنی بر اینکه هیچ دسترسی غیرمجازی صورت نمی‌گیرد. به علاوه، استفاده از ابرها نیاز به سرمایه‌گذاری در یکپارچه‌سازی زیرساخت و برنامه‌کاربردی با ابر دارد. در حال حاضر، استانداردی برای واسط‌های IaaS، PaaS و SaaS وجود ندارد. که این مساله انتخاب یک فراهم‌کننده ابری و سرمایه‌گذاری در یکپارچه‌سازی با ابرها را پر ریسک می‌سازد. با داشتن یک log in قوی می‌توان به نتیجه رسید که این برای فراهم‌کننده ابر مزیت است اما برای کاربران یک عیب می‌باشد. با وجود ریسک استفاده از ابرها، در هر حالت یک ارزیابی با دقت و مقایسه مزایای بالقوه و ریسک‌ها لازم است. همچنین، این مساله باید مورد ملاحظه قرار گیرد که چه داده و پروسسی برای منابع ابری مناسب است و چه داده و پروسسی را نباید در خارج از دیوارهای آتش سازمان استفاده کرد.

۲-۱۱ چالش‌های امنیتی محاسبات ابری

محاسبات ابری به‌طور ذاتی امن نیستد. امنیت در ابر اغلب نامحسوس و کمتر قابل مشاهده است. چالش‌های مربوط به امنیت اطلاعات، مدیریت هویت و دسترسی برخی از چالش‌های امنیتی محاسبات ابری می‌باشند. کاربران ابر معمولاً هیچ کنترلی روی منابع ابر استفاده‌شده ندارند و یک ریسک افشای داده‌ی ذاتی برای کاربر یا ارائه‌دهنده‌ی ابر وجود دارد. معماری محاسبات ابری نیازمند انطباق معیارهای مدیریت دسترسی و شناسایی است. هنگامی که بررسی یا ذخیره‌سازی داده‌ها درون یک محیط عمومی برای شخص خاصی تایید شده‌باشد، باید پیش‌بینی‌های مناسب برای اطمینان از کنترل کامل و بدون وقفه در سرتاسر داده‌های آنها توسط مالکان داده انجام شود [۳].

۲-۱۲ چالش‌های حفظ حریم خصوصی محاسبات ابری

در محیط محاسبات ابر، ارائه‌دهندگان ابر توسط مشتری تعریف می‌شوند که می‌تواند میزبان یا انبار داده‌های مهم، فایل‌ها و رکوردهای کاربران ابر باشند. حفظ کنترل اطلاعات برای صاحب اطلاعات یک موضوع مهم است. با توجه به حجم یا مکان ارائه‌دهندگان محاسبات ابر، نگهداری و کنترل اطلاعات یا داده‌ها در همه‌ی زمان‌ها برای شرکت‌ها و کاربران خصوصی مشکل است و به همین دلیل آنرا به تامین کنندگان ابر واگذار می‌کنند. حفظ حریم خصوصی برای جلب اعتماد کاربر و نیازهای مراحل طراحی، یک موضوع مهم در محاسبات ابری است. حساسیت محرمانگی اطلاعات، نحوه دسترسی به داده‌ها و شرایط انتقال داده‌ها از جمله چالش‌های حفظ حریم خصوصی هستند.

شرکت‌های در حال رکورد درک کرده‌اند که می‌توانند به سادگی با بهره‌برداری از ابر درون خود، دسترسی سریعی به بهترین برنامه‌های کسب‌وکار به دست آورند. اطلاعات زیادی از افراد و شرکت‌ها در ابر قرار داده‌شده است که ممکن‌است همه یا برخی از اطلاعات حساس (مثلاً سوابق بانکی) یا از نظر قانونی حساس (مثلاً پرونده‌های سلامت)، دارای محرمانگی یا ارزشمندی زیادی به عنوان دارایی شرکت باشند (مثلاً اسرار کسب‌وکار) که نشان‌دهنده‌ی اهمیت محرمانگی اطلاعات است. کاربران یک ابر مشابه، مفاهیم و اساس مشترک پردازش و ذخیره‌ی داده‌ها را به اشتراک می‌گذارند. آنها به‌طور طبیعی در معرض خطر نشت، افشای تصادفی یا عمدی اطلاعات هستند. در انتقال داده‌ها اگر داده مورد استفاده یا در دامنه‌ای قرار داده‌شود، ممکن‌است ابر به‌طور منظم موقعیت را تغییر دهد یا روی مکان‌های چندگانه همزمان مستقر شود [۷].

۲-۱۳ محافظت از داده‌ها

داده‌های ذخیره‌شده در یک ابر عمومی، معمولاً در یک محیط مشترک مرتب‌شده با داده‌ها برای مصرف‌کنندگان دیگر مستقر شده‌اند. سازمان‌ها، داده‌های حساس و منظم را درون یک ابر عمومی مستقر می‌کنند، بنابراین باید ابزارهایی برای کنترل دسترسی و نگهداری امن از داده‌ها در نظر گرفته شود. داده‌های در حال استراحت، در حال انتقال و در حال استفاده باید امن باشند و دسترسی به داده‌ها باید کنترل شود. استانداردهایی برای پروتکل‌های انتقال و مجوزهای کلید عمومی اجازه‌ی انتقال داده‌ها برای محافظت با استفاده از رمزنگاری را می‌دهد و می‌تواند معمولاً با کارهای مشابه در محیط‌های زیرساخت به عنوان سرویس، پلت‌فرم به عنوان سرویس و نرم‌افزار به عنوان سرویس پیاده‌سازی شود. امنیت یک سیستم با بکارگیری رمزنگاری به کنترل مناسب کلیدهای مرکزی و اجزای مدیریت کلید وابسته است. اخیراً، مسئولیت مدیریت کلید رمزنگاری به‌طور کلی روی مصرف‌کننده ابر رخ می‌دهد. تولید و ذخیره کلید معمولاً بیرون از ابر با استفاده از ماژول‌های امنیت سخت‌افزار انجام می‌گیرد.

۲-۱۴ راهکارهای حفاظت از داده‌ها

برای حفاظت از داده‌ها راهکارهایی ارائه‌شده است که برخی از آنها به شرح زیرند:

انتخاب مدل گسترش ابر: کدام مدل گسترش ابر انتخاب شود.

داده‌های حساس: نحوه‌ی طبقه‌بندی داده‌های ذخیره یا پردازش‌شده در ابر چگونه باشد.

فناوری‌های رمزگذاری داده‌ها: انتخاب الگوریتم‌های هش، رمزگذاری و کلیدهای طولانی مناسب برای محافظت از داده‌ها هنگام عبور از شبکه.

مالکیت داده و دسترسی کاربران مجاز: مالکیت حقوقی داده‌های مشتری حفظ و سیستم‌های مدیریت دسترسی برای ورود کاربران به سیستم استفاده‌شود.

مدیریت کلید رمزگذاری داده‌ها: مدیریت رمزگذاری و رمزگشایی داده‌ها و کلیدهای استفاده‌شده توسط فروشنده و مشتری انجام شود.

تهیه‌ی سخت‌افزار و نرم‌افزار: سخت‌افزار و نرم‌افزار مورد نیاز برای زیرساخت ابر توسط یک منبع عرضه‌ی مشروع مورد استفاده قرار گیرد [۳].

۲-۱۵ خطرات مشترک امنیت اطلاعات در ابر

خطرات متعددی برای امنیت داده‌های محاسبات ابری وجود دارد که باید هنگام پرداختن به امنیت داده‌ها در نظر گرفته شود. این خطرات شامل فیشینگ، امتیاز دسترسی ارائه‌دهنده‌ی‌سرویس ابر و منبع یا منشأ خود داده‌ها می‌باشد.

۲-۱۵-۱ فیشینگ

یکی از خطرات غیر مستقیم برای داده‌های در حال حرکت، فیشینگ است. هر چند امروزه به‌طور کلی شکستن زیرساخت کلید عمومی بعید است، فریب کاربران نهایی در ارائه اعتبار برای دسترسی به ابرها امکان‌پذیر است. فیشینگ تلاش برای به دست آوردن اطلاعاتی (گاهی اوقات به‌طور غیر مستقیم، پول) از قبیل نام‌کاربری، کلمه عبور و جزئیات کارت اعتباری با قیافه مبدل به عنوان یک نهاد قابل اعتماد در ارتباطات الکترونیکی است [۲۰]. فیشینگ از تکنیک‌های مهندسی اجتماعی برای فریب کاربران و سوء استفاده از قابلیت‌های ضعیف از فناوری‌های امنیت وب موجود استفاده می‌کند [۱۸].

۲-۱۵-۲ حق دسترسی پرسنل ارائه‌دهنده

خطر دیگر در امنیت داده‌های ابر، دسترسی نامناسب به داده‌های حساس مشتری توسط پرسنل ابر است. سرویس برون‌سپاری شده‌ی مبتنی بر ابر یا غیر ابر می‌تواند کنترل‌های سازمان‌های IT که از طریق کنترل‌های فیزیکی و منطقی اعمال شده‌اند را دور بزند. این خطر یک تابع با دو عامل اصلی است: اول، تا حد زیادی داده‌های رمزگذاری‌نشده در معرض افشا شدن قرار دارد و دوم، پرسنل ارائه‌دهنده ابر به آن داده دسترسی دارند. ارزیابی این خطر مستلزم شیوه‌های ارائه‌دهنده‌ی‌سرویس ابر و تضمین این است که پرسنل ارائه‌دهنده‌ی‌سرویس ابر با حق دسترسی، به داده‌های مشتری دسترسی نخواهند داشت [۲۱].

۲-۱۶ برنامه‌های کاربردی و محدودیت‌های رمزنگاری داده‌ها

بروس اشنایر، در مقاله خود [۲۲] در مورد چگونگی رمزنگاری داده‌های در حال استراحت توضیح می‌دهد. یکی از نکات کلیدی اشنایر برای داده‌های در حال حرکت، کلیدهای رمزنگاری بی‌دوام است. اظهارات اشنایر به این صورت است: "کل مدل بر روی اینترنت قرار می‌گیرد. بخش عمده‌ای از داده‌های ذخیره‌شده بر روی اینترنت به‌طور جانبی توسط افراد استفاده می‌شود، که برای استفاده‌ی کامپیوترهای دیگر در نظر گرفته شده است و مشکل در آن نهفته است. کلیدها نمی‌توانند مانند قبل در ذهن افراد ذخیره شوند و به ذخیره بر روی کامپیوترهای مشابه در شبکه، که داده‌ها در آن مستقر است نیاز دارند و این بسیار خطرناک‌تر است."

۲-۱۷ احراز هویت داده‌ها و شناسایی کاربران

حفظ محرمانگی، یکپارچگی و دردسترس بودن برای امنیت داده‌ها، یک برنامه‌ی‌کاربردی صحیح و پیکربندی‌شده از شبکه‌ها، سیستم‌ها و مکانیزم‌های امنیتی کاربردی در سطوح مختلف زیرساخت ابر است. احراز هویت کاربران و حتی سیستم‌های برقراری ارتباط از طریق وسایل مختلف انجام می‌شود، اما مبنای هر یک از این موارد رمزنگاری است. احراز هویت کاربران اشکال مختلفی دارد، اما همه‌ی آنها براساس ترکیبی از عوامل احراز هویت است: چیزی که یک فرد می‌داند (مانند رمز عبور)، چیزی که آنها دارند (مانند یک توکن امنیتی)، برخی کیفیت‌های قابل اندازه‌گیری که برای آنها اصلی است (مانند اثر انگشت). به‌طور کلی کنترل دسترسی به صورت اختیاری یا اجباری انجام می‌شود، که رایج‌ترین مدل‌های آن عبارتند از:

کنترل دسترسی اختیاری[۱]: در یک سیستم، هر شی دارای یک مالک است. کنترل دسترسی توسط مالک شی برای تصمیم‌گیری اینکه چه کسی دسترسی و چه امتیازاتی خواهد داشت تعیین می‌شود.

کنترل دسترسی براساس نقش[۲]: سیاست‌های دسترسی توسط سیستم تعیین می‌شود. کنترل دسترسی اجباری، براساس اعتماد یا اجازه موضوع است، اما کنترل دسترسی براساس نقش، براساس نقش موضوع می‌باشد. یک موضوع می‌تواند به یک شی دسترسی داشته‌باشد یا یک تابع را در صورتی اجرا کند که مجموعه مجوزهای آنها- یا نقش- به آن اجازه می‌دهد.

---

[۱] Discretionary Access Control [۲] Role Based Access Control [۳] Mandatory Access Control

کنترل دسترسی اجباری[۳]: سیاست‌های دسترسی توسط سیستم تعیین و توسط برچسب حساسیت پیاده‌سازی شده است، که به هر شی و موضوع اختصاص داده‌شده است. برچسب موضوع، سطح اطمینان آن و برچسب شی، سطح اطمینانی که برای دسترسی نیاز است را مشخص می‌کند. اگر موضوع به دست‌آوردن دسترسی به یک شی است، برچسب موضوع باید حداقل به اندازه برچسب شی غالب باشد.

۲-۱۸ ذخیره‌سازی داده‌ها در ابر

از جمله پیشرفت‌های محاسبات ابری ذخیره‌سازی آنلاین است. امنیت داده‌ها برای چنین سرویس ابری شامل جنبه‌های مختلفی از جمله کانال‌های امن، کنترل‌های دسترسی و رمزگذاری می‌شود. در مدل ذخیره‌سازی ابر، داده‌ها بر روی سرورهای مجازی متعددی ذخیره می‌شوند. مزیت دیگر، کاهش هزینه کلی مربوط به وظایف نگهداری ذخیره‌سازی مانند تهیه پشتیبان، تکثیر و بازیابی حادثه است، که توسط ارائه‌دهنده‌ی‌سرویس ابر اجرا می‌شود. یکی از روندهای اخیر در ذخیره‌سازی مبتنی بر ابر آنلاین، دروازه ذخیره‌سازی ابر است. این دستگاه‌ها می‌توانند ویژگی‌های متعددی، از جمله موارد زیر را ارائه‌دهند:

- ترجمه‌ی برنامه‌های کاربردی و پروتکل‌های مورد استفاده مشتری برای کسانی که از سرویس ذخیره‌سازی مبتنی بر ابر استفاده می‌کنند که هدف آن یکپارچه‌سازی با برنامه‌های کاربردی موجود روی پروتکل‌های استاندارد شبکه است.
- قابلیت‌های پشتیبانی و بازیابی که با ذخیره‌سازی در ابر کار می‌کنند.
- رمزگذاری داده‌ها در محل، که کلیدها را برای دستگاه، محلی نگه می دارد [۲۳].

ارائه‌دهندگان ابر نیازمند حفاظت از حریم خصوصی و امنیت داده‌های اشخاص می‌باشند که آنها به نمایندگی از سازمان و کاربران نگهداری می‌کنند. مسئولیت مدیریت داده‌های شخصی یک بخش مرکزی از ایجاد اعتماد است که زیربنای پیروی از سرویس مبتنی بر ابر می‌باشد که بدون وجود این اعتماد، مشتریان برای استفاده از سرویس مبتنی بر ابر بی‌میل می‌شوند. برای تواناسازی سازمان برای تمرکز روی هسته‌ی کسب‌وکارش، خریداری و نگهداری کارمندان متخصص IT، نرم‌افزار و سخت‌افزار محاسباتی برای ذخیره و پردازش داده می‌تواند به یک فروشنده برون‌سپاری شود، که در این صورت هنوز سازمان در نهایت مسئول حفاظت از داده‌هایش می‌باشد. نگرانی‌های امنیتی پیرامون ذخیره‌سازی داده‌ها در ابر در مقایسه با داده‌هایی که در محل سازمان ذخیره‌شده‌اند ذاتا منحصربه‌فرد نیستند. این به این معنی نیست که خطرات داده‌ها در محیط‌های بسیار متفاوت مشابه هستند. بزرگترین خطرات برای داده‌ها ممکن‌است با دسترسی پرسنل ارائه‌دهنده‌ی‌سرویس به اطلاعات یا عدم بررسی اطلاعات در شکل‌های مختلف به خوبی مطابق باشد [۳].

۲-۱۹ احراز هویت

احراز هویت، فرایند بدست‌آوردن اطمینان در هویت کاربران است. سطوح اطمینان احراز هویت باید بسته به حساسیت منابع برنامه و اطلاعات و ریسک‌های موجود متناسب باشد. تعداد زیادی از ارائه‌دهندگان ابر از استاندارد زبان نشانه‌گذاری اثبات امنیت پشتیبانی و آنرا برای اداره‌ی کاربران استفاده می‌کنند و آنها را قبل از ارائه دسترسی به برنامه‌ها و داده‌ها تصدیق می‌کنند. زبان نشانه‌گذاری اثبات امنیت ابزارهایی برای تغییر اطلاعات بین دامنه‌های مشترک ارائه‌می‌دهد. برای مثال، زبان نشانه‌گذاری اثبات امنیت ثابت می‌کند که یک کاربر توسط یک ارائه‌دهنده‌ی مجوز، تصدیق شده و شامل اطلاعاتی در مورد امتیاز و اعتبارات کاربر می‌شود. به محض دریافت تراکنش، ارائه‌دهنده سرویس پس از استفاده از اطلاعات برای بدست‌آوردن سطح دسترسی مناسب، مجوزها و اعتبارات تامین شده برای کاربر را به‌طور موفقیت‌آمیز بررسی می‌کند.

درخواست زبان نشانه‌گذاری اثبات امنیت و پیام‌های پاسخ به‌طور معمول روی پروتکل دسترسی به شی ساده نگاشت شده‌اند، که متکی بر زبان نشانه‌گذاری توسعه‌پذیر[۱] برای فرمت‌های آن است. در یک ابر عمومی، برای مثال، یک کاربر یک کلید عمومی خاص با سرویس ایجاد می‌کند، کلید خصوصی می‌تواند برای علامت‌گذاری درخواست‌های پروتکل دسترسی به شی ساده استفاده‌شود [۲۱].

۲-۲۰ زبان نشانه‌گذاری اثبات امنیت

همان‌طور که خدمات وب شایع‌تر می‌شوند و کسب‌وکار به دنبال ارائه خدمات ترکیبی به مشتریانی است که آنها را به اشتراک می‌گذارند، نیاز گروهی کسب‌وکارها برای ارائه یک نقطه ورود به مشتریان خود بسیار مهم است. این فرایند می‌تواند مسئولیت سنگینی برای مشتریان باشد که باید نام‌های کاربری و کلمه‌های عبور مختلف را به‌خاطر داشته‌باشند و فعالیت‌های مختلف روی بخش‌های مرورگرهای وب مختلف را با واسط‌های کاربری غیرواحد مختلف نگهداری کنند. همچنین می‌تواند یک بار سنگین برای کسب‌وکارهای مختلف باشد.

در جهان خدمات وب، یک برنامه‌کاربردی کلاینت ممکن است نیاز به ارسال یک پیام[۲] برای پردازش با یک سرویس را داشته‌باشد. یک روش احتمالی این است که مشتری را برای سرویس، احراز هویت کند و اعتبارات امنیتی را برای شناسایی مشتری نگه دارد. این سرویس ممکن است نیاز به ارسال این پیام برای پردازش بیشتر به یک یا چند سرویس را داشته‌باشد که در این صورت هر سرویس نیاز به شناسایی جداگانه مشتری و نگهداری سابقه‌ای از اعتبار مشتری برای یک سرویس منحصر به فرد دارد. تأیید اعتبار چندباره برای دریافت یک سرویس کاملاً منحصر به فرد، برای مشتری مسئولیت دارد، همچنین نیاز به نگهداری راه حل‌های احراز هویت و سوابق اعتبار خدمات منحصر به فرد وجود دارد. یک روش مقیاس‌پذیر می‌تواند مشتری را یکبار احراز هویت کند و در صورت موفقیت، نتایج احراز هویت و شناسایی و اعتبارات مشتری به تمام سرویس‌های مرتبطِ مبتنی بر یک رابطه معتبر (مطمئن) منتشر شود. بنابراین مشتری تنها یک بار احراز هویت می‌شود و هر سرویس منحصر به فرد، از مسئولیت احراز هویت مشتری و حفظ اطلاعات اعتبارات امنیت که برای هر کاربر ثبت شده است رهایی می‌یابد.

هدف اصلی راه حل‌های ورود تکی[۳]، حل این نوع مشکلات است. هر شخص یا سرویس تنها یکبار احراز هویت شود و دسترسی به طیف گسترده‌ای از خدمات آنلاین بدون نیاز به اعتبارسنجی و احراز هویت مجدد برای هر فرد امکان‌پذیر شود. حساسیت داده‌ها و حفظ حریم خصوصی اطلاعات به‌طور افزایشی به یک ناحیه نگرانی برای سازمان‌ها تبدیل می‌شود. جنبه‌های احراز هویت و اثبات هویت شامل استفاده، نگهداری و حفاظت از اطلاعات جمع‌آوری‌شده برای کاربران می‌باشد. جلوگیری از دسترسی غیرمجاز به منابع اطلاعات در ابر نیز یک عامل مهم است [۴ و ۲۴].

۱-۲۰-۲ تعریف

دو تعریف در زیر برای زبان نشانه‌گذاری اثبات امنیت ارائه‌شده است:

تعریف یک: زبان نشانه‌گذاری اثبات امنیت یک استاندارد مبتنی بر زبان نشانه‌گذاری توسعه‌پذیر برای ورود تکی مرورگر وب است و توسط کمیته فنی سرویس‌های امنیت سازمان گسترش استانداردهای اطلاعات ساختاریافته[۴] تعریف شده است. زبان نشانه‌گذاری اثبات امنیت پیچیده است و تنها شرکت‌های بزرگ می‌توانند هزینه سنگین استفاده و پیاده‌سازی زبان نشانه‌گذاری اثبات امنیت را توجیه کنند.

---

[۱] eXtensible Markup Language [۲] Simple Object Access Protocol [۳] Single Sign On
[۴] Organization for the Advancement of Structured Information Standards

تعریف دو: زبان نشانه‌گذاری اثبات امنیت یک چارچوب مبتنی بر زبان نشانه‌گذاری توسعه‌پذیر توسعه‌یافته توسط سازمان گسترش استانداردهای اطلاعات ساختاریافته برای تبادل اطلاعات ایمن بین بخش‌های مختلف استفاده می‌شود. این یک استاندارد باز است که برای تبادل اطلاعات ایمن بین محصولات مختلف مورد استفاده قرار می‌گیرد.

همه این موارد با ظهور محاسبات ابری و ارائه‌دهندگان مدیریت هویت مبتنی بر ابر مانند OneLogin در حال تغییر است. در حال حاضر هر کسی که استطاعت داشته‌باشد می‌تواند از زبان نشانه‌گذاری اثبات امنیت استفاده و در عرض چند دقیقه آنرا بارگذاری و اجرا کند. زبان نشانه‌گذاری اثبات امنیت توسط سازمان گسترش استانداردهای اطلاعات ساختاریافته توسعه‌یافته و یک چارچوب مبتنی بر زبان نشانه‌گذاری توسعه‌پذیر ارائه‌می‌دهد که هدف آن، امنیت تبادل اطلاعات است. با استفاده از اثبات‌های زبان نشانه‌گذاری اثبات امنیت، امنیت اطلاعات مربوط به یک موضوع در میان ارائه‌دهندگان سرویس در روش پلت‌فرم آگنوستیک به اشتراک گذاشته می‌شود. در خدمات وب، با استفاده از امنیت خدمات وب برای تامین امنیت پیام‌ها، زبان نشانه‌گذاری اثبات امنیت برای امنیت تبادل پیام میان سرویس‌های مختلف مورد استفاده قرار می‌گیرد. در زبان نشانه‌گذاری اثبات امنیت، مدل اطمینان مبتنی بر زیرساخت کلید عمومی[۱]برای ایجاد اطمینان استفاده می‌شود. به عنوان مثال، با امضای یک پیام با کلید خصوصی فرستنده، ثابت می‌شود که این پیام واقعاً توسط فرستنده فرستاده‌شده است. علاوه بر این، زیرساخت کلید عمومی برای توزیع کلید متقارن حفاظت‌شده توسط کلید عمومی گیرنده برای حل مشکل توزیع کلیدها با یک راه حل مقیاس‌پذیر استفاده می‌شود [۴].

زبان نشانه‌گذاری اثبات امنیت یک روش احراز هویت واقعی نیست بلکه ابزاری برای تبدیل واقعیت‌های موجود در مورد یک رویداد احراز هویت شده است. زبان نشانه‌گذاری اثبات امنیت می‌تواند در یک محیط ورود تکی مبتنی بر اینترنت به عنوان ابزاری برای انتقال اثبات‌های احراز هویت بین ارائه‌دهنده هویت و ارائه‌دهنده سرویس استفاده‌شود. زبان نشانه‌گذاری اثبات امنیت متکی بر مفهوم سرویس انتقال داخلی در ارائه‌دهنده هویت است. این سرویس، مسیریابی را از ارائه‌دهنده سرویس دریافت می‌کند، اطلاعات مورد نیاز برای ساخت اثبات‌های احراز هویت را نگاشت و کاربر را به ارائه‌دهنده سرویس جهت‌دهی می‌کند [۱۷]. زبان نشانه‌گذاری اثبات امنیت متشکل از تعدادی اجزای بلوک ساختمان است که هنگامی‌که به هم متصل می‌شوند، امکان پشتیبانی از تعدادی موارد استفاده را می‌دهد. مشخصات زبان نشانه‌گذاری اثبات امنیت، ساختار و محتوای اثبات‌ها، توضیحاتی در مورد یک اصل اثبات‌شده توسط یک بخش اثبات ارائه‌می‌دهد. این موارد توسط شمای زبان نشانه‌گذاری توسعه‌یافته تعریف شده است. اثبات‌ها یا درخواست‌شده هستند یا تنها برای ارائه‌دهنده سرویس بیان شده‌اند. پروتکل‌های زبان نشانه‌گذاری اثبات امنیت می‌توانند روی ارتباطات سطح پایین یا پروتکل‌های پیام (مانند پروتکل انتقال ابرمتن[۲] یا پروتکل دسترسی به شی ساده)، که توسط اتصالات تعریف شده‌اند، منتقل گردند. پروتکل‌ها و اتصالات زبان نشانه‌گذاری اثبات امنیت، همراه با ساختار اثبات‌ها برای ایجاد یک پروفایل با یکدیگر ترکیب می‌شوند. همچنین پروفایل‌های ویژگی نیز وجود دارد (برای مثال، پروفایل‌های LDAP و DCE)، که چگونگی تفسیر اطلاعات ویژگی که داخل یک اثبات انجام می‌شود را با استفاده از فناوری‌های ویژگی/دایرکتوری عمومی تعریف می‌کند. دو مولفه دیگر زبان نشانه‌گذاری اثبات امنیت در ساخت یک سیستم استفاده می‌شود:

فراداده: فراداده که چگونگی بیان و اشتراک‌گذاری اطلاعات مربوط به پیکربندی بین دو نهاد مرتبط را تعریف می‌کند. فراداده توسط شمای زبان نشانه‌گذاری توسعه‌یافته تعریف شده است. محل فراداده با استفاده از رکوردهای سرور نام دامنه[۳] تعریف شده است.

مفهوم احراز هویت: در بعضی موقعیت‌ها ارائه‌دهنده سرویس ممکن‌است تمایل به داشتن اطلاعات تکمیلی در تعیین صحت و محرمانگی اطلاعات درون یک اثبات داشته‌باشد. مفهوم احراز هویت اجازه تقویت اثبات‌ها با اطلاعات اضافی مربوط به اعتبار مدیر در ارائه‌دهنده‌ی شناسه مانند جزئیات احراز هویت چند عاملی را می‌دهد [۵ و ۲۵].

---

[۱] Public Key Infrastructure [۲] Hypertext Transfer Protocol [۳] Domain Name Server

۲-۲۰-۲ ویژگی‌ها

زبان نشانه‌گذاری اثبات امنیت ویژگی‌های متعددی دارد که در ادامه تعدادی از آنها آمده است.

مبتنی بر استانداردها: زبان نشانه‌گذاری اثبات امنیت مبتنی بر استاندارد است که قابلیت همکاری میان ارائه‌دهندگان هویت را تضمین می‌کند و شرکت‌ها برای انتخاب فروشنده آزادی عمل دارند.

قابلیت استفاده: دسترسی با یک کلیک از طریق پورتال یا اینترانت، ارتباط عمیق، حذف رمز عبور و تکرار جلسات خودکار باعث اجرای ساده‌تر برای کاربر می‌شود.

امنیت: مبتنی بر امضای دیجیتالی قوی برای احراز هویت و یکپارچگی است. زبان نشانه‌گذاری اثبات امنیت یک پروتکل ورود منحصربه‌فرد امن است که بزرگترین و اکثر شرکت‌های امنیتی در جهان به آن تکیه کرده‌اند.

سرعت: زبان نشانه‌گذاری اثبات امنیت سریع است. تغییر مسیر یک مرورگر، امنیت ورود یک کاربر به یک برنامه‌کاربردی را فراهم می‌کند.

پیشگیری از فیشینگ: اگر یک رمز عبور برای برنامه‌کاربردی وجود نداشته‌باشد، نمی‌توان با آن در یک صفحه ورود جعلی فریب زد.

موافق IT: زبان نشانه‌گذاری اثبات امنیت زندگی را برای IT آسان می‌کند، زیرا احراز هویت را متمرکز و وضوح بیشتری را فراهم می‌کند و یکپارچه‌سازی دایرکتوری را آسان‌تر می‌سازد [۲۶].

۳-۲۰-۲ اجزا

اجزای زبان نشانه‌گذاری اثبات امنیت و بخش‌های منحصربه‌فرد آن برای پشتیبانی از تبادل اطلاعات امن شامل اثبات‌ها، پروتکل‌ها، اتصالات و پروفایل‌ها می‌باشد که هر یک از آنها در ادامه توضیح داده شده‌اند:

اثبات‌ها

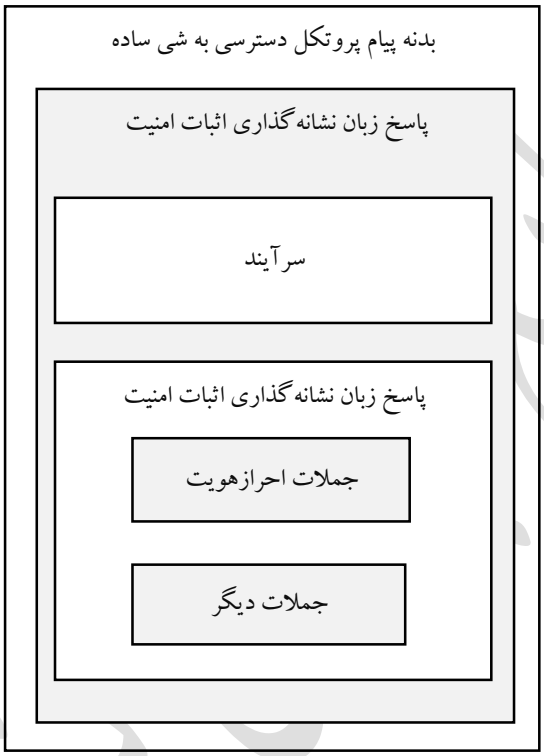
در هسته زبان نشانه‌گذاری اثبات امنیت، اثبات‌ها با یک بخش اثبات برای ارتباط احراز هویت، ویژگی‌ها و اطلاعات استحقاقی برای یک موضوع مشخص مورد استفاده قرار می‌گیرد. زبان نشانه‌گذاری اثبات امنیت یک چارچوب مستقل از پلت‌فرم و اساسی در پلت‌فرم مستقل از خصوصیات زبان نشانه‌گذاری توسعه‌پذیر می‌باشد. اثبات‌های زبان نشانه‌گذاری اثبات امنیت در میان سرویس‌های مختلفی که بر روی پلت‌فرم‌های مختلف در حال اجرا هستند مبادله می‌شود. به عبارت دیگر اثبات‌ها به زبان نشانه‌گذاری اثبات امنیت اجازه می‌دهد تا یک بخش، خصوصیات و ویژگی‌های یک نهاد را اثبات کند. برای مثال، یک اثبات زبان نشانه‌گذاری اثبات امنیت می‌تواند بیان کند که کاربر "John Doe" است، کاربر وضعیت "طلا" دارد، آدرس ایمیل کاربر john.doe@example.com است و کاربر عضو گروه "مهندسی" است. اثبات‌های زبان نشانه‌گذاری اثبات امنیت در شمای زبان نشانه‌گذاری توسعه‌پذیر کد گذاری شده است [۶]. زبان نشانه‌گذاری اثبات امنیت سه نوع جمله تعریف می‌کند که می‌تواند در اثبات انجام شود:

جملات احراز هویت: این جملات توسط بخش سوم انجام‌شده که با موفقیت کاربر را احراز هویت می‌کند. اینکه چه کسی اثبات را منتشر کرده، موضوع احراز هویت شده، مدت اعتبارسنجی و همچنین اطلاعات مربوط به احراز هویت دیگر را تعریف می‌کند. جملات احراز هویت برای ارائه‌دهنده سرویس اثبات می‌کند که مدیر، احراز هویت را با ارائه‌دهنده هویت در یک زمان خاص با استفاده از یک روش خاص احراز هویت انجام دهد.

جملات ویژگی: این جملات شامل اطلاعات خاصی در مورد کاربر (به عنوان مثال، که آنها وضعیت "طلا" دارد) می‌شود. یک جمله ویژگی ثابت می‌کند که یک موضوع با ویژگی‌های مشخص جمع‌آوری‌شده است.

جملات تصمیم مجوز: این جملات آنچه را که کاربر حق انجام آنها را دارد شناسایی می‌کند (برای مثال، آیا او مجاز به خرید یک آیتم مشخص شده می‌باشد). یک جمله تصمیم مجوز اثبات می‌کند که یک موضوع برای انجام فعالیت A روی منبع R با گواهی مشخص E مجاز است. جملات تصمیم احراز هویت پر معنی در زبان نشانه‌گذاری اثبات امنیت محدود هستند [۲۶].

اثبات متشکل از یک یا چند جمله است. برای ورود منحصربه‌فرد، معمولاً اثبات زبان نشانه‌گذاری اثبات امنیت شامل یک جمله احراز هویت منحصربه‌فرد و احتمالاً جمله ویژگی منحصربه‌فرد خواهدشد. شکل ۲-۵ یک اثبات زبان نشانه‌گذاری اثبات امنیت که در یک پاسخ زبان نشانه‌گذاری اثبات امنیت انجام‌شده و خود آن درون یک بدنه پروتکل دسترسی به شی ساده است را نشان می‌دهد.



شکل ۲-۵: ساختار اثبات زبان نشانه‌گذاری اثبات امنیت [۲۷].

شکل ۲-۶ یک نمونه اثبات با یک جمله احراز هویت تکی را نشان می‌دهد که جملات احراز هویت به صورت پررنگ نشان‌داده‌شده‌اند.

```
Version="2. 0" <saml: Assertion xmlns: saml="urn:oasis: names:tc:SAML:2. 0:assertion"
IssueInstant="2005-01-31T12:00:00Z">
 <saml:Issuer>
 www. acompany. com
 </saml:Issuer>
 <saml:Subject>
<saml:NameID Format="urn:oasis:names:tc:SAML:1. 1:nameid-format:emailAddress">
 j. doe@company. com
 </saml:NameID>
 </saml:Subject>
 <saml:Conditions NotBefore="2005-01-31T12:00:00Z"
 NotOnOrAfter="2005-01-31T12:00:00Z">
 </saml:Conditions>
 <saml:AuthnStatement
 AuthnInstant="2005-01-31T12:00:00Z" SessionIndex="67775277772">
 <saml:AuthnContext>
 <saml:AuthnContextClassRef>
```

```
urn:oasis:names:tc:SAML:2. 0:ac:classes:PasswordProtectedTransport
</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
</saml:Assertion>
```

شکل ۲-٦: اثبات زبان نشانه‌گذاری اثبات امنیت [۲۴].

عنصر <saml:Assertion> می‌تواند از جملات امنیت و اطلاعات اضافی محافظت کند. علاوه بر این زبان نشانه‌گذاری اثبات امنیت می‌تواند برای استفاده رسانه‌ها و وسایل انتقال اساسی توسط برخی از پروتکل‌های مفید پیش‌تعریف‌شده مانند پیاده‌سازی پروتکل ورود تکی محدود شود. پروتکل‌های پیش‌تعریف‌شده‌ی زبان نشانه‌گذاری اثبات امنیت، فایل‌های XSD ارائه‌می‌دهد که دقیقا ساختار پیام را تعریف می‌کنند. یکپارچگی و اعتبار پیام با استفاده از امضاهای دیجیتال اختیاری از طریق استاندارد امضای زبان نشانه‌گذاری توسعه‌پذیر به دست می‌آید، در حالیکه محرمانگی می‌تواند با استفاده از رمزگذاری اختیاری، با توجه به استاندارد رمزگذاری زبان نشانه‌گذاری توسعه‌پذیر ایجاد شود [۲۸].

پروتکل‌ها

پروتکل‌های زبان نشانه‌گذاری اثبات امنیت تعیین می‌کنند که چگونه عناصر زبان نشانه‌گذاری اثبات امنیت (مانند اثبات‌ها)، داخل عناصر درخواست و پاسخ زبان نشانه‌گذاری اثبات امنیت بسته‌بندی شوند و قوانین پردازش بیان می‌کند که موجودیت‌های زبان نشانه‌گذاری اثبات امنیت باید هنگام استخراج و مصرف از این عناصر دنبال شوند. زبان نشانه‌گذاری اثبات امنیت تعدادی از پروتکل‌های درخواست/پاسخ را تعریف می‌کند که در شمای زبان نشانه‌گذاری توسعه‌پذیر به عنوان مجموعه‌ای از جفت‌های درخواست/پاسخ کدگذاری شده است. مهمترین نوع درخواست پروتکل زبان نشانه‌گذاری اثبات امنیت، پرس‌و جو نامیده می‌شود. متناظر با سه نوع جملات، سه نوع پرس‌وجوی زبان نشانه‌گذاری اثبات امنیت وجود دارد:

- پرس‌وجوی احراز هویت
- پرس‌وجوی ویژگی
- پرس‌وجوی تصمیم مجوز

تعدادی از پروتکل‌های تعریف شده توسط زبان نشانه‌گذاری اثبات امنیت در زیر آمده‌اند:

پروتکل پرس‌وجو و درخواست اثبات: مجموعه‌ای از پرس‌وجوهایی که از طریق اثبات‌های زبان نشانه‌گذاری اثبات امنیت موجود به‌دست می‌آید را تعریف می‌کند. پرس‌وجو می‌تواند براساس یک مرجع، موضوع یا نوعی از جملات باشد.

پروتکل درخواست احراز هویت: پروتکلی تعریف می‌کند که توسط آن ارائه‌دهنده سرویس اثبات‌ها را از یک ارائه‌دهنده هویت، متناسب با نیازهای یک پروفایل زبان نشانه‌گذاری اثبات امنیت خاص مانند پروفایل ورود منحصر به فرد مرورگر وب درخواست می‌کند.

پروتکل تحلیل آرتیفکت:[۱] مکانیزمی ارائه‌می‌دهد که بوسیله آن پیام‌های پروتکل ممکن‌است توسط مرجع با استفاده از یک مقدار کوچک، با طول ثابت به نام آرتیفکت موافقت شود. دریافت‌کننده آرتیفکت از پروتکل آرتیفکت (ArtifactProtocol) برای تسلیم پیام پروتکل واقعی استفاده می‌کند.

پروتکل مدیریت شناسه نام: مکانیزم‌هایی برای تغییر مقدار و یا فرمت نام یک اصل فراهم می‌کند. صادرکننده درخواست می‌تواند ارائه‌دهنده سرویس یا ارائه‌دهنده هویت باشد. این پروتکل همچنین مکانیزمی برای پایان دادن به ارتباط بین نام یک ارائه‌دهنده هویت و ارائه‌دهنده سرویس فراهم می‌کند.

---

[۱] Artifact Resolution Protocol [۲] Single Logout Protocol

پروتکل خروج منحصربه‌فرد[۲]: یک درخواست تعریف می‌کند که اجازه خروج تقریباً همزمان همه‌ی جلسه‌های مرتبط با مدیر را می‌دهد. خروج از سیستم می‌تواند به‌طور مستقیم با مدیر یا به دلیل پایان زمان جلسه یا به دلیل اینکه حقوق دسترسی کاربر لغو شده است آغاز شود. خروج می‌تواند توسط سایت ارائه‌دهنده آغاز شود.

پروتکل نگاشت شناسه نام: ارائه مکانیزمی برای نگاشتِ برنامهِ شناسهِ نامِ زبان نشانه‌گذاری اثبات امنیت به دیگری برای کنترل‌های سیاسی مناسب [۶].

اتصالات

اتصالات زبان نشانه‌گذاری اثبات امنیت یک نگاشت از یک پیام پروتکل زبان نشانه‌گذاری اثبات امنیت روی فرمت‌های پیام استاندارد و/یا پروتکل‌های ارتباطی می‌باشد. پروتکل‌های نگاشت زبان نشانه‌گذاری اثبات امنیت برای تبادل درخواست/پاسخ به لایه‌های پایین‌تر انتقال استفاده می‌شوند. برای نمونه، اتصالات پروتکل دسترسی به شی ساده بیان می‌کند که چگونه پیام‌های درخواست و پاسخ زبان نشانه‌گذاری اثباتِ امنیتِ شرح داده‌شده در پروتکل‌های زبان نشانه‌گذاری اثبات امنیت می‌تواند با استفاده از تبادل پیام پروتکل دسترسی به شی ساده اجرا شود. به عبارت دیگر اتصالات دقیقاً چگونگی نگاشت‌های پروتکل زبان نشانه‌گذاری اثبات امنیت بر روی پروتکل‌های انتقال را شرح می‌دهد. برای مثال، مشخصات زبان نشانه‌گذاری اثبات امنیت، چگونگی انجام اتصال درخواست/پاسخ زبان نشانه‌گذاری اثبات امنیت با پیام‌های تبادل پروتکل دسترسی به شی ساده را فراهم می‌کند. اتصالات تعریف شده عبارتند از:

اتصال پروتکل دسترسی به شی ساده زبان نشانه‌گذاری اثبات امنیت: تعریف می‌کند که چگونه پیام‌های پروتکل زبان نشانه‌گذاری اثبات امنیت با پیام‌های پروتکل دسترسی به شی ساده منتقل شده است. همچنین تعریف می‌کند که چگونه پیام‌های پروتکل دسترسی به شی ساده روی پروتکل انتقال ابرمتن منتقل شده‌اند.

اتصال پروتکل دسترسی به شی ساده معکوس (PAOS): تبادل پیام پروتکل دسترسی به شی ساده/پروتکل انتقال ابرمتن چند مرحله‌ای را تعریف می‌کند که اجازه می‌دهد سرویس‌گیرنده‌ی پروتکل انتقال ابرمتن، پاسخگوی پروتکل دسترسی به شی ساده باشد. این اتصالات در پروفایل مشتری و پروکسی افزایش یافته مورد استفاده قرار می‌گیرد و به ویژه برای حمایت از دروازه‌های پروتکل برنامه‌های کاربردی بی‌سیم[۱] طراحی شده است.

اتصال مسیر مجدد پروتکل انتقال ابرمتن: تعریف می‌کند که چگونه پیام‌های پروتکل زبان نشانه‌گذاری اثبات امنیت می‌تواند با استفاده از پیام‌های مسیریابی مجدد پروتکل انتقال ابرمتن منتقل شود.

اتصال POST در پروتکل انتقال ابرمتن: تعریف می‌کند که چگونه پیام‌های پروتکل زبان نشانه‌گذاری اثبات امنیت می‌تواند درون محتوای کدگذاری‌شده‌ی مبنای ۶۴ کنترل فرم HTML منتقل شود.

اتصال آرتیفکت پروتکل انتقال ابرمتن: تعریف می‌کند چگونه یک رجوع به یک درخواست یا پاسخ زبان نشانه‌گذاری اثبات امنیت (مانند آرتیفکت) توسط پروتکل انتقال ابرمتن منتقل می‌شود. دو مکانیزم یا کنترل فرم HTML، یا یک رشته پرس‌وجو در URL را تعریف می‌کند.

اتصال شناسه منابع یکنواخت[۲] زبان نشانه‌گذاری اثبات امنیت: ابزاری برای بازیابی یک اثبات زبان نشانه‌گذاری اثبات امنیت با حل شناسه منابع یکنواخت تعریف می‌کند [۵، ۲۷، ۲۹ و ۳۰].

پروفایل‌ها

ترکیبی از اثبات‌ها، پروتکل‌ها و اتصالات را تعریف می‌کند که برای موارد استفاده خاص استفاده می‌شود. به عنوان مثال، یک پروفایل توکن زبان نشانه‌گذاری اثبات امنیت برای امنیت خدمات وب وجود دارد که چگونگی استفاده از اثبات‌های زبان

---

[۱] Wireless Application Protocol [۲] Uniform Resource Identifier

نشانه‌گذاری اثبات امنیت با امنیت سرویس‌های وب را تعریف می‌کند. به عبارت دیگر، پروفایل، هسته خصوصیات زبان نشانه‌گذاری اثبات امنیت را تعریف می‌کند که چگونه درخواست و پاسخ زبان نشانه‌گذاری اثبات امنیت منتقل می‌شود. نوعی پروفایل زبان نشانه‌گذاری اثبات امنیت، مجموعه‌ای از قواعد توصیف را تشریح می‌کند. همچنین پروفایل توصیف می‌کند چگونه اثبات‌های زبان نشانه‌گذاری اثبات امنیت همراه با اشیاء دیگر توسط یک بخش اصلی گنجانده شود و از بخش اصلی به یک بخش دریافت متصل‌شده و سپس در مقصد پردازش شود. نوع دیگری از پروفایل زبان نشانه‌گذاری اثبات امنیت مجموعه‌ای از محدودیت‌ها برای استفاده از پروتکل یا قابلیت اثبات زبان نشانه‌گذاری اثبات امنیت برای یک محیط خاص یا زمینه استفاده را تعریف می‌کند. بنابراین پروفایل‌ها ممکن‌است انتخاب را محدود سازند. برخی از آنها به‌طور خلاصه عبارتند از:

پروفایل ورود تکی مرورگر وب: مکانیزمی برای ورود تکی با مرورگرهای وب تغییرنیافته به ارائه‌دهندگان خدمات چندگانه با استفاده از پروتکل درخواست احراز هویت در ترکیب با مسیریابی مجدد پروتکل انتقال ابرمتن، پروتکل انتقال ابرمتن POST و اتصالات آرتیفکت تعریف می‌کند.

پروفایل مشتری و پروکسی افزایش‌یافته[1]: یک پروفایل پروتکل درخواست احراز هویت در رابطه با پروتکل دسترسی به شی ساده معکوس و اتصالات پروتکل دسترسی به شی ساده متناسب شده با مشتریان یا دستگاه‌های دروازه با دانش یک یا چند ارائه‌دهنده‌ی شناسه تعریف می‌کند.

پروفایل بازیابی ارائه‌دهنده هویت: یک مکانیزم احتمالی برای مجموعه‌ای از ارائه‌دهندگان هویت و سرویسِ مرتبط، برای به‌دست آوردن ارائه‌دهندگان هویت مورد استفاده توسط مدیر تعریف می‌کند.

پروفایل خروج منحصربه‌فرد: پروفایلی از پروتکل خروج منحصربه‌فرد زبان نشانه‌گذاری اثبات امنیت تعریف می‌کند. تعریف می‌کند چگونه اتصالات پروتکل دسترسی به شی ساده، مسیریابی مجدد پروتکل انتقال ابرمتن، پروتکل انتقال ابرمتن POST و اتصالات آرتیفکت پروتکل انتقال ابرمتن مورد استفاده قرار گیرد.

پروفایل مدیریت شناسه نام: تعریف می‌کند چگونه پروتکل مدیریت شناسه نام ممکن‌است با پروتکل دسترسی به شی ساده، مسیریابی مجدد پروتکل انتقال ابرمتن، پروتکل انتقال ابرمتن POST و اتصالات آرتیفکت پروتکل انتقال ابرمتن استفاده‌شود.

پروفایل حل آرتیفکت: تعریف می‌کند چگونه پروتکل حل آرتیفکت از اتصال همزمان، مثل اتصال پروتکل دسترسی به شی ساده استفاده کند.

پروفایل پرس‌وجو/درخواست اثبات: تعریف می‌کند چگونه پروتکل‌های پرس‌وجوی زبان نشانه‌گذاری اثبات امنیت (مورد استفاده برای به‌دست آوردن اثبات‌های زبان نشانه‌گذاری اثبات امنیت) از یک اتصال همزمان مانند اتصال پروتکل دسترسی به شی ساده استفاده کند.

پروفایل نگاشت شناسه نام: تعریف می‌کند چگونه پروتکل نگاشت شناسه نام از یک اتصال همزمان مانند اتصال پروتکل دسترسی به شی ساده استفاده می‌کند.

باید به یاد داشت که زبان نشانه‌گذاری اثبات امنیت، پایان کار با مجموعه‌ی اثبات‌ها، پروتکل‌ها، اتصالات و پروفایل‌ها نیست. بلکه برای انعطاف‌پذیری بیشتر طراحی شده است و بنابراین با نقاط توسعه‌پذیر در شمای زبان نشانه‌گذاری توسعه‌پذیر و همچنین دستورالعمل‌هایی برای طراحی سفارشی اتصالات و پروفایل‌های جدید در روشی برای تضمین حداکثر همکاری می‌آید. شکل ۲-۷ ارتباط بین اجزا را نشان می‌دهد.

---

[1] Enhanced Client or Proxy profile

۲-۲۱ زبان نشانه‌گذاری اثبات امنیت در امنیت سرویس‌های وب

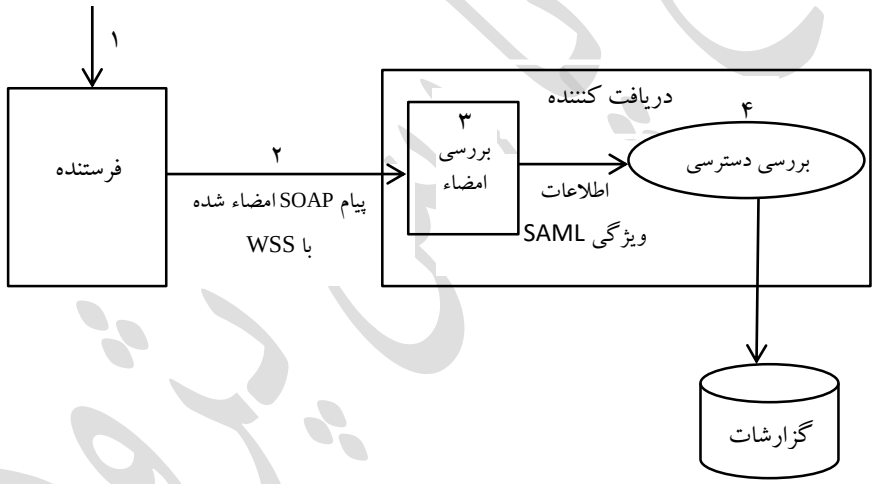
اثبات‌های زبان نشانه‌گذاری اثبات امنیت می‌تواند در سرویس‌های وب امن برای امنیت پیام‌های سرویس‌های وب مورد استفاده قرار گیرد که برای اتصال اطلاعات سرآیند امنیتی به درخواست‌های پروتکل دسترسی به شی ساده سرویس‌های وب بکار می‌رود. سرویس‌های وب امن، مجموعه‌ای از مشخصات است که ابزارهایی برای تامین حفاظت از امنیت پیام‌های پروتکل دسترسی به شی ساده تعریف می‌کند. امنیت پیام‌های پروتکل دسترسی به شی ساده سه جزء دارد: نشانه‌های احراز هویت، امضاهای دیجیتال و محرمانگی. سرویس‌های وب امن یک چارچوب انعطاف‌پذیر برای تبادل انواع مختلف نشانه‌های امنیتی شامل نشانه‌های نام‌کاربری/رمز عبور زبان نشانه‌گذاری توسعه‌پذیر و بلیط‌های کربروس ارائه می‌دهند [۲۱]. در [۱۷] خدمات اولیه‌ی ارائه‌شده‌ی سرویس‌های وب امن، احراز هویت، یکپارچگی و محرمانگی داده‌ها است. استاندارد سرویس‌های وب، استفاده از اثبات‌های زبان نشانه‌گذاری اثبات امنیت در قالب یک توکن امنیتی با پروفایل توکن زبان نشانه‌گذاری اثبات امنیت، سرویس‌های وب امن را تعریف می‌کند.

شکل ۲-۷: اجزای زبان نشانه‌گذاری اثبات امنیت [۲۴، ۲۷، ۳۱ و ۳۲].

زبان نشانه‌گذاری اثبات امنیت، روی اتصالات پروتکل دسترسی به شی ساده برای به‌دست‌آوردن اثبات‌های زبان نشانه‌گذاری اثبات امنیت از ارائه‌دهنده هویت استفاده می‌کند و زبان نشانه‌گذاری اثبات امنیت نمی‌تواند هیچ نقشی در حفاظت از پیام‌های پروتکل دسترسی به شی ساده بازی کند. در سرویس‌های وب امن، اثبات‌های زبان نشانه‌گذاری اثبات امنیتِ متعلق به هویت درخواست شونده قبلاً به دست آمده‌است. علاوه براین، در سرویس‌های وب امن، زبان نشانه‌گذاری اثبات امنیت می‌تواند نقش مهمی در حفاظت از خود پیام بازی کند. برای مثال، در یک توکن زبان نشانه‌گذاری اثبات امنیت با روش تصدیق دارنده کلید، کلید رمزنگاری برای تأیید موضوع استفاده می‌شود. حالت استفاده از زبان نشانه‌گذاری اثبات امنیت معمولی با استفاده از سرویس‌های وب امن به شرح زیر کار می‌کند:

- احراز هویت مشتری با یک سرویس توکن امنیتی[۱] برای درخواست یک توکن زبان نشانه‌گذاری اثبات امنیت. سرویس توکن امنیتی توسط مشتری و ارائه‌دهنده سرویس برای ارائه اعتبار تأیید شده است.
- سرویس توکن امنیتی، اثبات‌های زبان نشانه‌گذاری اثبات امنیت مورد نیاز برای انتقال و مسائل توکن امنیتی زبان نشانه‌گذاری اثبات امنیت را برای مشتری ایجاد می‌کند. سرویس توکن امنیتی، توکن را با کلید خصوصی خود رمز می‌کند و شامل گواهینامه X509 در توکن می‌شود.
- مشتری، یک توکن ایمن زبان نشانه‌گذاری اثبات امنیت به سرآیند سرویس‌های وب امنِ پیام پروتکل دسترسی به شی ساده اضافه می‌کند. سپس پیام پروتکل دسترسی به شی ساده را به ارائه‌دهنده سرویس می‌فرستد.
- سرویس تأیید می‌کند که توکن زبان نشانه‌گذاری اثبات امنیت می‌تواند قابل اطمینان باشد. برای انجام این کار، ابتدا گواهی سرویس توکن امنیتی موجود در توکن زبان نشانه‌گذاری اثبات امنیت در مقابل ذخیره مطمئن آن تأیید می‌شود. اگر گواهی، تأییدیه را گذراند، کلید عمومی گواهی X509 به منظور بررسی امضای دیجیتالی توکن مورد استفاده قرار می‌گیرد. ارائه‌دهنده سرویس، هویت موضوع را با استفاده از روش تأیید موضوع تأیید می‌کند که در توکن زبان نشانه‌گذاری اثبات امنیت از طریق اثبات تأیید موضوع مشخص شده است. در صورت معتبر بودن، برای دریافت دسترسی به منابع درخواست‌شده توسط مشتری اقدام می‌کند [۳۱ و ۳۲].

شکل ۲-۸ مراحل استفاده از اثبات‌های زبان نشانه‌گذاری اثبات امنیت با امنیت سرویس‌های وب را نشان می‌دهد.



شکل ۲-۸: استفاده‌ی عمومی از سرویس‌های امن وب و زبان نشانه‌گذاری اثبات امنیت [۳۲].

۱. فرستنده، اثبات زبان نشانه‌گذاری اثبات امنیت را توسط درخواست/پاسخ زبان نشانه‌گذاری اثبات امنیت یا سایر پروفایل‌های زبان نشانه‌گذاری اثبات امنیت به‌دست می‌آورد. اثبات‌ها شامل جملات ویژگی و روش تأییدیه موضوع دارنده کلید است.

۲. فرستنده، پیام پروتکل دسترسی به شی ساده که شامل سرآیند امنیت است را ایجاد می‌کند. اثبات‌های زبان نشانه‌گذاری اثبات امنیت در سرآیند امنیت وجود دارند. کلید که توسط اثبات‌های زبان نشانه‌گذاری اثبات امنیت برای ایجاد امضای دیجیتال روی داده‌ها در بدنه پیام استفاده‌شده است اشاره دارد. اطلاعات امضا در سرآیند امنیتی نیز گنجانده شده است.

۳. گیرنده، امضای دیجیتال را تأیید می‌کند.

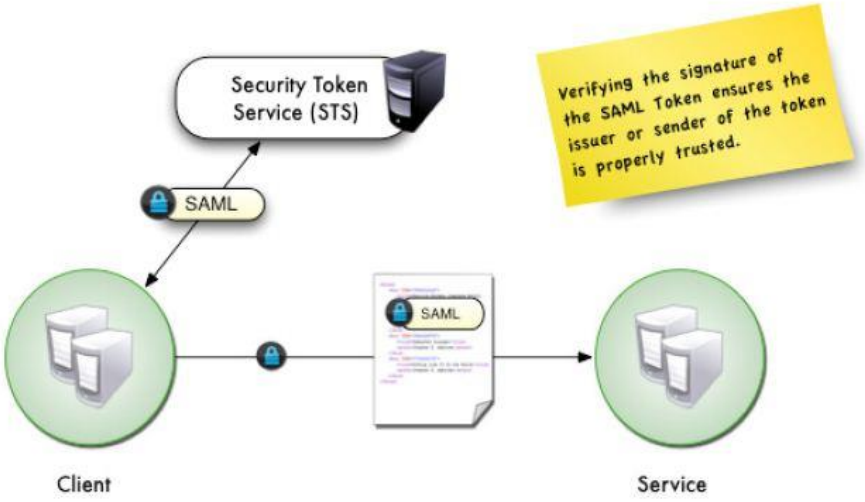
۴. اطلاعات، در اثبات زبان نشانه‌گذاری اثبات امنیت برای اهدافی مانند کنترل دسترسی و بررسی ورود به سیستم مورد استفاده قرار می‌گیرد.

---

[۱] Security Token Services

پروفایل توکن زبان نشانه‌گذاری اثبات امنیت سه روش تأیید موضوع را به منظور تأیید اعتبار توکن زبان نشانه‌گذاری اثبات امنیت تعریف می‌کند. هر یک از این روش‌ها، مجموعه‌ای از معیارها را برای تأیید این که اثبات‌های توکن زبان نشانه‌گذاری اثبات امنیت واقعاً با درخواست موضوع سرویس مرتبط است، دریافت می‌کند.

روش تأیید موضوع حامل[۱]: در این روش، توکن زبان نشانه‌گذاری اثبات امنیت حامل هویت و ویژگی‌های موضوع است. هیچ نیازی به بررسی درستی پروفایل وجود ندارد. همچنین فرض شده است که توکن قابل اطمینان است. با این حال اعتبارسنجی امضای زبان نشانه‌گذاری توسعه‌پذیر برای تأیید اینکه توکن توسط سرویس توکن امن ایجاد شده است توصیه می‌شود. به‌طور پیش فرض، سرور برنامه‌کاربردی وب به شرح زیر امضای دیجیتالی صادرکننده را تأیید و تصدیق می‌کند. این در حالاتی که در آن لایه سوکت‌های امنیتی[۲] برای تضمین امنیت بدست‌آوردن پیام در حالت نقطه به نقطه استفاده‌می‌شود بسیار مفید است. شکل ۲-۹ این موضوع را نشان می‌دهد.



شکل ۲-۹: روش تأیید موضوع حامل [۳۲].

روش تأیید موضوع دارنده کلید[۳]: در این روش، توکن زبان نشانه‌گذاری اثبات امنیت حامل هویت و صفات موضوع می‌شود و می‌تواند حفاظت از پیام را فراهم کند. گیرنده توکن نیازمند بررسی این است که توکن می‌تواند مطمئن باشد. به‌طور معمول چک کردن امضای دیجیتالی توکن با کلید خصوصی سرویس توکن امن انجام‌می‌شود. فرستنده توکن زبان نشانه‌گذاری اثبات امنیت، باید دانش یک کلید رمزنگاری مشخص شده در عنصر تأیید موضوع اثبات توکن زبان نشانه‌گذاری اثبات امنیت را داشته باشد و همچنین بتواند کلید را برای محافظت رمزنگاری پیام استفاده کند. هنگامی که کلید متقارن است، با استفاده از کلید عمومی گیرنده، رمزگذاری شده، به‌طوری که هنگامی که گیرنده، پیام را دریافت می‌کند می‌تواند آن را استخراج کند. فرستنده می‌تواند به صورت دیجیتالی پیام را با کلید متقارن امضا کند. هنگامی که گیرنده پیام را دریافت می‌کند، می‌تواند کلید متقارن موجود در عنصر تأیید موضوع توکن را با رمزگشایی محتوای آن با کلید خصوصی خود به دست آورد. پس از آن، گیرنده می‌تواند کلید را به منظور بررسی امضای دیجیتالی پیام استفاده کند و تأیید کند که فرستنده دارای کلید می‌باشد.

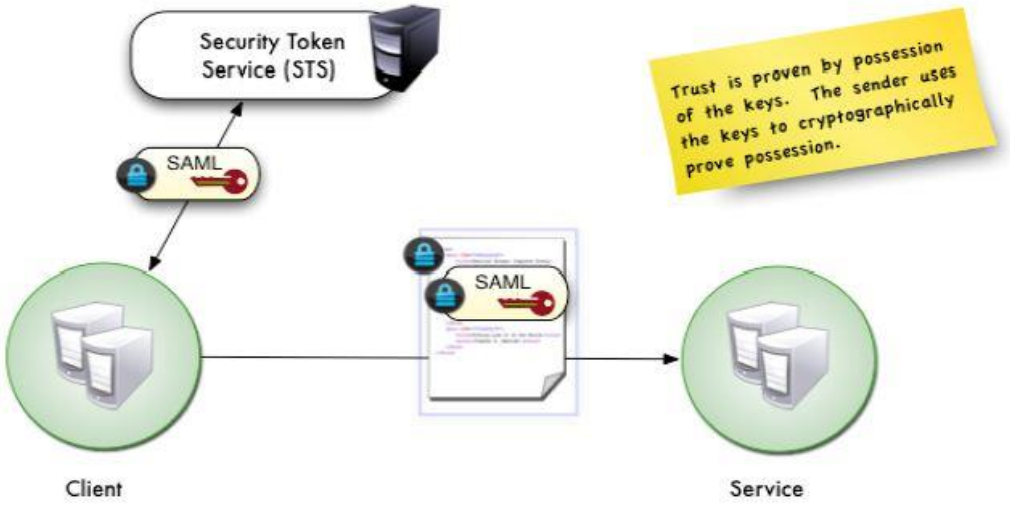
هنگامی که کلید نامتقارن است، عنصر تأیید موضوع شامل داده X509 یا ارزش کلید RSA از یک جفت نامتقارن است. کلید خصوصی این جفت نزد فرستنده و برای امضای دیجیتالی پیام استفاده‌می‌شود. هنگامی که گیرنده توکن را دریافت می‌کند،

---

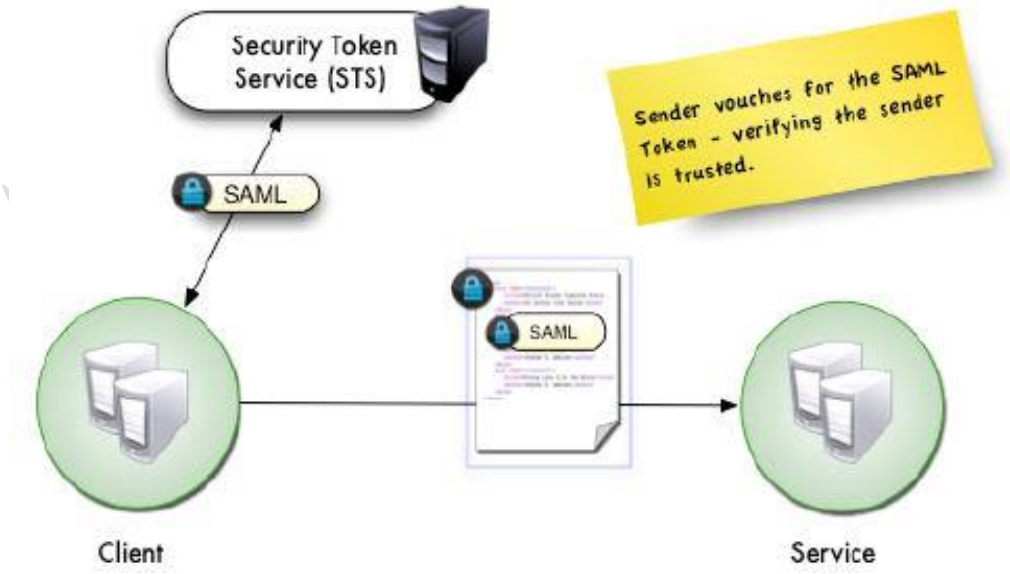
[۱] Bearer Subject Confirmation [۲] Security sockets layer [۳] Holder of Key Subject Confirmation

کلید عمومی را با استفاده از اطلاعات موجود در عنصر تأیید موضوع استخراج می‌کند و تأیید می‌کند که فرستنده کلید خصوصی جفت را دارد. شکل ۲-۱۰ این روش را نشان می‌دهد.

روش تأیید موضوع ضمانت‌های فرستنده: اگر چه این روش تأیید در حال حاضر توسط سرورهای برنامه‌های‌کاربردی وب جدید پشتیبانی نمی‌شود، اما سزاوار بحث است. در این روش، توکن زبان نشانه‌گذاری اثبات امنیت، هویت و ویژگی‌های موضوع را انجام می‌دهد. قابلیت پذیرش روش تأیید موضوع ضمانت‌های فرستنده توسط اینکه آیا فرستنده قابل اطمینان است اثبات شده است، به‌طوریکه فرستنده مسئولیت تأیید اعتبار توکن زبان نشانه‌گذاری اثبات امنیت را بر عهده دارد. فرستنده باید یکپارچگی پیام را برای اثبات این اطمینان محافظت کند. در این روش فرستنده همیشه نیازمند حفاظت از یکپارچگی توکن زبان نشانه‌گذاری اثبات امنیت است و دریافت‌کننده باید یکپارچگی را تأیید کند. شکل ۲-۱۱ این روش را نشان می‌دهد.



شکل ۲-۱۰: روش تأیید موضوع دارنده کلید [۳۲].



شکل ۲-۱۱: روش تأیید موضوع ضمانت‌های فرستنده [۳۱ و ۳۲].

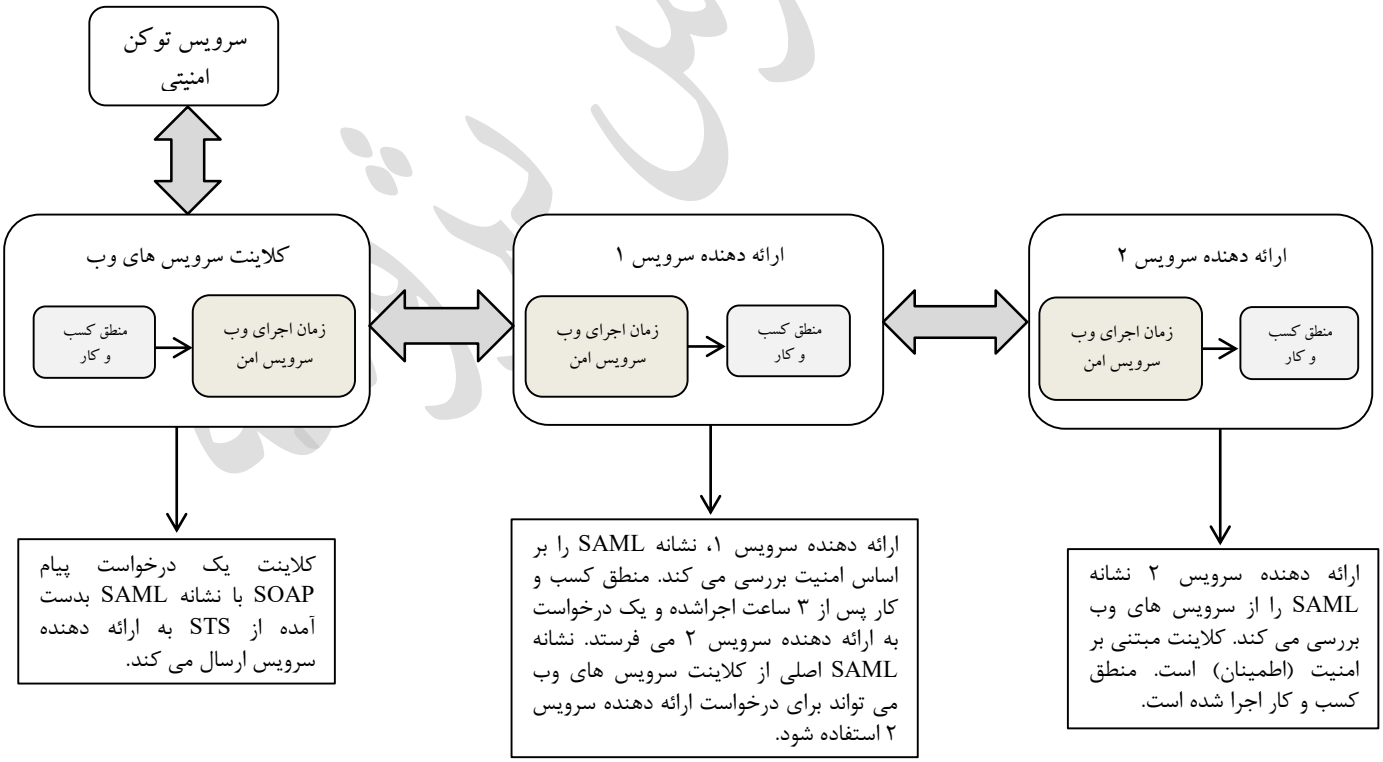
Sender-Vouches Subject Confirmation[۱]

پروتکل‌های زبان نشانه‌گذاری اثبات امنیت و سرویس‌های وب امن هنوز از ضعف‌های بومی مربوط به تکنولوژی‌های اصلی مانند فاش‌سازی مرورگر، کوکی‌ها، DNS و NTP رنج می‌برند. همچنین تهدیدهای اجتماعی مانند فیشینگ، وب سایت‌های کلاهبردار و ارائه‌دهندگان سرویس کلاهبردار وجود دارد. ارائه‌دهنده هویت یک نقطه اصلی حملات برای جمع‌آوری اعتبارات کاربر است. ارائه‌دهنده هویت می‌تواند با فریب، کاربران را به داخل وارد کند که می‌تواند به خوبی برای ورود تکی بکار گرفته شود. زبان نشانه‌گذاری اثبات امنیت و سرویس‌های وب امن افشاسازی را کاهش می‌دهند، بنابراین اعتبارات کاربر نیاز به ارسال به ارائه‌دهندگان سرویس شخصی ندارد.

۲-۲۲ انتشار توکن زبان نشانه‌گذاری اثبات امنیت در سرویس‌های وب

همان‌طور که پیش از این بحث شد، مشتری‌های سرویس‌های وب می‌توانند یک توکن زبان نشانه‌گذاری اثبات امنیت از سرویس توکن امنیت[۱] بدست آورند که دارای هویت و ویژگی‌های امنیتی آن است. سپس مشتری می‌تواند توکن زبان نشانه‌گذاری اثبات امنیت را روی یک درخواست برای یک ارائه‌دهنده سرویس ارسال کند. سرویس قصد اعتبارسنجی توکن را دارد که توسط صادرکننده به‌طور مطمئن امضا شود و ویژگی‌های هویت و امنیتی را از توکن به دست آورد. ارائه‌دهنده سرویس تمایل دارد از یک یا چند ارائه‌دهنده سرویس برای تکمیل منطق کسب‌وکار خود استفاده کند.

به جای نیاز مشتری به سرویس توکن امنیت برای تأیید هویت، هر یک از این سرویس‌ها می‌تواند راه حل بهتری برای سرویس برای اولین انتشار توکن زبان نشانه‌گذاری اثبات امنیت هنگامی که نیازهای خود را برای سرویس‌های دیگری ایجاد می‌کند بکار برد. توکن زبان نشانه‌گذاری اثبات امنیت در حال حاضر شامل ویژگی‌های امنیتی هویت و تصدیق است و می‌تواند به خدمات پایین دست منتشر شود. شکل ۲-۱۲ این سناریو را نشان می‌دهد:

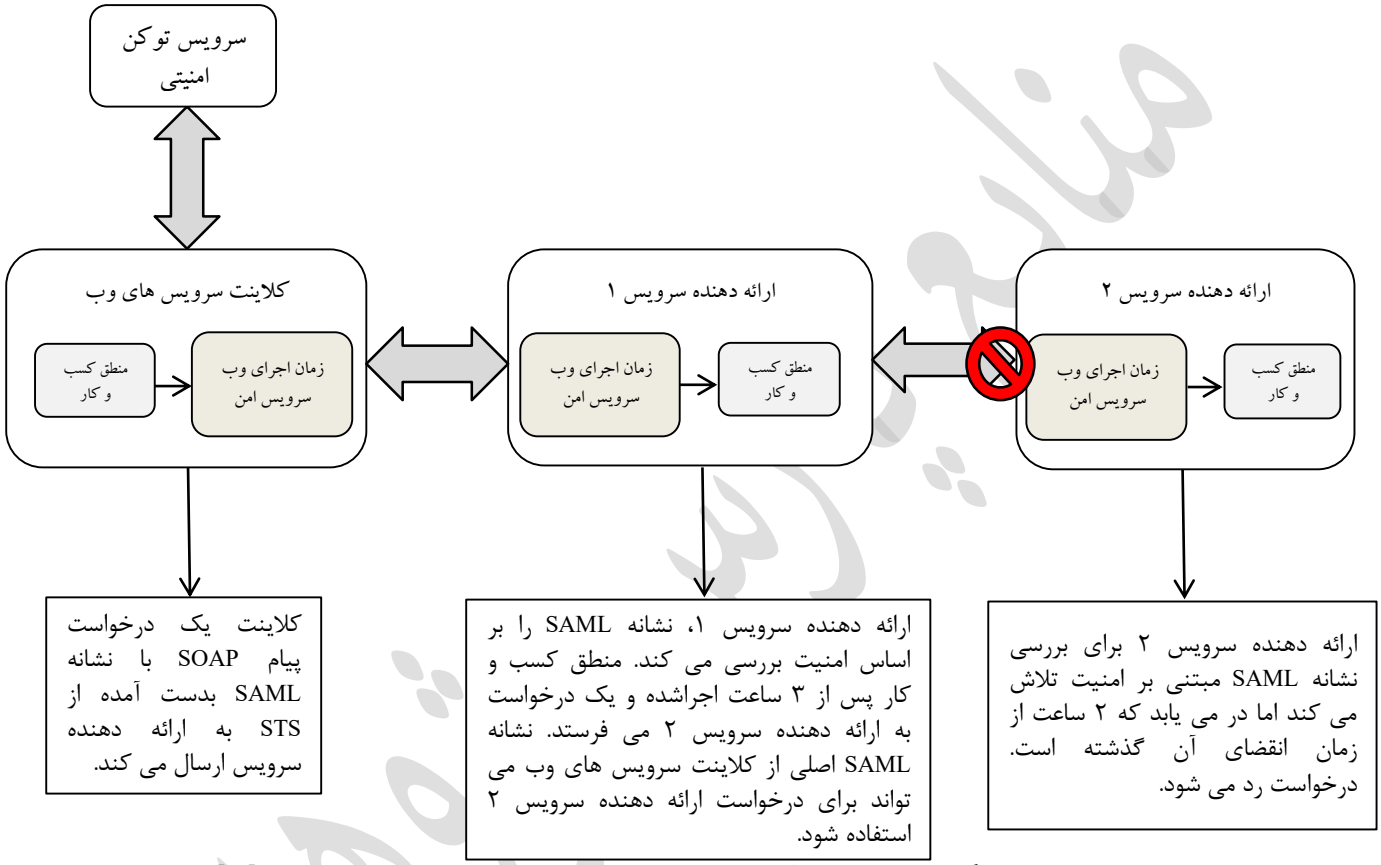


شکل ۲-۱۲: توزیع توکن زبان نشانه‌گذاری اثبات امنیت با استفاده ورود تکی [۳۲].

---

[۱] Security Token Service

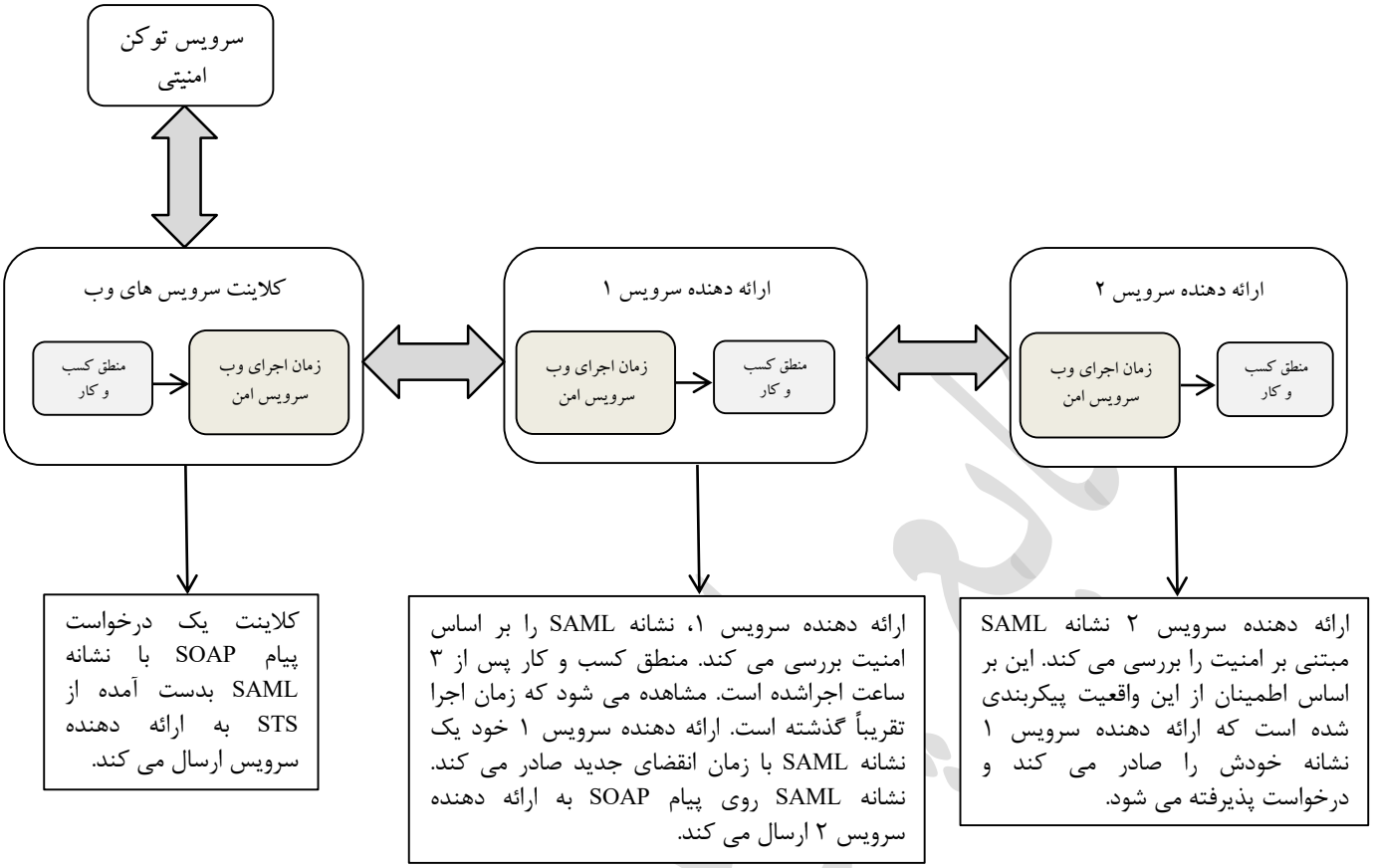
توانایی انتشار توکن زبان نشانه‌گذاری اثبات امنیت برای مشتری اصلی، راه حل‌های امنیتی پایان به پایان فراهم می‌کند. با این حال، یکی از عواملی که باید در نظر گرفته شود زمان انقضای توکن زبان نشانه‌گذاری اثبات امنیت است و چه زمانی برای همه‌ی سرویس‌های پایین دست برای پردازش، درخواست می‌گردد. اگر یک سرویس بیش از حد برای اجرای منطق کسب‌وکار خود طول بکشد، ممکن است توکن قبل از انتشار به یک سرویس منقضی شود. این فرایند در شکل ۲-۱۳ نشان‌داده‌شده است. یک راه حل، پیکربندی سرویس توکن امنیت برای صدور یک توکن زبان نشانه‌گذاری اثبات امنیت با زمان انقضای طولانی‌تر است. اگر زمان احضار کل درخواست به خوبی شناخته‌شده‌باشد، این راه حل ممکن است کار کند. با این حال، در واقع، زمان احضار کل درخواست غیرقطعی است.



شکل ۲-۱۳: توکن زبان نشانه‌گذاری اثبات امنیت یکسان برای ارائه‌دهنده سرویس شماره دو توزیع و منقضی شده [۳۲].

صدور مجدد توکن زبان نشانه‌گذاری اثبات امنیت یک راه حل ممکن است. در این صورت، هنگامی که یک سرویس در حال انتشار توکن زبان نشانه‌گذاری اثبات امنیت است، زمان انقضای اصلی را بررسی می‌کند. اگر مشخص شود که زمان انقضا تمام شده و یا نزدیک به انقضا است، سرویس، خودش، می‌تواند توکن زبان نشانه‌گذاری اثبات امنیت جدید با کپی اثبات و ویژگی‌های امنیتی توکن زبان نشانه‌گذاری اثبات امنیت اصلی، با زمان انقضای جدید صادر کند. سرویس دوم می‌تواند این توکن زبان نشانه‌گذاری اثبات امنیت خود صدور جدید با زمان انقضای جدید را بپذیرد که این بدان معنی است که یک تغییر در رابطه مطمئن بین سرویس‌ها وجود دارد. توکن زبان نشانه‌گذاری اثبات امنیت برای سرویس توکن امنیت در میان خدمات منتشر شده باعث می‌شود ویژگی‌های امنیت هویت و اعتبار موضوع در توکن نیز منتشر شوند. این کار این امکان را فراهم می‌کند که هر یک از بخش‌ها در اطمینان سرویس توکن امنیت درگیر شوند. با این حال، در این مورد این رابطه مطمئن تغییر کرده است، چرا که یک

سرویس زبان نشانه‌گذاری اثبات امنیت، توکن خود صدور می فرستد، سرویس دریافت کننده باید از سرویس فرستنده برای پذیرش توکن خود صدور مطمئن شود، نه سرویس توکن امنیت. این فرایند در شکل ۲-۱۴ نشان‌داده‌شده است.



شکل ۲-۱٤: زمان انقضای توکن زبان نشانه‌گذاری اثبات امنیت [۴، ۳۱ و ۳۳].

۲-۲۳ نتیجه‌گیری

برای درک کامل مسائلی که در فصل‌های آینده مورد بحث قرار گرفته‌است، نیاز به یک آشنایی اولیه با مفاهیم و تعاریف اولیه، احساس می‌شد. در این فصل مفاهیم و تعاریف اولیه مرتبط با پردازش ابری، احراز هویت، زبان نشانه‌گذاری اثبات امنیت و نیز آشنایی کلی با مفاهیم مورد استفاده بدست آمد. همچنین بررسی مختصری در مورد استاندارد زبان نشانه‌گذاری اثبات امنیت انجام‌شد که در فصل‌های بعدی از آنها استفاده خواهد شد.

فصل سوم
بررسی و تجزیه تحلیل کارهای انجام‌شده

۳-۱ مقدمه

در این فصل به مرور و بررسی کارهای انجام‌شده در زمینه امنیت محاسبات ابری، روش‌های ورود تکی، مزایا، معایب و امنیت آنها پرداخته شده است. در نهایت یکی از روش‌های ورود تکی به‌طور اجمالی مورد بررسی قرار خواهد گرفت. با وجود نو بودن بحث محاسبات ابری، تاکنون روش‌های زیادی برای ورود تکی ارائه و کارهای زیادی در این زمینه انجام‌شده است. فرایند ورود تکی از سال ۱۹۸۳ توسط موسسه فناوری ماساچوست برای یکپارچگی شبکه‌های کامپیوتری در پروژه آتن به منظور یکپارچگی ورود تکی، سیستم‌های فایل شبکه شده، محیط گرافیکی متحدشده و سرویسِ قرار دادن نام آغاز گردید. در زیر به بررسی تعدادی از کارهای انجام شده در این زمینه پرداخته شده است و مقایسه‌ای بین این روش‌ها انجام گرفته‌است. در نهایت یک مدل ورود تکی مبتنی بر ابر امن‌تر پیشنهاد شده است. مدل پیشنهادی با بررسی وکمک روش‌های ارائه‌شده قبلی ارائه‌شده است. مدیریت نام‌های‌کاربری و رمز عبورهای چندگانه تنها یک جنبه رنجش‌آور از اینترنت کنونی نیست، بلکه یکی از مهمترین ضعف‌های امنیتی است. هر سیستم نیازمند اینست که مشتری، برای دسترسی به سرویس‌ها خودش را ثبت کند، اما بیشتر اوقات یک کاربر در وب‌سایت‌های مختلفی با یک نام مشابه و رمز عبورهای بسیار مشابه ثبت شده است. این یک فعالیت امن نیست به عبارت دیگر یا کاربران اغلب نام‌کاربری و رمز عبور خود را فراموش می‌کنند و سیستم مدیریت کاربر یک ایمیل رمزگذاری نشده با داده‌های محرمانه ارسال می‌کند [۴].

۳-۲ سیستم‌های ورود تکی

۳-۲-۱ سازمانی

مانند بیشتر سیستم‌های ورود تکی، سیستم‌های ورود تکی سازمانی برای کاهش زمانی که یک کاربر برای ورود اعتباراتش برای ورود به برنامه‌های‌کاربردی مختلف دارد، طراحی شده‌اند. این کار با استفاده از تکنیک پُرکردن خودکار رمز عبورها برای کاربر انجام‌می‌شود، بنابراین آنها نیاز به وارد کردن دستی آنها ندارند. راه حل‌های ورود تکی معمولاً مبتنی بر نرم‌افزار هستند که همراه با کاربر برای ایجاد دسترسی به برنامه‌های‌کاربردی به‌طور ساده حرکت می‌کنند و از روش‌های احراز هویت مبتنی بر سخت‌افزارهای‌پیچیده دور می‌مانند. ورود تکی با ذخیره مجموعه‌های چندگانه اعتبارات فعالیت می‌کند که برای هر برنامه‌کاربردی یکبار به یاد آورده‌می‌شود و کاربر نیاز به دانستن آنها ندارد. به عبارت دیگر، برای افزایش سطح امنیت، پس از اینکه این اعتبارات داخل ورود تکی بدست‌می‌آیند، پیشنهادهایی برای افزایش نقش و سیاست‌های قدرت رمز عبورها، برای تقویت اعتبارات برای هر برنامه‌کاربردی ارائه می‌شود و حدس زدن آن برای مهاجم سخت‌تر می‌شود.

۳-۲-۲ مجتمع (فدرالی شده)

مدیریت هویت مجتمع برای سازمان‌های مجاز و ارائه‌دهندگان سرویس برای تبادل آسان اطلاعات در سرتاسر کانال‌های مختلف مانند بخش‌های مختلف دیگر، همکاران، ریسیلرها و مشتریانِ مهم است که اجازه می‌دهد پروفایل یک کاربر تکی، کاربر را در سرتاسر برنامه‌های کاربردی نامتجانس در زیرساخت‌های محلی و همچنین منابع مبتنی بر اینترنت کنترل‌شده توسط بخش‌های سوم مطمئن (امن شده) احراز هویت کند. درک این موضوع مهم است که اطمینان بین شرکت‌ها برای یک برنامه‌کاربردی کنترل‌شده توسط شرکت A که اجازه احراز هویت برای یک کاربر در شرکت B را می‌دهد، کسب شود. در این حالت، کاربر تنها یک پروفایل کاربر تکی را درون شرکت B نگه‌می‌دارد و اطمینان بدست‌آمده اجازه می‌دهد به‌طور خودکار وارد برنامه‌کاربردی شرکت A شده و از آن استفاده کند [۳۴ و ۳۵].

۳-۳ روش‌های ورود تکی

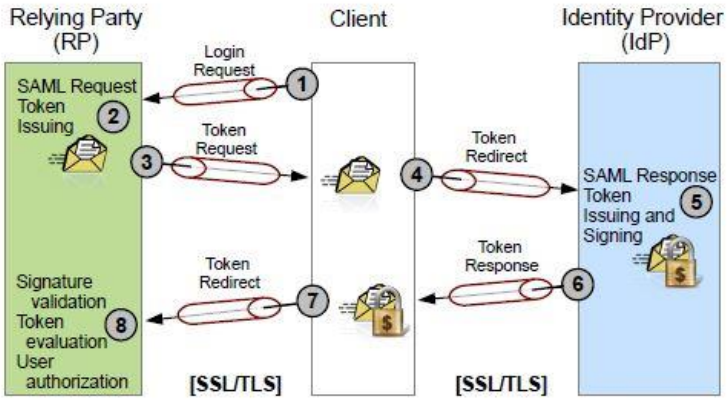
پروتکل‌های ورود تکی با توانمندی شرکت‌ها برای بدست‌آوردن یک محیط متحدشده مشکل را حل می‌کنند به این صورت که مشتریان یک مرتبه به محیط وارد می‌شوند و در عین حال قابلیت دسترسی به سرویس‌های ارائه‌شده توسط شرکت‌های مختلف را دارند. پروفایل ورود تکی مرورگر وب زبان نشانه‌گذاری اثبات امنیت یک استاندارد نوظهور در این متن است که یک فرمت مبتنی بر XML برای رمزگذاری اثبات‌های امنیتی تعریف می‌کند. همچنین تعدادی از پروتکل‌ها و اتصالات را تعریف می‌کند که توضیح می‌دهد چگونه اثبات‌ها باید در برنامه‌های کاربردی گوناگون و/یا سناریوهای گسترش مبادله شوند.

با توجه به افزایش روزافزون استفاده از اینترنت و فراگیر شدن خدمات وب و رایانش ابری، ورود کاربران به سایت‌ها و استفاده از خدمات مورد نیازشان به یک موضوع مهم تبدیل شده است. کاربران اینترنت معمولاً هویت‌های زیادی را برای برنامه‌های کاربردی وب مختلف مدیریت می‌کنند. برای حل این مشکل، ورود تکی توسعه یافته‌بود. در این روش، کاربران تنها یکبار برای ارائه‌دهنده هویت قابلِ اطمینان، احراز هویت می‌شوند. پس از ورود موفق کاربر، ارائه‌دهنده هویت نشانه‌های امنیتی مورد تقاضا را صادر می‌کند. این نشانه‌ها برای احراز هویت بخش‌های وابسته استفاده می‌شوند. یک حالت ورود تکی ساده در شکل ۳-۱ نشان‌داده‌شده است. در این شکل، کاربرِ وارد شده، ابتدا توسط ارائه‌دهنده هویت، بخش وابسته خواسته‌شده را ملاقات می‌کند. بخش وابسته یک درخواست نشانه صادر می‌کند. این نشانه به کاربر فرستاده می‌شود که کاربر آنرا به ارائه‌دهنده هویت ارسال می‌کند. ارائه‌دهنده هویت یک پاسخ نشانه شامل چندین درخواست (مانند حق دسترسی یا زمان انقضا) برای کاربر صادر می‌کند. با توجه به محافظت از احراز هویت و یکپارچگی درخواست‌ها، نشانه امضا شده است. در نتیجه، نشانه به کاربر فرستاده می‌شود که کاربر آنرا به بخش وابسته ارسال می‌کند. بخش وابسته امضا را اعتبارسنجی می‌کند و سپس دسترسی به سرویس یا منبع محافظت‌شده را اگر کاربر احراز هویت شده‌باشد، تصدیق می‌کند. این تصمیم کنترل دسترسی مبتنی بر درخواست‌ها در نشانه معتبر است.

ورود تکی مبتنی بر کوکی[۱] کوکی‌های HTTP مبتنی بر وب برای انتقال اعتبارات کاربر از مرورگر وب به سرور بدون ورودی از کاربر فعالیت می‌کنند. اعتبارات روی ماشین کلاینت جمع‌آوری شده‌اند و قبل از ذخیره در کوکی و ارسال به سرور مقصد، رمزگذاری شده‌اند. سرور کوکی‌ها را دریافت می‌کند، اعتبارات را استخراج و رمزگشایی و آنها را در مقابل دایرکتوری سرور داخلی کاربران اعتبارسنجی می‌کند. ورود تکی مبتنی بر کوکی برای محل‌هایی است که از قبل یک مدل احراز هویت با استفاده از یک جلسه مرورگر/ورود در سازمان وجود دارد. در برخی موارد، سیستم ممکن است از یک مدل کوکی مشترک برای تعیین اینکه آیا یک کاربر احراز هویت شده است یا نه استفاده کند.

---

[۱] Cookie-based SSO



شکل ۳-۱: حالت ورود تکی ساده [۳۴].

مراحل پیاده‌سازی ورود تکی مبتنی بر کوکی به صورت زیر است:

۱. سیستم احراز هویت (پس از ورود کاربر) باید یک کوکی سطح جلسه (هنگامی که مرورگر بسته و منقضی شد) و یک کوکی سطح دامنه تنظیم کند. نامگذاری کوکی برای فراخوانی به صورت دلخواه است. مقدار کوکی باید یک رشته رمزگذاری شده DES و کدگذاری مبنای ۶۴ آدرس ایمیل کاربر باشد.

- کوکی سطح دامنه (دامنه= mycompany.com)
- کوکی سطح جلسه (مهلت=هنگامی که مرورگر بسته شد)
- نام کوکی (اختیاری)
- مقدار کوکی (رشته کدگذاری‌شده DES و کدگذاری مبنای ۶۴ آدرس ایمیل کاربر)

۲. تنظیم پورتال با یک URL دامنه سفارشی (ideas.mycompany.com)

۳. تغییر تنظیمات روی پورتال برای انجام ورود تکی مبتنی بر کوکی.

۴. اطمینان از انجام موارد زیر:

- احراز هویت URL: URLی که سیستم را به یک کاربر که بدون یک کوکی به محل می‌آید جهت‌دهی مجدد می‌کند. این معمولاً صفحه ورود کاربر به اینترانت/سایت است.
- نام سایت: نام کوکی که در گام ۱ بالا استفاده‌شده است [۳۴، ۳۵ و ۳۶].

ورود تکی مبتنی بر کربروس[۱]: کربروس‌ها یک کاربر را قادر به ورود (لاگین) درون پنجره‌های دامنه حساب‌هایشان می‌کنند و سپس ورود تکی را برای برنامه‌های‌کاربردی داخلی آنها دریافت می‌کنند. کربروس نیاز به اتصال کاربر به یک مرکز توزیع کلید مرکزی[۲] (KDC) دارد. در پنجره‌ها، هر کنترل‌کننده دامنه اکتیو دایرکتوری همانند یک KDC عمل می‌کند. کاربران خودشان را برای سرویس‌ها (مثلاً سرورهای وب) احراز هویت می‌کنند، در ابتدا برای KDC احراز هویت می‌شوند، سپس بلیط‌های سرویس رمزگذاری شده از KDC را برای یک سرویس خاص که قصد استفاده از آن را دارند درخواست می‌کنند که به‌طور خودکار در همه مرورگرهای مهم با استفاده از SPNEGO[۳] رخ می‌دهد [۳۴ و ۳۵].

تکه‌تکه کردن صفحه[۴]: تکه‌تکه‌کردن صفحه به تشخیص و به‌خاطرآوردن جعبه‌های گفتگو (دیالوگ) گفته‌می‌شود که کاربران برای اعتباراتشان بکار می‌گیرند. ایده برش فیلدها و طرح‌بندی این گفتگوها و وارد کردن خودکار اعتبارات کاربر، اساس پشت این نوع از ورود تکی است.

---

۱ Kerberos-based SSO ۲ Key Distribution Center ۳ Simple and Protected GSSAPI Negotiation Mechanism
۴ Screen Scraping

تکه‌تکه‌کردن صفحات مبتنی بر وب، اصطلاحی است که به توانایی پورتال برای جذب یک صفحه وب درست و کامل یا بخش‌های خاصی از یک صفحه وب به درون یک پنجره پورتال اشاره‌می‌کند. معمولاً این کار با یک برنامه‌کاربردی انجام‌می‌شود که تگ‌های HTML را تجزیه و یک صفحه وب تولیدمی‌کند و اجازه می‌دهد بخش‌های خاص به داخل کشیده‌شوند. این شکل از یکپارچه‌سازی اجازه سفارشی‌سازی بزرگتر محتوای پورتال با همکاری محتوای استاتیک منابع مبتنی بر وب دیگر را می‌دهد. با این وجود، تکه‌تکه‌کردن صفحه یک واسط انعطاف‌پذیرتری ایجاد می‌کند، در حالی که یکپارچه‌سازی به دانش موقعیت عناصر داده روی صفحه وابسته است. حتی به‌روزرسانی‌ها یا تغییرات کوچک به یک وب سایت می‌تواند باعث شکست یکپارچه‌سازی شود [۳۴ و ۳۵].

ورود تکی مبتنی بر درخواست‌ها[1] درخواست‌ها توسط یک صادرکننده درخواست ایجاد شده‌اند که توسط بخش‌های چندگانه مطمئن و امن شده‌اند. درخواست‌ها معمولاً درون یک نشانه‌ی امضاشده‌ی دیجیتال، بسته‌بندی شده‌اند که می‌توانند با استفاده از زبان نشانه‌گذاری اثبات امنیت روی شبکه فرستاده شوند.

ورود تکی مبتنی بر درخواست به صورت زیر عمل می‌کند:

۱. کاربر به برنامه‌کاربردی بخش متکی دسترسی پیدا می‌کند.

۲. در حالی که کاربر احراز هویت نشده است، برنامه‌کاربردی بخش متکی کاربر را به سمت ارائه‌دهنده هویت مطمئن خودش می‌فرستد (ارائه‌دهنده مجتمع احراز هویت شده).

۳. ارائه‌دهنده مجتمع، خودش یک ارائه‌دهنده هویت نیست و به ارائه‌دهندگان هویت متعدد وابسته است. بنابراین لیستی از ارائه‌دهندگان هویت را برای احراز هویت کاربر بدست می‌آورد.

۴. کاربر یک لیست از ارائه‌دهندگان هویت مطمئن بدست می‌آورد و یک ارائه‌دهنده هویت انتخاب می‌کند (که یک اکانت دارد) و خودش را احراز هویت می‌کند. پس از یکبار احراز هویت، یک نشانه برای کاربر توسط ارائه‌دهنده هویت انتخاب‌شده صادر می‌شود و به ارائه‌دهنده یکپارچه عبور داده‌می‌شود.

۵. همان‌طور که ارائه‌دهنده مجتمع از ارائه‌دهنده هویت مطمئن است، می‌تواند نشانه را پیدا کند. ابتدا نشانه را بررسی می‌کند و اگر نیاز باشد آنرا رمزگشایی می‌کند. سپس آنرا بررسی می‌کند و نشانه وارد شونده را می‌خواند و یک نشانه جدید صادر می‌کند و درخواست‌ها را از نشانه ارائه‌دهنده هویت با استفاده از قوانین درخواست به نشانه جدید منتقل می‌کند.

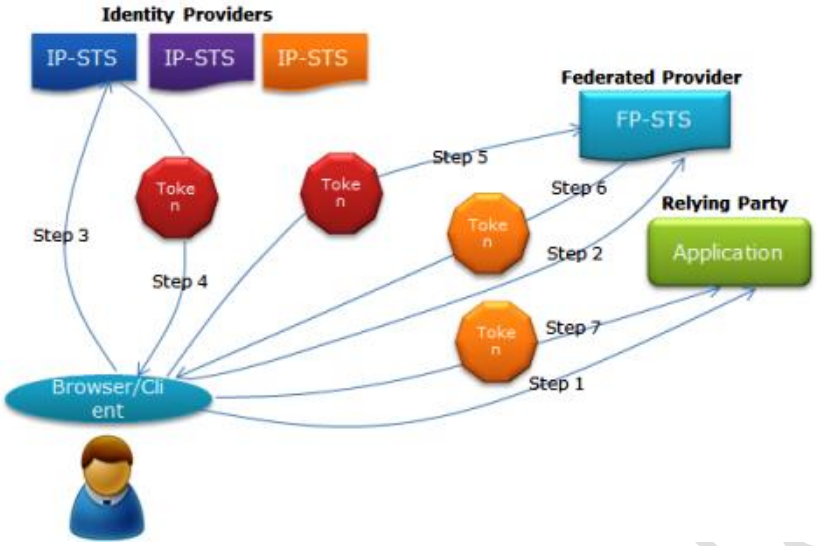
۶. نشانه جدید به برنامه‌کاربردی بخش متکی عبور داده‌می‌شود.

۷. نشانه به بخش وابسته فرستاده شده است. همان‌طور که بخش متکی از ارائه‌دهنده مجتمع مطمئن است، می‌تواند نشانه را پیدا کند و آن را بررسی کند و تصدیق یکباره موفقیت‌آمیز باشد، که اجازه دسترسی به برنامه‌کاربردی را می‌دهد.

فرایند بالا در پشت صحنه انجام می‌شود و کاربر نیاز به دقت در مورد آن ندارد. کاربر تنها نیاز به انتخاب یکی از ارائه‌دهندگان هویت لیست شده، انتخاب و بکار بردن اعتبارات برای احراز هویت دارد. شکل ۳-۲ این فرایند را نشان می‌دهد. در سناریو بالا، ۲ ارائه‌دهنده هویت وجود دارد. ارائه‌دهنده اول نشانه را با درخواست‌ها به ارائه‌دهنده دیگر می‌فرستد. اکنون ارائه‌دهنده دوم یک گزینه برای انتقال مانند حذف یک درخواست، یک درخواست جدید، تغییر دو یا چند درخواست به یک درخواست، تفکیک یک درخواست به دو یا چند درخواست و غیره دارد که می‌تواند مبتنی بر درخواست انجام شود (مانند ارائه‌دهنده مجتمع سرویس کنترل دسترسی ویندوز آژور) [۳۴، ۳۵ و ۳۷].

---

[1] Claim-based SSO



شکل ۳-۲: ورود تکی مبتنی بر درخواست [۳۴].

ورود تکی مبتنی بر کارت هوشمند[۱] با ورود تکی کارت هوشمند، کاربر نیاز به وارد کردن کارت هوشمند خود به داخل یک خواننده کارت[۲] دارد که سپس به آنها اجازه ورود به برنامه‌کاربردی خواسته‌شده را می‌دهد. سپس اطلاعات کارت هوشمند برای اجازه به ورود تکی به برنامه‌های‌کاربردی دیگر که کاربران برای دسترسی به آنها تلاش می‌کنند استفاده‌می‌شود. کارت‌های هوشمند، کلید خصوصی کاربر که در یک کلید مشتق شده از یک رمز عبور رمزگذاری شده است را نگه می‌دارد و به صورت زیر عمل می‌کند:

گام ۱: کاربر کارت خود را داخل یک کارت‌خوان مستقر در یک محیط کاری درج می‌کند. کربروس کلاینت، Id کاربر را درخواست می‌کند.

گام ۲: کربروس کلاینت، Id کاربر را به KAS ارسال می‌کند و کاربر یک رمز عبور انتخاب می‌کند. کربروس کلاینت یک کلید از رمز عبور استخراج می‌کند و آنرا بکارت هوشمند ارسال می‌کند. کارت هوشمند از کلید مشتق‌شده از رمز عبور برای رمزگشایی کلید خصوصی کاربر استفاده‌می‌کند.

گام ۳: KAS، گواهی (بلیط) سرویس ارائه گواهی (TGS) را تولیدمی‌کند و کلید جلسه TGS را با استفاده از کلید خصوصی کاربر رمزگذاری و پیام را به کلاینت ارسال می‌کند.

گام ٤: کربروس کلاینت، گواهی TGS را ذخیره و کلید جلسه TGS رمزگذاری شده را بکارت هوشمند منتقل می‌کند.

گام ٥: کارت هوشمند از کلید خصوصی کاربر برای رمزگشایی کلید جلسه رمزگذاری شده استفاده‌می‌کند. کارت هوشمند کلید جلسه TGS را درون حافظه فرّار خود ذخیره، کلید مشتق‌شده رمز عبور را خراب و کپی مشتق‌شده را از کلید خصوصی کاربر رمزگشایی، یک کپی از کلید جلسه TGS را با استفاده از نسخه ذخیره‌شده از کلید جلسه TGS به عنوان کلید رمزگذاری شده، رمزگذاری و کپی رمزگذاری شده را به سمت عقب به کربروس کلاینت منتقل می‌کند.

گام ٦: برای دسترسی به سرویس سیستم، کربروس کلاینت ابتدا تعیین می‌کند که آیا یک بلیط برای آن سرویس مورد نیاز است (ممکن است فردی دسترسی دیرتری بدست آورد و بنابراین فرایند به گام ۱۲ پرش کند). اگر یک بلیط مورد نیاز است، کربروس کلاینت اطلاعات هویت و یک مهر زمان را بکارت هوشمند همراه با کلید جلسه TGS رمزگذاری شده منتقل می‌کند.

---

[۱] Smart Card-based SSO

[۲] Card Reader

گام ۷: کارت هوشمند یک احراز هویت‌کننده برای سرویس TGS با رمزگشایی کلید جلسه TGS رمزگذاری شده ایجاد و اطلاعات احراز هویت و مهر زمان را با استفاده از کلید جلسه‌ی TGS رمزگشایی‌شده، رمزگذاری می‌کند. این احراز هویت‌کننده‌ی رمزگشایی‌شده به سمت کربروس کلاینت ارسال می‌شود.

گام ۸: کربروس کلاینت درخواست سرویس را همراه با گواهی TGS و احراز هویت‌کننده‌ی رمزگشایی‌شده به KAS ارسال می‌کند.

گام ۹: KAS درخواست را اعتبارسنجی می‌کند و اعتبار بلیط سرور مناسب و کلید جلسه سرور مرتبط را تولیدمی‌کند، کلید جلسه، سرور را با استفاده از کلید جلسه TGS درخواست کاربر، رمزگذاری و پیام را به کربروس کلاینت ارسال می‌کند.

گام ۱۰: کربروس کلاینت بخشی از پیام رمزگذاری شده با استفاده از کلید جلسه TGS را بکارت هوشمند منتقل می‌کند.

گام ۱۱: کارت هوشمند پیام را رمزگشایی می‌کند، کلید جلسه سرور را با استفاده از کلید جلسه TGS رمزگشایی مجدد و آنرا به کربروس کلاینت ارسال می‌کند.

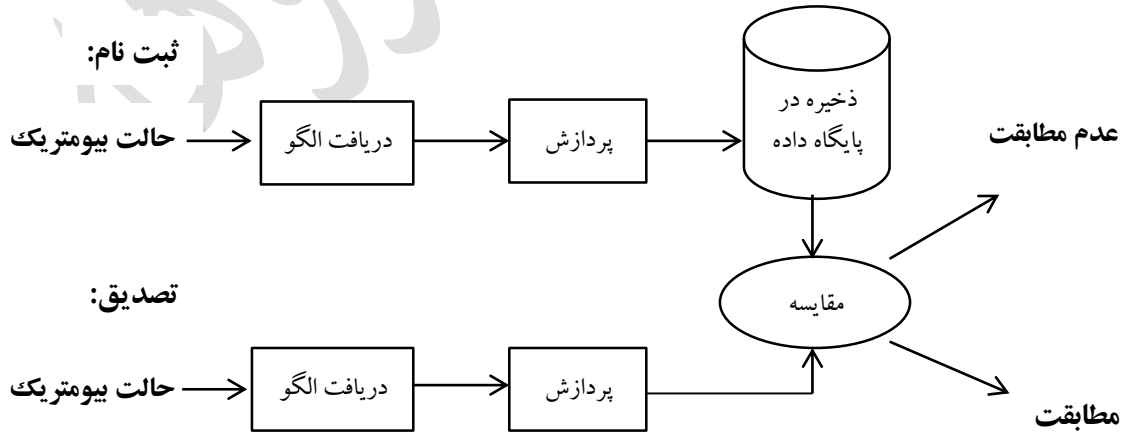
گام ۱۲: کربروس کلاینت، اطلاعات احراز هویت را منتقل، یک مهر زمان و یک کلید جلسه سرور رمزگشایی خواسته‌شده را بکارت هوشمند ارسال می‌کند (بازمی‌گرداند).

گام ۱۳: کارت هوشمند، کلید جلسه سرور رمزگذاری شده را رمزگشایی و اطلاعات احراز هویت و مهر زمان را در کلید جلسه سرور رمزگشایی‌شده رمزگذاری می‌کند. کارت هوشمند، احراز هویت‌کننده‌ی رمزگذاری شده را به کربروس کلاینت ارسال می‌کند.

گام ۱٤: کربروس کلاینت، گواهی سرور را ارسال و احراز هویت‌کننده را برای سرویس درخواست‌شده رمزگذاری می‌کند.

گام ۱۵: کربروس سرور، گواهی سرور و احراز هویت‌کننده را رمزگشایی و کاربر را احراز هویت می‌کند [۳۴، ۳۵ و ۳۸].

ورود تکی مبتنی بر بیومتریک[۱] احراز هویت بیومتریک می‌تواند با فناوری‌های ورود تکی برای امنیت بیشتر و ساده‌کردن حیات نیروی کار روزانه ترکیب شود. احراز هویت بیومتریک می‌تواند شامل استفاده از اثر انگشت، اسکن‌های شبکیه‌ای، اسکن‌های مربوط به صورت، هندسه دست و حتی DNA باشد. احراز هویت بیومتریک نیازمند مقایسه یک نمونه بیومتریک ثبت شده یا عضو (الگوی بیومتریک یا تعیین‌کننده‌هویت) در برابر یک نمونه بیومتریک جدید (برای مثال، استفاده از اثر انگشت در حین ورود) می‌باشد. در طول ثبت‌نام، همان‌طور که در شکل ۳-۳ نشان‌داده‌شده است، یک نمونه از خصوصیات بیومتریک بکارگرفته‌شده، توسط کامپیوتر پردازش و برای مقایسه‌های بعدی ذخیره می‌شود.



شکل ۳-۳: مکانیزم تشخیص بیومتریک [۳۹].

---

[۱] Biometric-based SSO

تشخیص بیومتریک می‌تواند در حالت تشخیص هویت استفاده‌شود که سیستم بیومتریک، یک شخص را از جمعیت ثبت‌نام‌شده با جستجو در یک پایگاه‌داده برای انطباق صرفاً مبتنی بر بیومتریک، تشخیص دهد. برای مثال، یک پایگاه‌داده کامل می‌تواند برای تصدیق اینکه یک شخص برای استفاده از مزایای حقوق، که تحت دو نام مختلف بکار رفته‌باشد جستجو شود که اغلب انطباق یک به چند نامیده می‌شود. همچنین یک سیستم می‌تواند در حالت تصدیق استفاده‌شود که سیستم بیومتریک هویت درخواست‌شده، شخص را از الگوهای ثبت‌شده‌ی قبلی‌اش احراز هویت کند که انطباق یک به یک نامیده می‌شود. در دسترسی بیشتر به کامپیوترها یا محیط‌های دسترسی به شبکه، حالت تصدیق می‌تواند استفاده‌شود. کاربرِ یک اکانت، نام‌کاربری را وارد یا یک نشانه مانند یک کارت هوشمند درج می‌کند اما در عوضِ ورود رمز عبور، یک لمس ساده با انگشت یا یک نگاه اجمالی در یک دوربین برای احراز هویت کاربر کافی است [۳۴، ۳۵ و ۳۹]. فناوری‌های بیومتریک منتظر بکارگیری یک نقش کلید در احراز هویت شخصی برای محیط‌های احراز هویت‌های شبکه‌های سطح وسیع سازمانی و برای محافظت از همه انواع محتوای دیجیتال مانند مدیریت حقوق دیجیتال و برنامه‌های کاربردی سالم هستند.

ورود تکی مبتنی بر پُرکردن فرم[۱]: پُرکردن فرم، اجازه ذخیره‌سازی قوی اطلاعات را می‌دهد که معمولاً داخل یک فرم پُر شده است. برای کاربران که به‌طور مکرر فرم‌ها را پر می‌کنند، خصوصاً برای دسترسی امن، این فناوری قصد به یادآوری/ذخیره همه‌ی این اطلاعات و امنیت آن با یک رمز عبور منحصر را دارد. برای دسترسی به اطلاعات، کاربر تنها یکی از رمز عبورها را به‌خاطر می‌آورد و فناوری پُرکردن فرم می‌تواند با دقت، پر کردن فرم‌ها را انجام دهد. یک پُرکننده فرم یک برنامه نرم‌افزاری است که به‌طور خودکار فرم‌های در یک UI را پُر می‌کند. پُرکنندگان فرم می‌توانند بخشی از یک برنامه بزرگتر مانند یک مدیریت رمز عبور یا یک راه حل مبتنی بر ورود تکی سازمانی باشند. پُرکننده فرم متضاد تکه‌تکه‌کردن صفحه است که داده‌ها را از یک فرم استخراج می‌کند [۳۴ و ۳۵].

ورود تکی مبتنی بر NTLM[۲]: برای یک کاربر، اثبات اینکه آنها رمز عبورهایشان را بدون ارائه واقعی خود رمز عبور می‌دانند، امکان‌پذیر است. NTLM این را با استفاده از یک پروتکل چالش و پاسخ بدست می‌آورد که ابتدا نوع NTLM و مکانیزم‌های رمزگذاری را که کلاینت و سرور به‌طور متقابل و دو طرفه پشتیبانی می‌کنند را تعیین می‌کند، سپس به‌طور پنهانی رمز عبورهای کاربر را هَش می‌کند و آن را به سرور نیازمند احراز هویت ارسال می‌کند.

NTLM یک پروتکل احراز هویت پاسخ-چالش است که از ۳ پیام برای احراز هویت یک کلاینت در یک محیط ارتباط‌گرا استفاده‌می‌کند و پیام اضافی چهارم اگر یکپارچگی خواسته‌شود مورد استفاده قرار می‌گیرد. اول، کلاینت یک مسیر شبکه به سرور بدست می‌آورد و یک اعلانِ پیام مذاکره از قابلیت‌هایش ارسال می‌کند. در گام بعدی، سرور با پیام چالش پاسخ می‌دهد که برای بدست‌آوردن هویت کلاینت استفاده‌می‌شود. سرانجام، کلاینت به چالش با یک پیام احراز هویت پاسخ می‌دهد.

پروتکل NTLM، یک یا هر دو مقدار رمز عبور هَش‌شده را استفاده‌می‌کند که روی سرور (یا کنترل‌کننده دامنه) نیز ذخیره شده است و مشابه رمز عبور است، بدین معنا که اگر مقدار هَش از سرور سرقت شود می‌تواند بدون آگاهی از رمز عبور واقعی، احراز هویت شود. درحالی که کربروس به عنوان یک پروتکل احراز هویت پیش‌فرض در اکتیودایرکتوری مبتنی بر شمای ورود تکی جایگزین NTLM شده است،NTLM هنوز در موقعیت‌هایی که یک کنترل‌کننده دامنه در دسترس نیست یا غیرقابل دستیابی است بطور گسترده‌ای استفاده‌می‌شود. برای مثال، اگر یک کلاینت قابلیت کربروس را ندارد، سرور به یک دامنه متصل نباشد یا کاربر از راه دور روی وب احراز هویت شده‌باشد، NTLM می‌تواند استفاده‌شود [۳۴، ۳۵ و ۴۰].

---

[۱] Form-filling SSO

[۲] NTLM-based SSO

ورود تکی مبتنی بر SPNEGO[1]: یک مکانیزم شبه کد GSSAPI است که برای مذاکره‌ی یکی از مکانیزم‌های واقعی ممکن، استفاده‌شده است. SPNEGO هنگامی که یک برنامه‌کاربردی کلاینت قصد احراز هویت یک سرور دور را دارد استفاده‌شده است اما در انتها تضمین نمی‌کند که پروتکل‌های احراز هویت دیگر را پشتیبانی کند. مکانیزم شبه کد از یک پروتکل برای تعیین اینکه مکانیزم‌های GSSAPI مشترک در دسترس هستند، انتخاب یکی از آنها و سپس عدم مطابقت همه‌ی فعالیت‌های امنیتی اضافی برای آنها، استفاده‌می‌کند. هنگامی که برنامه‌کاربردی کاربر و سرور دور، نوع احراز هویتی که پشتیبانی می‌کند را نمی‌داند، در این زمان، SPNEGO (مکانیزم مذاکره GSSAPI ساده و محافظت‌شده) می‌تواند برای یافتن مکانیزم‌های احراز هویت دو طرفه‌ای که دردسترس و قابل استفاده هستند استفاده‌شود. برخی از این مکانیزم‌ها می‌تواند شامل احراز هویت کربروس و NTLM شود. همچنین بیشترین استفاده از SPNEGO در توسعه احراز هویت مذاکره HTTP مایکروسافت است [۳۴ و ۳۵].

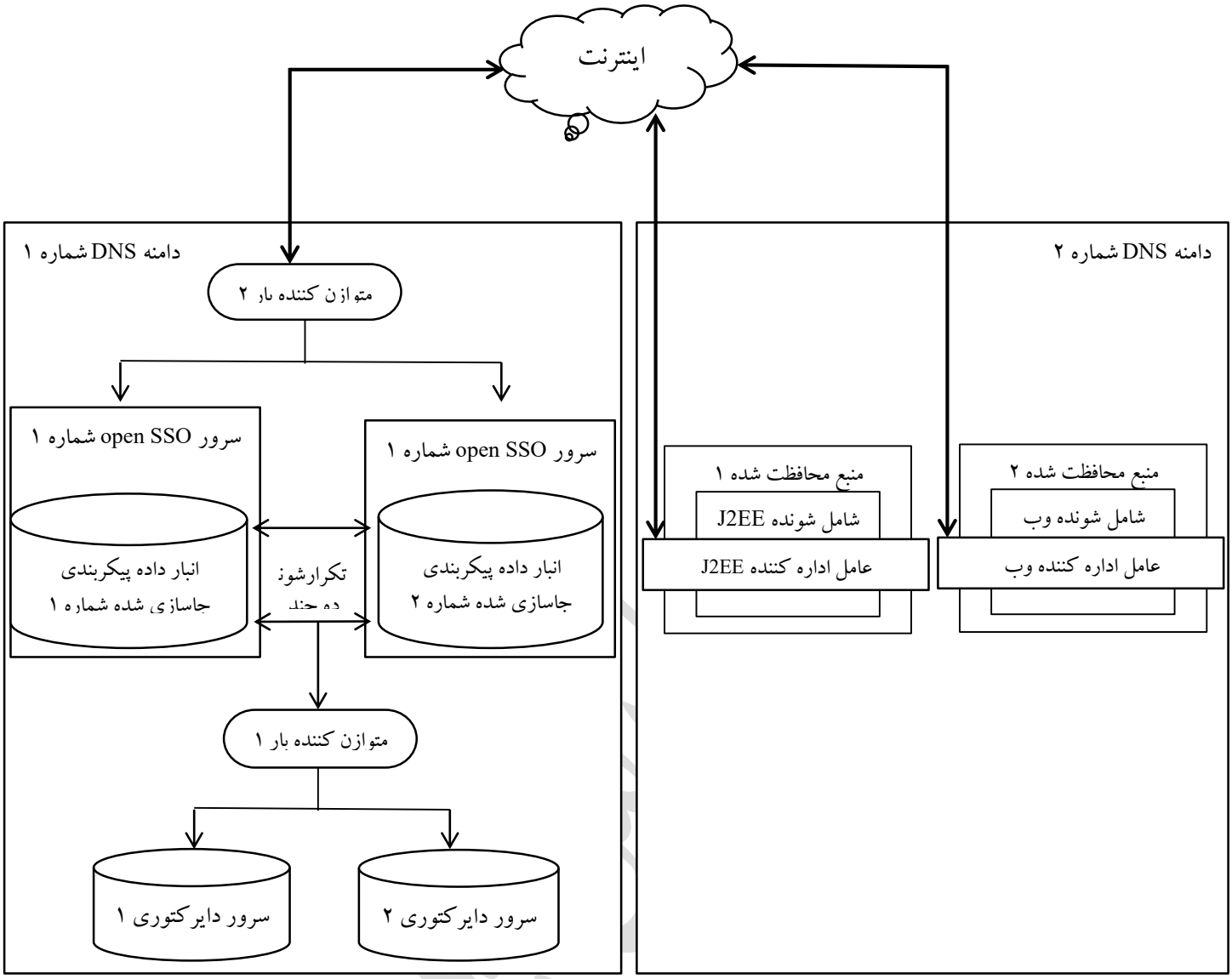
ورود تکی کاهش‌یافته[2]: ورود تکی کاهش‌یافته به‌طور گسترده‌ای برای محدود کردن تعداد دفعاتی که یک کاربر نیاز به وارد کردن اعتباراتشان برای دسترسی به برنامه‌های کاربردی مختلف دارند استفاده‌می‌شود. با برنامه‌های کاربردی بحرانی، ورود تکی کاهش‌یافته نیز یک تکنیک برای اطمینان از اینکه یک کاربر بدون یک احراز هویت دو عاملی که توسط کاربر ارائه می‌شود وارد نشده‌باشد، ارائه‌شده است. احراز هویت دو عاملی می‌تواند به عنوان یک قطعه سخت‌افزار مانند کارت هوشمند، سوالات چالشی یا حتی بیومتریک پیاده‌سازی شود.

ورود تکی کاهش‌یافته اجازه دسترسی به منابع مطمئن با یک مجموعه از اعتبارات را می‌دهد اما به اعتبارات اضافی برای منابع حیاتی بیشتر نیاز دارد. ورود تکی کاهش‌یافته، روش‌های احراز هویت/رمز عبور مختلف یا اضافی روی سرورها و برنامه‌های کاربردی ارائه می‌دهد که به‌طور امن‌تری کنترل می‌شوند. ورود تکی کاهش‌یافته نسبت به ورود تکی یک مزیت دارد، به‌طوریکه از دسترسی به هر چیزی که باید یک رمز عبور یا وسیله احراز هویت توافق کرده‌باشد جلوگیری می‌کند. از دید کاربر، ورود تکی کاهش‌یافته مانند ورود تکی برای استفاده، محرمانه و آسان نیست. مدیران IT از آن برای افزایش امنیت خود روی ورود تکی کاهش‌یافته بهره می‌برند. استفاده موفقیت‌آمیزِ ورود تکی کاهش‌یافته تنها نیازمند اینست که حقوق مشخصی برای بهبود امنیت، بدون ایجاد هیچ زحمت اضافی برای کاربر، برای فعالیت استفاده‌کند [۳۴ و ۳۵].

ورود تکی بین چند دامنه[3]: اعتبارات ممکن است نیازمند انتقال بین سرورها و دامنه‌های مختلف باشند که به ورود تکی بین چنددامنه (CDSSO) باز می‌گردد. با متکی نبودن به یک سرور احراز هویت ماهر، ورود تکی بین چنددامنه به کاربر اجازه می‌دهد به آسانی بین دامنه‌های امن مختلف، هنگامی که منبع از جای دیگری درخواست می‌شود احراز هویت شود. ورود تکی بین چنددامنه، ورود تکی را فراتر از یک دامنه تکی گسترش می‌دهد. ورود تکی بین چنددامنه، یک مکانیزم برای عبور نشانه‌های ورود تکی به منابع محافظت‌شده‌ی سیاست‌های عامل ارائه‌شده در دامنه‌های DNS مختلف است. ورود تکی بین چنددامنه این امکان را برای کاربران برای احراز هویت یکباره در برابر سرور سازمان OpenSSO در یک دامنه DNS اصلی ایجاد می‌کند و سپس توسط سیاست‌های عامل ارائه‌شده در دامنه‌های DNS دیگر بدون داشتن احراز هویت مجدد به منابع محافظت‌شده دسترسی پیدا می‌کند. ورود تکی بین چنددامنه یک مکانیزم اختصاصی سازمانی OpenSSO برای پشتیبانی از ورود تکی در سرتاسر دامنه‌های چندگانه است. بعلاوه می‌توان از پروتکل‌های یکپارچه مبتنی بر استاندارد برای بدست‌آوردن ورود تکی در سرتاسر دامنه‌های چندگانه استفاده کرد. مزیت استفاده از ورود تکی بین چنددامنه این است که منابع در بین دامنه‌های چندگانه محافظت می‌شوند. شکل ۳-۴ یک معماری توسعه‌یافته ورود تکی بین چنددامنه ساده و معمولی را نشان می‌دهد.

---

[1] SPNEGO-based SSO [2] Reduced SSO [3] Cross-domain SSO



شکل ۳-٤: یک معماری توسعه‌یافته ورود تکی بین چنددامنه ساده و معمولی [۳۴، ۳۵ و ۴۱].

ورود تکی مبتنی بر ثبت‌نام[۱]: یک کاربر که درون یک وب سایت وارد می‌شود ممکن است بخواهد اعتبارات خود را به‌طور دائمی برای آن سایت به‌خاطر داشته‌باشد. این با ایجاد یک کوکی رمزگذاری شده روی ماشین کاربر برای آن مرورگر وب انجام‌می‌شود که اعتبارات کاربر را شامل می‌شود. این کوکی بر شروع دوباره ماشین در سرتاسر جلسات مرورگرهای مختلف پافشاری می‌کند اما پس از یک دوره‌ی زمانی برای منقضی‌شدن تنظیم خواهدشد. در گام بعدی، کاربر به وب سایت دسترسی پیدا می‌کند، سرور کوکی را تشخیص می‌دهد، آنرا برای بدست‌آوردن اعتبارات کاربر رمزگشایی می‌کند و پس از اعتبارسنجی کامل صفحه ورود به‌طور موفقیت‌آمیز، سبب انشعاب می‌شود.

ورود تکی مبتنی بر جلسه[۲]: ورود اولیه کاربر به یک سرور HTTP از طریق نتایج مرورگر وب در یک نشانه جلسه روی سرور تولید شده است و از طریق یک کوکی داخل حافظه به کاربر بازگردانده شده است. از آن به بعد، ورود تکی با ارائه نشانه جلسه به سرور به عنوان اثباتی از احراز هویت انجام‌می‌شود. ورود تکی مبتنی بر جلسه، محرمانگی ورود به یک سرور یا دامنه را با

---

[۱] Enrollment-based SSO

[۲] Session-based SSO

ورود یکباره به کاربر ارائه می‌دهد و برای دسترسی به منابع در دامنه‌های مشابه یا سرورهای مختلف نیاز به ورود دوباره ندارد. اساس ورود تکی مبتنی بر جلسه احراز هویت اولیه است، ایجاد یک نشانه جلسه و منابعی که می‌دانند چگونه کاربر را با نشانه جلسه احراز هویت کنند. ورود تکی مبتنی بر جلسه شامل مراحل زیر است:

- احراز هویت اولیه- برخی ابزارهای کاربر، هویت آنها را برای سرور منبع تصدیق می‌کنند. اعتبارات معمولاً در شکلی از یک جفت نام‌کاربری و رمز عبور هستند.
- نشانه جلسه- کوکی که شامل اطاعات مورد نیاز برای احراز هویت کاربر به‌طور خودکار است.
- جلسه- زمانی که یک کاربر به‌طور فعال با یک کوکی به یک منبع وارد می‌شود.
- سرور جلسه- سروری که احراز هویت اصلی را انجام می‌دهد، جلسه را در یک پایگاه‌داده یا حافظه انجام می‌دهد و کوکیِ جلسه را به کلاینت ارائه می‌دهد.
- اعتبارسنجی نشانه- پیاده‌سازی‌شده‌ی تعدادی از روش‌ها. برخی سیستم‌ها یک سرور جلسه مرکزی دارند که می‌توانند نشانه را اعتبارسنجی کنند. سیستم‌های دیگر، برنامه‌های کاربردی دارند که می‌توانند ثبت شوند و در استفاده‌ی نشانه برای اعتبارسنجی شریک دخالت کنند.

هنگامی که یک جلسه پایان می‌یابد، سرور، جلسه و اطلاعات هر برنامه‌کاربردی که با سرور برای این اطلاعات ثبت شده است را از بین می‌برد، بنابراین از دسترسی بیشتر بدون احراز هویت دستی جلوگیری می‌شود.

ورود تکی صحیح[۱] ورود تکی صحیح، توانایی ارائه اعتبارات، یک مرتبه در طول جلسه را دارد و برای اعتبارات مجدداً پرسیده نمی‌شود. این توسط نفوذ اعتبارات در هنگام هدایت به منابع دیگر در طول جلسات انجام‌می‌شود که نیاز به تصحیح اعتبارات را خواهد داشت. ورودتکی صحیح، معمولاً هنگامی که کاربر به ماشین رومیزی خودش در آغاز روز کاری خودش وارد می‌شود، به یکبار وارد کردن رمز عبور نیاز دارد. برخی پیاده‌سازی‌های ورود تکی صحیح از رمز عبورهای مشابه و ID کاربر در برابر یک پایگاه‌داده مرکزی برای احراز هویت یک کاربر استفاده می‌کنند به‌طوریکه آنها به منابع محافظت‌شده‌ی اضافی در سرتاسر روز دسترسی دارند. همچنین برای ورودتکی صحیح، استفاده از یک کلید امنیت مورد نیاز است. کاربر یکبار با نام‌کاربری و رمز عبور خودش در اولین بار احراز هویت می‌شود. سرور احراز هویت همچنین یک نشانه رمزگذاری شده یا کلیدی که به عنوان شناسه برای دسترسی آینده به منابع مورد استفاده قرار خواهدگرفت به کاربر ارائه می‌دهد که می‌داند چگونه نشانه را رمزگشایی کند و کاربر را همان‌طور که احراز هویت شده است تشخیص دهد [۳۴ و ۳۵].

٤-۳ روش کربروس

کربروس سال ۱۹۸۳ هنگامی که MIT[۲] تصمیم به یکپارچگی شبکه‌های کامپیوتری به عنوان بخشی از دوره‌های آموزشی خود گرفت بوجود آمد. هدف از پروژه آتن یکپارچگی ورودتکی، سیستم‌های فایل شبکه‌شده، محیط گرافیکی متحدشده و سرویسِ قراردادنِ نام، بود [۴۱].

۱-٤-۳ پروتکل کربروس

پروتکل کربروس برای فرایند احراز هویت کاربران بدین صورت عمل می‌کند:

مبادله احراز هویت: مشتری از سرور احراز هویت برای یک گواهی به سرور ارائه گواهی[۳] پاسخ می‌دهد. سرور احراز هویت، مشتری را در پایگاه‌داده خود جستجو می‌کند. سپس یک کلید جلسه[۴] (SK1) برای استفاده بین مشتری TGS تولید می‌کند.

---

۱ True SSO
۲ Massachusetts Institute of Technology
۳ Ticket-Granting Server
۴ Session Key

کربروس SK1 را با استفاده از کلید رمز مشتری، رمزگذاری می‌کند. سرور احراز هویت همچنین از کلید رمز TGS (شناخته‌شده تنها برای سرور احراز هویت و TGS) برای ایجاد و ارسال یک گواهی تولید گواهی به کاربر[1] استفاده‌می‌کند.

مبادله سرویس ارائه گواهی: مشتری پیام را رمزگشایی و کلید جلسه را بازیابی می‌کند، سپس از آن برای ایجاد محتوای تاییدیه نام کاربر، آدرس IP و مهر زمان استفاده‌می‌کند. مشتری، احراز هویت‌کننده را همراه با TGT، برای درخواست دسترسی به سرور هدف به TGS، ارسال می‌کند. TGS، TGT را رمزگشایی می‌کند، سپس از SK1 درون TGT برای رمزگشایی تاییدکننده استفاده می‌کند. اطلاعات تاییدکننده، گواهی، آدرس شبکه مشتری و مهر زمان، بررسی می‌شود. اگر همه چیز منطبق بود، اجازه ارسال درخواست داده‌می‌شود. سپس TGS یک کلید جلسه جدید (SK2) برای مشتری و سرور هدف برای استفاده ایجاد می‌کند، این با استفاده از SK1 رمزگذاری و به مشتری ارسال می‌شود. TGS نیز یک محتوای گواهی جدید شامل نام مشتری، آدرس شبکه، مهر زمان و یک زمان انقضا برای گواهی ارسال می‌کند که همگی با کلید رمز سرور هدف و نام سرور رمزگذاری شده‌اند.

مبادله سرور/ مشتری: مشتری پیام را رمزگشایی می‌کند و SK2 را بدست‌می‌آورد. مشتری یک تاییدکننده جدید رمزگذاری شده با SK2 ایجاد می‌کند و سرانجام برای نزدیک شدن به سرور هدف آماده می‌شود. مشتری، گواهی جلسه (رمزگذاری شده با کلید رمز سرور هدف) را ارسال و تاییدکننده را رمزگذاری می‌کند. بنابراین تاییدکننده شامل متن اصلی رمزگذاری شده با SK2 است که اثبات می‌کند که مشتری کلید را می‌داند. مهر زمان رمزگذاری شده از یک استراق سمع برای ثبت گواهی و تاییدکننده، جلوگیری می‌کند و بعداً آنها را پاسخ می‌دهد. سرور هدف ،گواهی، تاییدکننده، آدرس مشتری و مهر زمان را رمزگشایی و بررسی می‌کند. برای برنامه‌های کاربردی که نیازمند احراز هویت دو عاملی هستند، سرور هدف یک پیام شامل مهر زمان به اضافه یک را بازمی‌گرداند که با SK2 رمزگذاری شده است. این به مشتری ثابت می‌کند که سرور واقعاً کلید رمز خود را می‌داند و بنابراین می‌تواند گواهی و تاییدیه را رمزگشایی کند.

ارتباطات امن: سرور هدف می‌داند که مشتری کسی است که ادعا کرده است و هر دو اکنون کلید رمزگذاری برای ارتباطات امن را به اشتراک می‌گذارند. بنابراین تنها مشتری و سرور هدف این کلید را به اشتراک می‌گذارند. همچنین آنها می‌توانند فرض‌کنند که یک پیام جدید در کلید مرتبط با بخش دیگر رمز شده است [۴۲]. خنثی‌کردن یک تهاجم یکی از ویژگی‌های اصلی کربروس است، که رمز عبورها در یک متن واضح روی یک شبکه فرستاده‌نمی‌شود. کربروس یک راه حل امنیتی امن درنظر گرفته می‌شود. کربروس یک فناوری است که اجازه احراز هویت قوی در شبکه‌های توزیع‌شده و باز را می‌دهد و به چهار دلیل اصلی یک راه حل امنیتی معتبر است.

۱- کربروس کامل است. کربروس به‌طور وسیعی استفاده‌می‌شود و برای زمان‌های طولانی مورد مطالعه قرار گرفته‌است. به‌طور امنیتی، برای مقیاس‌های وسیع بکار می‌رود.

۲- کربروس نیازهای سیستم‌های توزیع‌شده مدرن را برآورده‌می‌کند که در پاسخ به تفکر خوش تعریف و روشن از طریق مجموعه‌ای از نیازها برای احراز هویت امن در یک محیط باز با لینک‌های ارتباطی ناامن توسعه یافته‌بود. این بیان می‌کند که این نیازها تقریباً با نیازهای سیستم‌های توزیع‌شده‌ی مدرن که روی شبکه‌های مبتنی بر پروتکل‌های اینترنت عمل می‌کنند مطابق است.

۳- کربروس از نظر معماری دقیق است. کربروس پیرامون یک مجموعه واضحی از انتزاع ساختاری و تابعی طراحی شده است که این معماری دقیق، اجازه بکارگیری روی زمان را می‌دهد و باعث سهولت یکپارچگی آن، داخل سیستم‌های دیگر می‌شود. این معماری دقیق باعث سهولت تجزیه‌وتحلیل اینکه کربروس چگونه رفتار خواهد کرد می‌شود.

۴- کربروس در محل حضور دارد. کربروس تقریباً در بیشتر سیستم‌عامل‌ها و بسیاری از برنامه‌های کاربردی نرم‌افزاریِ مورد استفاده در سطح وسیع، یکپارچه‌شده است. این موضوع یک بخش کامل از زیرساخت IT امروزی است [۴۳].

---

[1] Ticket-Granting Ticket

۳-٤-۲ مزایای کربروس

محافظت از رمز عبورها. نیاز به ارسال رمز عبورهای کاربر روی شبکه یا در متن اصلی یا تحت رمزنگاری نیست. این پروتکل در مقابل روی کلیدهای رمز تکیه می‌کند که به صورت رمزگذاری ارسال می‌شوند و نمی‌توان از آنها جلوگیری کرد. اگر امنیت شبکه برقرار باشد این امکان وجود ندارد که متجاوزان به محتوای ارتباط شبکه پی ببرند.

احراز هویت سرور/کلاینت. کلاینت و سرور باید هر کدام برای دیگری احراز هویت شوند. اگر اینگونه نشود ارتباطی برقرار نمی‌شود.

گواهی بلیط کلاینت/سرور. علاوه بر احراز هویت متقابل، برای بلیط‌های عبور کرده از سرور به کلاینت و برعکس، مهر زمان، ایجاد و اطلاعات چرخه حیات را شامل می‌شود.

پایایی، ایستایی و قابلیت استفاده مجدد. احراز هویت توسط کربروس کامل، ایستا، پایا و قابل استفاده مجدد است. هنگامی که کاربر یک مرتبه احراز هویت می‌شود، احراز هویت برای چرخه حیات آن بلیط قابل استفاده مجدد است. در واقع، احراز هویت از طریق کربروس بدون وارد کردن مجدد نام‌کاربری و رمز عبور در سرتاسر شبکه (تا زمانی که احراز هویت منقضی نشده) باقی‌می‌ماند.

تولید کلید جلسه سرویس. با توجه به این که مدل کربروس از روش رمزنگاری کلید دوتایی استفاده‌می‌کند، کلید جلسه سرویس که منجر به یک ارتباط خاص بین کلاینت و سرویس می‌شود دارای امنیت کامل است.

استانداردهای اینترنت. پروتکل کربروس کاملاً بر استانداردهای اینترنت باز متکی است و به کدهای اختصاصی یا مکانیزم‌های احراز هویت محدود نیست. این ویژگی به توسعه‌دهندگان اجازه تکیه بر هر تعداد از پیاده‌سازی‌های منابع باز و رایگان از طریق ابزارهای عمومی را می‌دهد.

حضور در همه جا در یک لحظه. کربروس در ارتباط با چالش‌های جهان واقعی ساخته‌شده است. بزرگترین ویژگی کربروس قدرت در تعداد است. به دلیل اینکه کربروس به‌طور وسیع استفاده‌می‌شود و توسط توسعه‌دهندگان سطح بالا، خبرگان امنیتی و رمزگذاران تایید شده است، هر ضعف یا نقص شناسایی و سریعاً پوشش داده‌می‌شود [۴۴].

۳-٤-۳ معایب

علاوه بر مزایای ذکر شده، پروتکل کربروس معایبی دارد که تعدادی از آنها در زیر آمده است:

- کربروس برای طراحی و پیاده‌سازی یک سیستم امنیتی مناسب نیست.
- اگر یک کلید کربروس که یک ماشین برای خودش استفاده‌می‌کند به صورت توافقی بدست‌آمده‌باشد، مهاجم می‌تواند به‌طور مشابه هر کاربر را روی آن کامپیوتر با جعل درخواست‌های تایید شده برای آن ماشین جعل هویت کند.
- اگر مهاجم بتواند در مکانیزم‌های امنیتی روی کامپیوتر محلی رخنه کند، همه‌ی کلیدهای جلسه موجود می‌توانند جعل شوند.
- در کامپیوترهای چندکاربره، کربروس با مشکل مواجه است و اگر رخنه‌هایی در امنیت میزبان وجود داشته‌باشد، مهاجم می‌تواند به کلیدها دسترسی داشته‌باشد.
- کلیدها روی دیسک‌های محلی استخراج می‌شوند که بسیار نامطمئن و ناامن هستند.
- پروتکل کربروس از لحاظ مقاومت در برابر نفوذ آنگونه که باید باشد نیست. مهمترین دلیل آن استفاده از یک احراز هویت‌کننده برای جلوگیری از پاسخ به حملات است. احراز هویت‌کننده متکی بر استفاده از یک مهر زمان برای محافظت در برابر استفاده مجدد است که باعث بروز مشکلاتی می‌شود. یکی از این مشکلات اینست که هیچ پاسخی داخل زمان حیاتِ (معمولاً ۵ دقیقه) احراز هویت‌کننده محتمل نیست.

- به دلیل اینکه کربروس از الگوریتم‌های رمزگذاری استفاده می‌کند و اینکه مهاجم می‌تواند دیالوگ‌های ورود زیادی را ضبط کند و با توجه به الگوریتم‌هایی که استفاده می‌شود و این الگوریتم‌ها شناخته‌شده هستند و اینکه کاربران معمولاً رمز عبورهای خوبی انتخاب نمی‌کنند، مهاجم می‌تواند رمز عبورهای کاربران را حدس بزند.
- در یک محیط کاری، مهاجم می‌تواند به سادگی یک دستور ورود (Login) را با نسخه‌ای که رمز عبورهای کاربران را قبل از بکارگیری آنها در یک گفتگوی کربروس، ضبط و آنها را جایگزین کند و ورود را جعل کند (به عبارت دیگر، با یک دستور جعلی هنگامی که کاربران رمز عبور خود را وارد می‌کنند، قبل از اینکه پروتکل کربروس از آنها استفاده کند آنها را ضبط و به جای دستور ورود اصلی از آنها استفاده کند).
- چون کلیدها در چندین جلسه استفاده می‌شوند امکان افشای کلیدها بیشتر است.
- بلیط‌های کربروس در زمان و ناحیه محدود هستند و تنها قابل استفاده در ناحیه‌ی سرور تصدیق بلیط و در یک دوره زمانی خاص هستند.
- کربروس هرگز رمز عبورها را روی شبکه منتقل نمی‌کند که این می‌تواند به عنوان یک مزیت درنظر گرفته شود.
- طراحی اصلی کربروس نیازمند مقداری حافظه است که به علت اینکه در سیستم‌های یونیکس برای سرورهای TC، ذخیره احراز هویت مشکل می‌باشد و کربروس به شدت به پالس‌های زمانی سنکرون‌شده وابسته‌است هرگز پیاده‌سازی نخواهدشد [۵۴].

کربروس برای سیستم‌های امروزی مهم و با ارزش است. دلایل زیر ارزشمندی و اهمیت کربروس را نشان می‌دهد:

- سهولت و کیفیت یکپارچه‌سازی
- مقیاس‌پذیری و جهانی بودن
- بکارگیری سیاست‌ها و قابلیت بررسی و ممیزی
- عمل کردن در جهان واقعی
- انتخاب مکانیزم‌های احراز هویت
- اثربخشی- هزینه در توسعه جهان واقعی
- گزینه‌های پشتیبانی فراوان از ارائه‌دهندگان مختلف

۵-۳ احراز هویت ورود تکی به وب با استفاده از زبان نشانه‌گذاری اثبات امنیت

سازمان‌ها اخیراً از منابع احراز هویت مرکزی برای برنامه‌های کاربردی داخلی و سامانه‌های مبتنی بر وب برای بیشتر قسمت‌های خود استفاده می‌کنند. برای مبارزه با پراکندگی برنامه‌های کاربردی و به حداقل رساندن تاثیر بر کاربران نهایی، اکثر سازمان‌ها در حال حرکت به سمت راه حل‌های ورود تکی هستند. احراز هویت منبع تکی، هنگامی که به درستی پیکربندی شده‌باشد، باعث ایجاد یک امنیت قوی می‌شود. این روش همچنین باعث سهولت مدیریت و حسابرسی کاربران می‌شود.

اکثر خدمات وبی که توسط ارائه‌دهندگان خدمات خارجی میزبانی می‌شوند، مشکل تعدد کلمات عبور برنامه‌های خارجی و لزوم به‌خاطر سپردن آنها را دارند. همچنین برای ارائه‌دهندگان سرویس خارجی نیز باعث ایجاد مشکلاتی می‌شوند. هر کاربر در یک سازمان نیازمند راه‌اندازی تنظیماتی برای ارائه‌دهندگان سرویس برنامه‌کاربردی است که باعث تکرار مجموعه‌ای از داده‌ها می‌شود. در حالی که اگر سازمان بتواند این داده‌های کاربر را کنترل کند، می‌تواند در زمان ارائه سرویس با عدم نیاز به راه‌اندازی و خاتمه دسترسی کاربر به صورت روزانه صرفه‌جویی کند. علاوه بر این، یک منبع مرکزی می‌تواند باعث دقیق‌تر و به‌روز بودن داده‌ها شود.

راه حل این مشکلات، استفاده از یک استاندارد برای احراز هویت اطلاعاتِ مبادله‌شده روی اینترنت است. زبان نشانه‌گذاری اثبات امنیت، یک راه حل مبتنی بر زبان نشانه‌گذاری قابل توسعه و امن برای تبادل اطلاعات امنیتی کاربر بین ارائه‌دهنده هویت و ارائه‌دهنده سرویس فراهم می‌کند که اجازه احراز هویت و مجوز، هنگام ورود تکی را می‌دهد.

در مبادله زبان نشانه‌گذاری اثبات امنیت سه نقش درگیر وجود دارد: یک بخش اثبات، یک بخش مسئول و یک مدیر (معمولاً یک کاربر). بخش اثبات (ارائه‌دهنده هویت) یک سیستم قدرتمند است که اطلاعات کاربر را فراهم می‌کند. بخش مسئول (ارائه‌دهنده سرویس) سیستمی است که اطمینان اطلاعات بخش اثبات را انجام می‌دهد و از داده‌ها برای ارائه برنامه‌کاربردی به کاربر استفاده می‌کند. کاربر و شناسه آن که در مبادله دخیل هستند به عنوان موضوع شناخته می‌شوند. مدیر، یک سرویس را از ارائه‌دهنده سرویس درخواست می‌کند. ارائه‌دهنده سرویس یک اثبات هویت از ارائه‌دهنده هویت درخواست می‌کند و آنرا بدست می‌آورد. براساس این اثبات، ارائه‌دهنده سرویس می‌تواند یک تصمیم کنترل دسترسی ایجاد کند. قبل از تحویل اثبات هویت به ارائه‌دهنده سرویس، ارائه‌دهنده هویت ممکن است برخی اطلاعات (از قبیل نام‌کاربری و رمز عبور) را از مدیر درخواست کند، به عبارت دیگر مدیر را احراز هویت کند. زبان نشانه‌گذاری اثبات امنیت، اثبات‌های بین بخش‌ها را مشخص می‌کند. پیام‌ها، هویتی که از ارائه‌دهنده هویت به ارائه‌دهنده سرویس منتقل شده است را اثبات می‌کند. در زبان نشانه‌گذاری اثبات امنیت، یک ارائه‌دهنده هویت ممکن است اثبات‌های زبان نشانه‌گذاری اثبات امنیت را برای ارائه‌دهندگان سرویس متعددی فراهم کند. به‌طور مشابه، یک ارائه‌دهنده سرویس ممکن است اثبات‌ها را برای ارائه‌دهندگان هویت مستقل متعددی تامین و تضمین کند.

مبادله از بخش اثبات به بخش مسئول، اثبات زبان نشانه‌گذاری اثبات امنیت نامیده می‌شود. بخش مسئول فرض می‌کند که تمام اطلاعات موجود در اثبات برای بخش اثبات معتبر است. ساختار استاندارد زبان نشانه‌گذاری اثبات امنیت که توسط شمای زبان نشانه‌گذاری توسعه‌پذیر تعریف شده است شامل اطلاعات سرآیند، موضوع و جملاتی در مورد موضوع در فرمی از ویژگی‌ها و شرایط می‌شود. اثبات همچنین می‌تواند حاوی جملات مجوز، تعریف‌کننده‌ی آنچه که کاربر مجاز به انجام آن داخل برنامه‌های‌کاربردی وب است، باشد. زبان نشانه‌گذاری اثبات امنیت روش احراز هویت در ارائه‌دهنده هویت را مشخص نمی‌کند. احراز هویت ممکن است از نام‌کاربری و رمز عبور یا شکل‌های دیگری از احراز هویت مانند احراز هویت چند عاملی استفاده کند.

اصلی‌ترین کاربرد زبان نشانه‌گذاری اثبات امنیت، ورود تکی مرورگر وب نام دارد. کاربر با بکارگیری یک عامل کاربر (معمولاً یک مرورگر وب) یک منبع وب محافظت‌شده را توسط یک ارائه‌دهنده سرویس زبان نشانه‌گذاری اثبات امنیت درخواست می‌کند. ارائه‌دهنده سرویس، تمایل به دانستن هویت کاربر درخواست‌دهنده دارد. درخواست احراز هویت از طریق عامل کاربر به یک ارائه‌دهنده هویت زبان نشانه‌گذاری اثبات امنیت فرستاده‌می‌شود. جریان پروتکل در دیاگرام جریان شکل ۳-۵ به تصویر کشیده شده است.

۱. درخواست منبع هدف در ارائه‌دهنده سرویس

مدیر از طریق یک عامل کاربر (HTTP) یک منبع هدف در ارائه‌دهنده سرویس درخواست می‌کند:

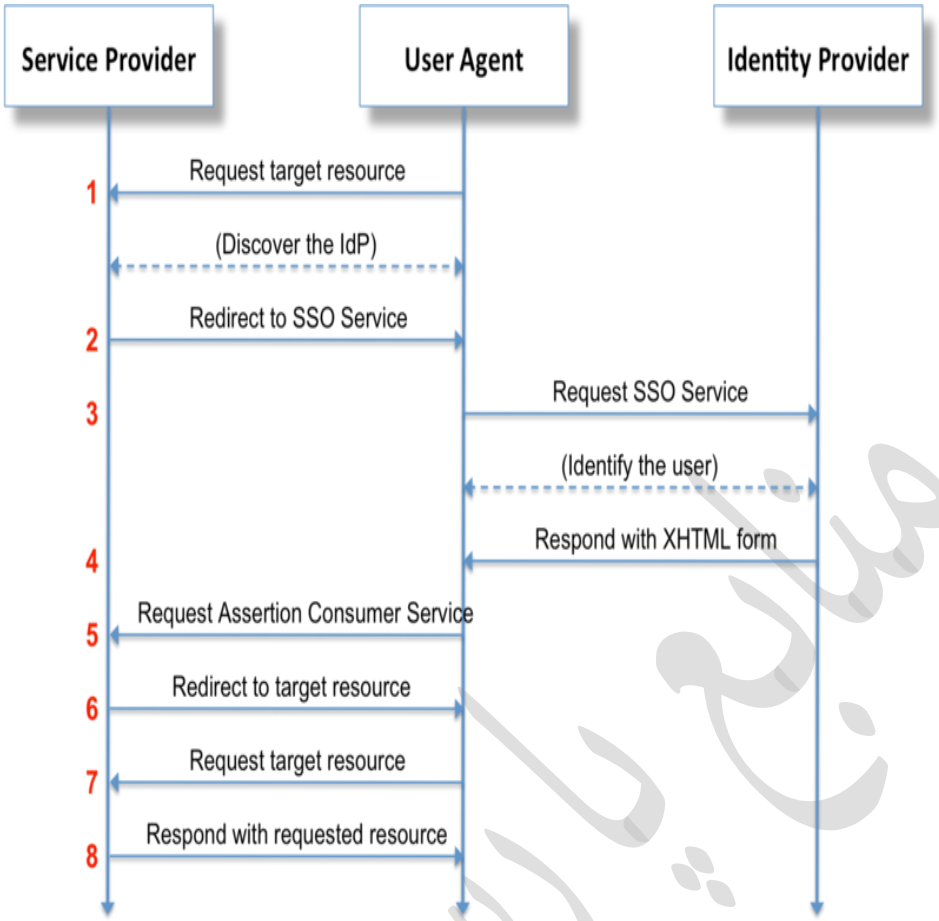
http://sp. example. com/myresource

ارائه‌دهنده سرویس یک بررسی امنیتی روی سمتی از منبع هدف انجام می‌دهد. اگر یک متن امنیتی معتبر در ارائه‌دهنده سرویس از قبل موجود باشد، به گام ۲-۷ می‌رود.

۲. مسیردهی مجدد به سرویس ورود تکی در ارائه‌دهنده هویت

ارائه‌دهنده سرویس، بهترین ارائه‌دهنده هویت کاربر را مشخص می‌کند و عامل کاربر را به سرویس ورود تکی در ارائه‌دهنده هویت مسیردهی مجدد می‌کند:

https://idp. example. org/SAML2/SSO/Redirect?SAMLRequest=request



شکل ۳-۵: احراز هویت ورود تکی به وب با زبان نشانه‌گذاری اثبات امنیت [۴].

۳. درخواست سرویس ورود تکی در ارائه‌دهنده هویت

عامل کاربر یک درخواست GET برای سرویس ورود تکی به ارائه‌دهنده هویت ارسال می‌کند که مقدار پارامتر SAML Request از رشته پرس‌وجوی URL در گام ۲ گرفته می‌شود. سرویس ورود تکی، Authn Request را پردازش می‌کند و یک بررسی امنیتی انجام می‌دهد. اگر کاربر یک متن امنیتی معتبر نداشته‌باشد، ارائه‌دهنده هویت کاربر را احراز هویت می‌کند.

۴. پاسخ با یک فرم XHTML

سرویس ورود تکی، درخواست و پاسخ را با یک متن شامل یک فرم XHTML اعتبارسنجی می‌کند:

```
<form method="post" action="https://sp. example. com/SAML2/SSO/POST" …>
< /"input type="hidden" name="SAMLResponse" value="response>
. . .
<input type="submit" value="Submit" />
</form>
```

۵. درخواست سرویسِ مصرف‌کننده اثبات در ارائه‌دهنده سرویس

عامل کاربر یک درخواست POST به سرویس مصرف‌کننده اثبات در ارائه‌دهنده سرویس ارسال می‌کند. مقدار پارامتر SAML Response از فرم XHTML در گام ۴ گرفته می‌شود.

۶. جهت‌دهی مجدد به منبع هدف

سرویسِ مصرف‌کننده اثبات، پاسخ را پردازش می‌کند، یک متن امنیتی در ارائه‌دهنده سرویس ایجاد می‌کند و عامل کاربر را مجدداً به منبع هدف جهت‌دهی می‌کند.

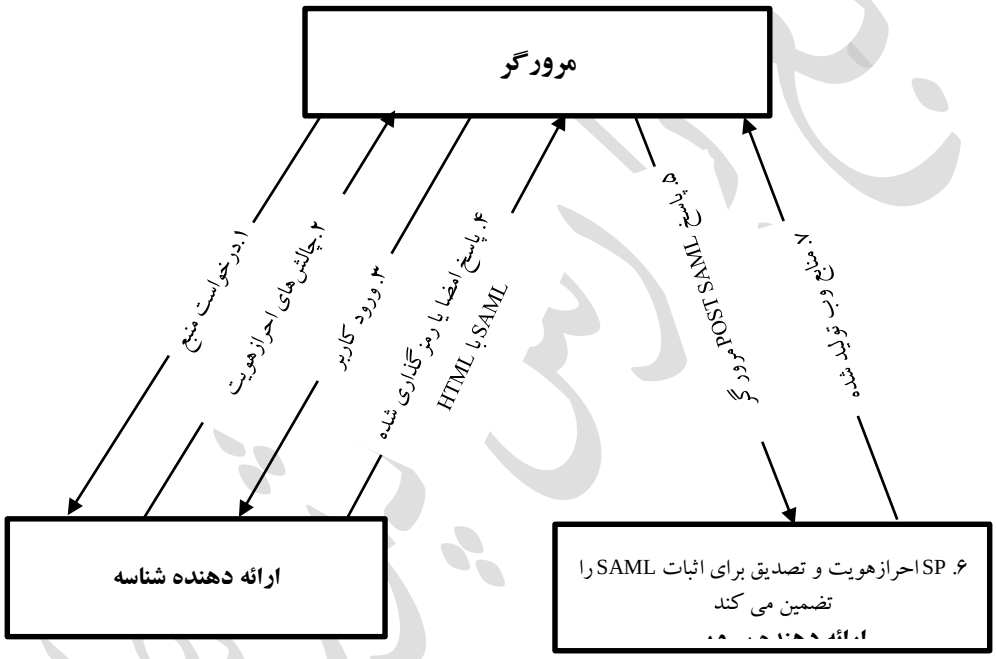
۷. درخواست مجدد منبع هدف در ارائه‌دهنده سرویس

عامل کاربر منبع هدف را در ارائه‌دهنده سرویس درخواست می‌کند (مجدداً):

https://sp.example.com/myresource

۸. پاسخ به منبع درخواست‌شده

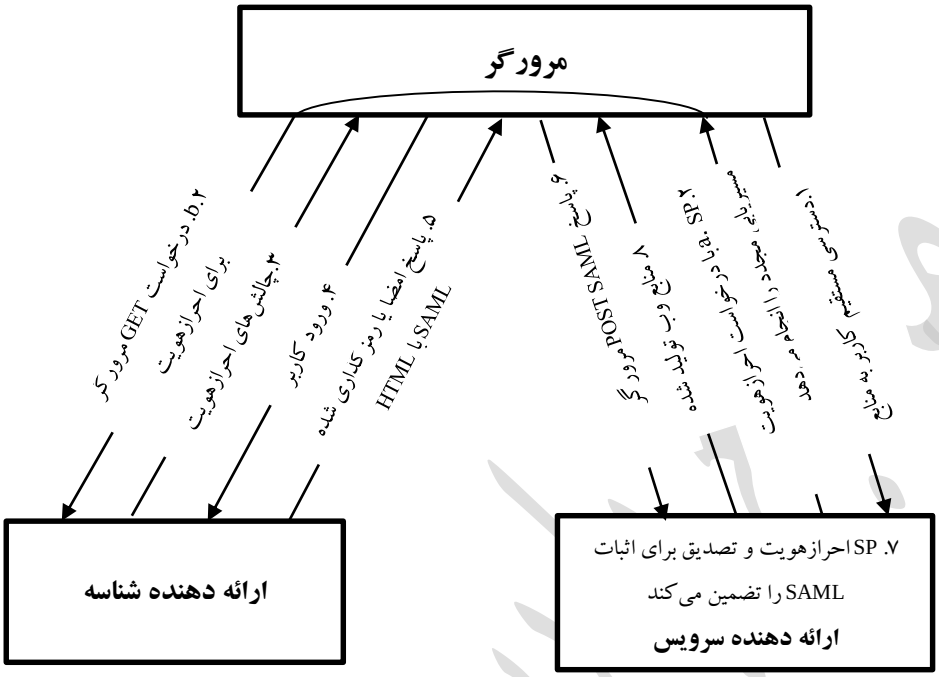
با وجود یک متن امنیتی، ارائه‌دهنده سرویس منبع را به عامل کاربر باز می‌گرداند. پروفایل ورود تکی مرورگر وب ممکن‌است توسط ارائه‌دهنده هویت یا ارائه‌دهنده سرویس آغاز شود. اگر توسط ارائه‌دهنده هویت آغاز شود، اثبات‌ها یا امضا شده یا رمزگذاری شده یا هر دو نوع هستند. در پروفایل ورود تکی مرورگر وب، همه‌ی اطلاعات اثبات یکبار با استفاده از هر یک از اتصالات و پروتکل‌های پروتکل انتقال ابرمتن به ارائه‌دهنده سرویس فرستاده می‌شوند. ارائه‌دهنده سرویس در صورت لزوم آنها را رمزگشایی می‌کند و آنرا برای یکپارچگی پیام در برابر امضا بررسی می‌کند. سپس جملات زبان نشانه‌گذاری توسعه‌پذیر، زبان نشانه‌گذاری اثبات امنیت را تجزیه می‌کنند و هر گونه صفاتی که عبور کرده است را جمع‌آوری و پس از آن، ورود تکی را با استفاده از سرویس مصرف‌کننده‌ی اثبات ایجاد می‌کنند. شکل ۳-۶ نشان می‌دهد که ارائه‌دهنده هویت اثبات زبان نشانه‌گذاری اثبات امنیت را آغاز کرده است.



شکل ۳-٦: فلوچارت اثبات زبان نشانه‌گذاری اثبات امنیت آغاز شده توسط ارائه‌دهنده هویت.

در صورتی که کاربر بدون عبور از طریق مدیر هویت مجتمع داخلی برای اولین بار به صفحه وب خارجی دسترسی یابد، ارائه‌دهنده سرویس نیازمند فرستادن درخواست زبان نشانه‌گذاری اثبات امنیت به ارائه‌دهنده هویت از طرف کاربر است. این روند ورود تکی نامیده می‌شود و توسط ارائه‌دهنده سرویس آغاز می‌شود. در این مورد، کاربر بدون یک اثبات زبان نشانه‌گذاری اثبات امنیت به یک صفحه وب خاص دسترسی دارد. ارائه‌دهنده سرویس، توسط یک درخواست زبان نشانه‌گذاری اثبات امنیت، کاربر را به صفحه وب مجتمع ارائه‌دهنده هویت باز می‌گرداند. پس از دریافت درخواست از ارائه‌دهنده سرویس، ارائه‌دهنده هویت، درخواست زبان نشانه‌گذاری اثبات امنیت را پردازش می‌کند. شکل ۳-۷ نشان می‌دهد که ارائه‌دهنده سرویس مورد استفاده را آغاز می‌کند.محبوب‌ترین مورد استفاده کسب‌وکار برای زبان نشانه‌گذاری اثبات امنیت، پروفایل ورود تکی مرورگر وب است که در رابطه با اتصال POST پروتکل انتقال ابرمتن و پروتکل درخواست احراز هویت استفاده می‌شود. زبان نشانه‌گذاری اثبات امنیت

توانایی مبادله اطلاعات احراز هویت و مجوز امن بین دامنه‌های امنیتی مختلف از جمله سازمان‌های مجزا یا حتی کمپانی‌ها را می‌دهد. در فرایند مبادله زبان نشانه‌گذاری اثبات امنیت، یک اثبات توسط ارائه‌دهنده هویت ساخته می‌شود که مسئولیت پاسخگویی نگهداری از شناسه کاربر را برعهده دارد و کاربر را از طریق ابزارهای گوناگون مانند نام‌کاربری/رمز عبور یا حتی فناوری‌های احراز هویت قوی‌تر مثل بیومتریک احراز هویت می‌کند.



شکل ۳-۷: فلوچارت اثبات زبان نشانه‌گذاری اثبات امنیت آغاز شده توسط ارائه‌دهنده سرویس [۴ و ۳۱].

۳-۶ سرویس‌های وب امنیتی

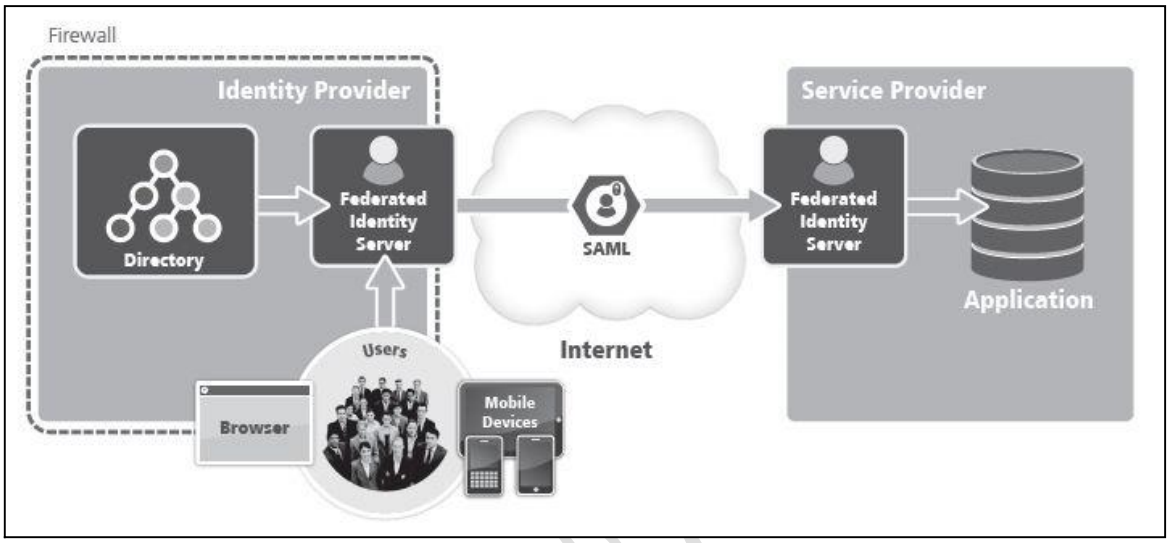
یک استاندارد OASIS است که توسط آی‌بی‌ام، مایکروسافت و وری‌ساین بوجود آمده است. سرویس‌های وب امنیتی چارچوبی برای اتصال اطلاعات سرآیند امنیتی به درخواست‌های SOAP سرویس‌های وب است. امنیت پیام SOAP سه جزء دارد: نشانه‌های احراز هویت، امضاهای دیجیتال و محرمانگی. سرویس‌های وب امنیتی یک چارچوب انعطاف‌پذیر برای تبادل انواع مختلف نشانه‌های امنیتی شامل نشانه‌های نام‌کاربری/رمز عبور XML، گواهی‌های x.509 و بلیط‌های کربروس ارائه می‌دهد. نشانه‌های زبان نشانه‌گذاری اثبات امنیت می‌تواند داخل سرآیندهای SOAP جاسازی شوند. سرویس‌های وب رمزگذاری شده‌ی امن، اجازه حفاظت از محرمانگی به‌طور مستقل از انتقال اصول را می‌دهد.

۳-۷ احراز هویت مجتمع

هنگامی که کاربر برای دسترسی در ارائه‌دهنده سرویس تلاش می‌کند، نرم‌افزار احراز هویت مجتمع یک درخواست احراز هویت زبان نشانه‌گذاری اثبات امنیت ایجاد می‌کند و آنرا به ارائه‌دهنده هویت مناسب کاربر تحویل می‌دهد. سپس نرم‌افزار احراز هویت مجتمع، درخواست احراز هویت را دریافت و اعتبارسنجی می‌کند. ارائه‌دهنده هویت، کاربر را احراز هویت و یک اثبات زبان نشانه‌گذاری اثبات امنیت ایجاد می‌کند که شناسه و ویژگی‌های کاربر را نشان می‌دهد. اثبات به صورت دیجیتالی برای تضمین

احراز هویت، امضا و رمزگذاری شده و ممکن است شامل داده‌های دیگر مورد نیاز توسط برنامه‌کاربردی مقصد شود. سپس اثبات به‌طور امنی به ارائه‌دهنده سرویس منتقل می‌شود.

نرم‌افزار احراز هویت مجتمع[۱] در ارائه‌دهنده سرویس، اثبات را دریافت، هویت آنرا بررسی و محتوای آنرا رمزگشایی می‌کند و سپس اطلاعات داخل اثبات (عامل شناسه کاربر) را با برنامه‌کاربردی به اشتراک می‌گذارد. سپس برنامه‌کاربردی از داده‌ها برای ورود کاربر و فعال‌سازی ورود تکی استفاده‌می‌کند. از دیدگاه کاربر، آنها تنها لینک برنامه‌کاربردی را کلیک می‌کنند و کار آغاز می‌شود که به صورت کامل از محل قرارگیری احراز هویت مجتمع در طرف آنها جدا شده است. شکل ۳-۸ این نرم‌افزار را نشان می‌دهد.



شکل ۳-۸: نرم افزار احراز هویت مجتمع [۱۷].

۳-۸ سرویس‌های وب مجتمع

سرویس‌های وب مجتمع، بخشی از سرویس‌های وب امن است که درون مشخصات قرار می‌گیرد و چگونگی استفاده از پروتکل‌های دیگر برای بدست‌آوردن راه حل‌های مدیریت هویت متحدشده، شامل موضوعات اداره و اطمینان را نشان می‌دهد. پروفایل‌های زبان نشانه‌گذاری اثبات امنیت و سرویس‌های وب امنیتی، دستورالعمل‌هایی برای پیاده‌سازی هستند که نیازهای کاهش خطر را مشخص می‌کنند. این پروتکل‌ها هنوز از ضعف‌های مربوط به تکنولوژی مانند نشر یا فاش‌سازی مرورگر، کوکی‌ها، سرویس‌های نام دامنه و NTP رنج می‌برند. همچنین هنوز موضوعاتی چون تهدیدهای اجتماعی مانند فیشینگ، وب‌سایت‌های کلاهبردار و ارائه‌دهندگان سرویس کلاهبردار وجود دارد. ارائه‌دهنده هویت، نقطه اصلی حملات جهت تلاش برای جمع‌آوری اعتبارات کاربر است. ارائه‌دهنده هویت می‌تواند با فریب، کاربران را به داخل وارد کند. زبان نشانه‌گذاری اثبات امنیت و سرویس‌های وب امنیتی خطر افشاسازی را کاهش می‌دهد، بنابراین اعتبارات کاربر نیاز به ارسال به ارائه‌دهندگان سرویس شخصی ندارد.

زبان نشانه‌گذاری اثبات امنیت و سرویس‌های وب امنیتی برای ایجاد یک محیط ورود تکی، انعطاف‌پذیرند. کارفرما می‌تواند برای احراز هویت کارمندان خود از زبان نشانه‌گذاری اثبات امنیت و سرویس‌های وب امنیتی استفاده کند و اثبات‌ها را به عنوان مثال به یک ارائه‌دهنده مزایای خارجی عبور دهد. این پروتکل‌ها یک لایه پیچیده اضافی برای توسعه‌دهندگان فراهم می‌کند. پیاده‌سازی این پروتکل‌ها نیاز به یک مکانیزم احراز هویت را کم نمی‌کند. با این حال، سازمان‌های بزرگ و پیچیده می‌توانند از این پروتکل‌ها

---

[۱] Federated identity software

به عنوان اعتباراتی بین سیستم‌های مختلف و سرتاسر نواحی سازمان استفاده‌کنند. توسعه پروتکل‌های مبتنی بر استاندارد برای ورود تکی تمایل به کاهش هزینه‌های توسعه دارد که باعث کاهش خطرات پیاده‌سازی معیوب می‌شود. همچنین هزینه‌های توسعه، پیاده‌سازی و نگهداری آنها را کم می‌کند. کاربران تمایل به کاهش تعداد اکانت‌ها و تعداد مرتبه‌های ورود دارند [۱۷ و ۴۵].

۹-۳ زبان نشانه‌گذاری اثبات امنیت و سرویس‌های وب مجتمع

یکی از ارزش‌های زبان نشانه‌گذاری اثبات امنیت، توسعه گزینه‌های موجود از جمله محصولات نرم‌افزاری احراز هویت مجتمع اقتصادی، انتخاب منابع باز و کتابخانه‌های توسعه‌یافته اقتصادی می‌باشد. سرویس‌های وب مجتمع بخشی از سرویس‌های وب یا دنباله‌ای از مشخصات سرویس‌های وب هستند که توسط مایکروسافت یا آی‌بی‌ام ایجاد شده‌اند. دنباله سرویس‌های وب شامل تعدادی از مشخصات برای پیاده‌سازی سرویس‌های وب در یک روش مناسب و امن می‌باشد. سرویس‌های وب مجتمع، دنباله مشخصات برای نشانه‌های امن صادره (مانند اثبات زبان نشانه‌گذاری اثبات امنیت) است که شامل صفت‌های مورد نیاز برای احراز هویت مجتمع و عملکرد قیاس‌پذیر ارائه‌شده برای قابلیت‌های ورود تکی به اینترنت با استفاده از زبان نشانه‌گذاری اثبات امنیت است.

زبان نشانه‌گذاری اثبات امنیت مزایای گوناگونی دارد. به دلیل اینکه زبان نشانه‌گذاری اثبات امنیت مجموعه‌ای از واسط‌های استاندارد قابل همکاری را ارائه می‌دهد، به سیستم‌های امنیتی و نرم‌افزارهای برنامه‌کاربردی اجازه توسعه و ارزیابی مستقل را می‌دهد. استانداردسازی واسط‌ها بین سیستم‌ها، امکان یکپارچگی سریع‌تر، ارزان‌تر و قابل اطمینان‌تر را می‌دهد. اکثر پروفایل‌های استفاده از زبان نشانه‌گذاری اثبات امنیت توسعه یافته‌اند که این باعث افزایش استفاده بی‌نهایت از انواع مختلف مدیریت دسترسی می‌شود. تولیدکنندگان نرم‌افزارهای امنیت، از داشتن طرح‌ها و پروتکل‌های استاندارد برای بیان اطلاعات امنیت سود می‌برند. توسعه‌دهندگان برنامه‌های کاربردی از تجزیه نرم‌افزار برای زیرساخت‌های امنیت اصلی بهره می‌برند. سرانجام، کاربران پایانی سود می‌برند، چرا که زبان نشانه‌گذاری اثبات امنیت، ورود تکی (توانایی استفاده از منابع اینترنت مختلف بدون ورود مجدد) را بهبود می‌دهد و باعث شخصی‌سازی بیشتر کاربر از طریق تجربه می‌شود که با این وجود می‌تواند باعث حفظ حریم خصوصی دوستانه شود. در زیر برخی مزایای مهم زبان نشانه‌گذاری اثبات امنیت آمده است:

پلت‌فرم خنثی: زبان نشانه‌گذاری اثبات امنیت، چارچوب‌های پیوسته امنیتی را از معماری‌های پلت‌فرم و پیاده‌سازی‌های فروشنده خاص تجرید می‌کند و باعث امنیت بیشتر منطق برنامه‌کاربردی که یک اصل مهم از معماری سرویس‌گراست می‌شود.

اتصال بی‌قاعده دایرکتوری‌ها: زبان نشانه‌گذاری اثبات امنیت به اطلاعات کاربر برای نگهداری و همگام‌سازی بین دایرکتوری‌ها نیاز ندارد.

بهبود فعالیت آنلاین برای کاربران پایانی: زبان نشانه‌گذاری اثبات امنیت امکان ورود تکی با اجازه به کاربران برای احراز هویت در یک ارائه‌دهنده هویت را می‌دهد و سپس به ارائه‌دهندگان سرویس بدون احراز هویت اضافی دسترسی پیدا می‌کند. بعلاوه، احراز هویت مجتمع (ارتباط شناسه‌های چندگانه) با زبان نشانه‌گذاری اثبات امنیت اجازه فعالیت بهتر به کاربر سفارشی‌سازی‌شده در هر سرویس درحال ترویج حریم خصوصی را می‌دهد.

کاهش هزینه‌های اجرایی برای ارائه‌دهندگان سرویس: زبان نشانه‌گذاری اثبات امنیت می‌تواند هزینه نگهداری اطلاعات اکانت برای استفاده مجدد یک فعالیت احراز هویت چندباره (مانند ورود با نام‌کاربری و رمز عبور) در سرتاسر سرویس‌های چندگانه را کاهش دهد. این بار سنگین به ارائه‌دهنده هویت منتقل می‌شود.

ریسک انتقال: زبان نشانه‌گذاری اثبات امنیت می‌تواند برای محول کردن مسئولیت‌پذیری مدیریت مناسب شناسه‌ها به ارائه‌دهنده هویت عمل کند که اغلب با مدل کسب‌وکار آن ارائه‌دهنده سرویس منطبق و سازگار است [۴۵ و ۴۶].

۳-۱۰ نسخه دوم زبان نشانه‌گذاری اثبات امنیت (SAML2)

نسخه دوم زبان نشانه‌گذاری اثبات امنیت (SAML2)، یک استاندارد برای ارتباط اثبات‌ها در مورد اصول، خصوصاً کاربران است. اثبات می‌تواند مفاهیم، که یک موضوع را احراز هویت می‌کند، ویژگی‌ها که با موضوع جمع‌آوری‌شده و یک تصمیم مجوز برای بدست‌آوردن منابع را شامل شود. مزایای اصلی SAML2 به صورت زیر است:

ورود تکی با SAML2: زبان نشانه‌گذاری اثبات امنیت یک استاندارد برای ورود تکی در سرتاسر دامنه ارائه می‌دهد. روش‌های دیگری نیز برای ورود تکی سرتاسر دامنه وجود دارد، اما آنها به راه حل‌های مناسب برای عبور از اطلاعات احراز هویت در سرتاسر دامنه‌ها نیاز دارند. SAML2 از ارائه‌دهنده هویت آغاز شده و از ورود تکی موجود در SAML1 پشتیبانی می‌کند. SAML2 همچنین از ارائه‌دهنده هویت آغاز شده با ورود تکی پشتیبانی می‌کند.

خروج تکی با SAML2: خروج تکی، کاربران را قادر به خروج صحیح از همه جلسات در یک دورنمای SAML2، حتی سرتاسر دامنه می‌کند. نه تنها انجام این کار منابع سیستم را ذخیره می‌کند بلکه می‌تواند تا زمانی که جلسه تمام شود آنها را به صورت ذخیره باقی نگه‌دارد. خروج تکی همچنین خطرات دزدی از جلسات ناامن را کاهش می‌دهد.

۳-۱۱ احراز هویت مجتمع

احراز هویت مجتمع ابزارهایی برای اشتراک اطلاعات شناسه بین شرکا ارائه می‌دهد. با وجود اینکه شرکا باید از ارائه‌کنندگان‌هویت مختلف برای کاربران مشابه استفاده‌کنند، برای اشتراک اطلاعات در مورد کاربر، شرکا باید قادر به شناسایی کاربر باشند. استاندارد SAML2، ارائه‌کنندگان‌هویت نام (ID نام) را به عنوان ابزارهایی برای بدست‌آوردن یک ارائه‌کننده‌هویت مشترک تعریف می‌کند.

دو جزء اصلی از دورنمای SAML2، ارائه‌دهنده هویت و ارائه‌دهنده سرویس هستند. ارائه‌دهنده سرویس یک نهاد سیستم شامل مجموعه‌ای از برنامه‌های‌کاربردی وب با مدیریت جلسه مشترک، مدیریت شناسه و مدیریت اعتبار است. ارائه‌دهنده هویت یک نهاد سیستم است که اطلاعات شناسه برای اصول را مدیریت و سرویس‌های احراز هویت را برای ارائه‌دهندگان سرویس مطمئن‌شدهٔ دیگر فراهم می‌کند. به عبارت دیگر، ارائه‌دهندگان سرویس، فعالیت‌های احراز هویت کاربر برای ارائه‌دهندگان سرویس را برون‌سپاری می‌کنند. ارائه‌دهنده هویت لیستی از ارائه‌دهندگان را نگه می‌دارد که کاربر در آن وارد شده است و درخواست‌های خروج برای ارائه‌دهندگان سرویس دیگر را عبور می‌دهد [۴۷].

۳-۱۲ مزایای احراز هویت ورود تکی

پس از پیاده‌سازی ورود تکی در برنامه‌های‌کاربردی وب، مزایای احراز هویت ورود تکی در ادامه بیان شده است:

- کاربران رمز عبورهای قوی‌تری انتخاب می‌کنند، بنابراین از نیاز به رمز عبورهای چندگانه و همگام‌سازی تغییرات اجتناب می‌شود.
- وقفه و فاصله‌های عدم فعالیت و آستانه‌های تلاش به‌طور یکنواخت و نزدیک‌تر به نقاط ورود کاربر بکار گرفته می‌شود.
- کارایی/هدر رفتن زمان هنگام فعالیت نکردن همهٔ اکانت‌های شبکه/کامپیوتر برای کاربران پایانی را بهبود می‌دهد.
- توانایی مدیریت برای مدیریت کاربران و پیکربندی کاربران به همه سیستم‌های مجتمع را بهبود می‌دهد.
- مخارج کلی اجرا در شروع مجدد رمز عبورهای فراموش‌شده روی پلت‌فرم‌ها و برنامه‌های‌کاربردی چندگانه را کاهش می‌دهد.
- به سهولت به کاربران مجموعه‌ای از اعتبارات را ارائه می‌دهد که امنیت را بهبود می‌دهد به‌طوری که کاربران به راحتی اعتبارات خود را به یاد می‌آورند و نیازی به نوشتن آنها ندارند. همچنین اجازه کارایی بیشتر به فرایند ورود کاربران را می‌دهد.
- زمان گرفته‌شده توسط کاربران برای ورود به برنامه‌های‌کاربردی و پلت‌فرم‌های چندگانه را کاهش می‌دهد [۴۸].

۳-۱۳ مزایای زبان نشانه‌گذاری اثبات امنیت

زبان نشانه‌گذاری اثبات امنیت مانند استانداردهای موجود دیگر معایب و مزایایی دارد. در ادامه تعدادی از مزایای زبان نشانه‌گذاری اثبات امنیت بیان و هر یک به طور مختصر توضیح داده شده‌اند:

- رمز عبورهای کاربر هرگز با فایروال روبرو نمی‌شود، بنابراین احراز هویت کاربر داخل فایروال انجام می‌شود و رمز عبورهای برنامه‌های کاربردی وب چندگانه مورد نیاز نیستند.
- برنامه‌های کاربردی وب با هیچ رمز عبوری به صورت مجازی قابل هک کردن نیستند، بنابراین کاربر باید در مقابل اولین IdM کلاس سازمانی احراز هویت شود که می‌تواند مکانیزم‌های احراز هویت قوی‌تری را شامل شود.
- ارائه‌دهنده سرویس آغازکننده ورود تکی زبان نشانه‌گذاری اثبات امنیت، دسترسی به برنامه‌های کاربردی وب را برای کاربران خارج از فایروال فراهم می‌کند. اگر یک کاربر خارجی درخواست دسترسی به یک برنامه‌کاربردی وب را داشته‌باشد، ارائه‌دهنده سرویس می‌تواند به‌طور خودکار کاربر را به یک پرتال احراز هویت مستقر در ارائه‌دهنده هویت مسیر دهی کند. پس از احراز هویت، کاربر برای دسترسی به برنامه‌های کاربردی تضمین می‌شود درحالی که ورود و رمز عبور آنها به صورت کاملاً امن در فایروال، قفل‌شده باقی‌می‌ماند [۴۹].

۳-۱۴ خطاهای رایج در زبان نشانه‌گذاری اثبات امنیت

هنگام استفاده از زبان نشانه‌گذاری اثبات امنیت ممکن است با خطاهایی مواجه شویم. برخی از این خطاها در ادامه آمده است:

۱- خطاهای مربوط به گواهی و تصدیق.
۲- خطاهای مربوط به احراز هویت و ورود.
۳- خطاهای مربوط به خروج.
۴- خطاهای مربوط به مسیریابی (جهت‌دهی) مجدد.
۵- خطاهای مربوط به ارائه و انتقال فریم.

۳-۱۵ زبان نشانه‌گذاری اثبات امنیت به عنوان یک استاندارد ابری امن

امروزه افراد حرفه‌ای در زمینه امنیت فناوری‌اطلاعات، زمان بیشتر و بیشتری برای انجام کارهای طاقت فرسایی چون مدیریت شناسه‌های کاربر صرف می‌کنند. حتی برای سازمان‌هایی که مکانیزم‌های احراز هویت پیشرفته اتخاذ می‌کنند، مدیریت شناسه هنوز هم یک موضوع پرهزینه و وقت‌گیر است. تنظیم رمز عبورها به تنهایی یک مقدار بیهوده از منابع فناوری‌اطلاعات را بازمی‌گرداند. همان‌طورکه بیشتر برنامه‌های کاربردی به سمت فایروال‌ها و SaaS مهاجرت می‌کنند، سرویس‌های وب و برنامه‌های کاربردی مبتنی بر ابر همچنان به ترقی ادامه می‌دهند. برای مبارزه با پراکندگی برنامه‌های کاربردی و به حداقل رساندن تاثیر بر کاربران نهایی، اکثر سازمان‌ها در حال حرکت به سمت راه حل‌های ورود تکی هستند. با این حال، راه حل‌های ورود تکی قبلی نمی‌تواند بسیاری از برنامه‌های کاربردی داخل سازمان را با آنهایی که در سمت فایروال هستند، منطبق کند. پلت‌فرم‌های کنترل دسترسی، ابزارهای احراز هویت دو عاملی و شناسه‌های مجتمع، همگی با بخش‌هایی از مشکل مقابله می‌کنند، اما راه حل یکپارچه‌ای وجود ندارد. برای جلوگیری از راه حل‌های رقابتی برای ایجاد هرج و مرج بیش از حد، بدنه‌های استانداردها به سمت ورود تکی و استانداردهای احراز هویت مجتمع، مانند زبان نشانه‌گذاری اثبات امنیت و OpenID جهت‌دهی شده‌اند.

زبان نشانه‌گذاری اثبات امنیت به سرعت ارائه دهندگان مبتنی بر ابر مانند گوگل، Salesforce.com و WebExرا جذب می‌کند و سازمان‌های سنتی مانند آی‌بی‌ام و مایکروسافت حمایت خود را پشت زبان نشانه‌گذاری اثبات امنیت می‌اندازند که این کار باعث حرکت پروتکل‌های ورود تکی به برنامه‌های کاربردی SaaS می‌شود. زبان نشانه‌گذاری اثبات امنیت یک چارچوب

است که امکان تبادل اطلاعات امنیت و هویت را می‌دهد. این راه حلی نیست که اجازه دسترسی یا اجرای شناسه را بدهد. تفاوت اصلی بین زبان نشانه‌گذاری اثبات امنیت و مکانیزم‌های شناسه دیگر اینست که زبان نشانه‌گذاری اثبات امنیت متکی بر "اثبات‌ها" در مورد هویت‌ها است. فرض بر این است که ارائه‌دهنده هویت سازنده‌ی اثبات است. همچنین ارائه‌دهنده هویت مسئول حفظ شناسه‌های کاربر، احراز هویت کاربران و تعیین‌کننده امتیازات می‌باشد.

زبان نشانه‌گذاری اثبات امنیت، سازمان‌ها را قادر به احراز هویت انتزاعی از برنامه‌های‌کاربردی می‌کند. به جای نیاز به مدیریت اطلاعات کاربری‌های متعدد برای انواع برنامه‌های‌کاربردی، زبان نشانه‌گذاری اثبات امنیت اجازه می‌دهد تا سازمان‌ها شناسه‌ها را از منابع داخلی به ارائه‌دهندگان سرویس خارجی گسترش دهند که باعث افزایش امنیت می‌شود. هنگامی که کاربران دارای چندین اعتبار مختلف برای برنامه‌های‌کاربردی مختلف هستند، میزان امنیت بسیار کم است و اگر یک هکر یکی از آنها را نقض کند، به‌طور موثری همه آنها را نقض کرده است که در صورت انتشار اعتبار نیز به همین مشکل وجود دارد. زبان نشانه‌گذاری اثبات امنیت به سازمان‌ها اجازه می‌دهد تا بتوانند مواردی که در ادامه آمده را انجام دهند:

- اثبات‌های احراز هویت را استانداردسازی کنند،
- شناسه‌ها را در یک مخزن منحصر به فرد نگه دارند،
- استفاده از احراز هویت انتزاعی به‌طوری که به یک برنامه خاص وابسته نباشد،
- گسترش شناسه‌ها از منابع داخلی به خارجی انجام شود،
- احراز هویت ورود به صورت محلی انجام شود.

مشکل زبان نشانه‌گذاری اثبات امنیت این است که افسانه‌های متعددی پیرامون آنچه که هست و آنچه که انجام می‌دهد وجود دارد. موضوع اصلی که آفت زبان نشانه‌گذاری اثبات امنیت است اینست که به عنوان یک راه حل مدیریت هویت کامل درنظر گرفته می‌شود که البته اینگونه نیست. کارهایی را که زبان نشانه‌گذاری اثبات امنیت نجام نمی‌دهد در ادامه توضیح داده شده‌اند:

- تعیین چگونگی امنیت سرورهای وب ارائه‌دهنده هویت.
- اطمینان از امنیت فرم‌های وب.
- استانداردسازی مکانیزم‌های احراز هویت.
- تعیین این که داده‌ها از کجا استخراج شده و چه شناسه‌ای درخواست‌شده است.
- مکانیزمی برای گزارش رویدادها وجود ندارد.

همان‌طور که در بالا ذکر شد، زبان نشانه‌گذاری اثبات امنیت فرض می‌کند که ارائه‌دهنده هویت باعث ایجاد یک اثبات دقیق می‌شود و اینکه ارائه‌دهنده هویت مسئول حفظ شناسه‌های کاربران، کاربران احراز هویت‌شده و تعیین امتیازات است. در ادامه، هر یک از موارد بالا را به‌طور اجمالی بررسی شده است. زبان نشانه‌گذاری اثبات امنیت چگونگی امنیت سرور وب ارائه‌دهنده هویت را مشخص نمی‌کند. زبان نشانه‌گذاری اثبات امنیت به منظور بررسی کیفیت ارائه‌دهنده هویت هیچ کاری انجام نمی‌دهد. هیچ چیز برای تضمین اینکه ارائه‌دهنده هویت با قوانین صنعت سازگار است و هیچ چیزی برای تعیین چگونگی اشکالات سرور وب ارائه‌دهنده هویت وجود ندارد. به عبارت دیگر، خود ارائه‌دهنده هویت می‌تواند لینک ضعیفی در زنجیره امنیتی کاربر ایجاد کند و زبان نشانه‌گذاری اثبات امنیت هیچ راهی برای شناختن آن ندارد.

تفاوت دیگر بین زبان نشانه‌گذاری اثبات امنیت و مکانیزم‌های امنیتی دیگر این است که چگونه شناسه‌ها اجرا شده‌اند. درحالی که رویکردهای اجرای شناسه متکی به مقامات گواهی مرکزی برای صدور گواهی‌های تضمین‌کننده ارتباطات ایمن از نقطه A به نقطه B است، زبان نشانه‌گذاری اثبات امنیت در یک روش مبتنی بر وب طراحی شده است. تحت زبان نشانه‌گذاری اثبات امنیت، هر نقطه در داخل شبکه می‌تواند باعث ایجاد یک حالت اثبات شود که شناسه‌ی یک کاربر یا مجموعه‌ای از داده‌ها را

شناسایی و بررسی می‌کند. پس از آن، برنامه‌کاربردی به پذیرش یک کاربر یا داده پاسخ می‌دهد که باید تصمیم بگیرد آیا آن اثبات مطمئن است یا نه. همان‌طور که دیده می‌شود، ارتباط ضعیف در زنجیره هویت زبان نشانه‌گذاری اثبات امنیت، یکپارچگی کاربران است.

زبان نشانه‌گذاری اثبات امنیت تضمین نمی‌کند که فرم‌های وب امن هستند. مسئله مهم دیگر، صفحه‌ی مربوط به آن کاربرانی است که اعتبار خود را وارد می‌کنند. برای اطمینان از امنیت، نیاز به دانستن چگونگی ساخته‌شدن صفحات وب است. از آنجا که موسسه SANS[۱]به این نتیجه رسیده است که اولویت فرم‌های مهم به عنوان یک نقطه ضعف در هنگام هک درنظر گرفته می‌شود، دانستن این موضوع مهم است که آیا فرم‌ها در صفحات احراز هویت برای تست نفوذ دقیق مقاومت می‌کنند یا نه. اگر آنها مقاومت ندارند، موضوع اصلی، اطمینان از احراز هویت قوی در محلی است که می‌تواند توسط یک وب سایت ناقص تضعیف شود.

زبان نشانه‌گذاری اثبات امنیت، مکانیزم‌های احراز هویت را استاندارد نمی‌کند، در حالی که این زبان، اثبات‌های هویت را استانداردسازی می‌کند، مثلاً نوع احراز هویتی (نام‌کاربری و رمز عبور، اس‌ام‌اس، تلفن، نشانه‌ها و غیره) که سازمان‌ها یا شرکت‌ها برای یکپارچه‌سازی احراز هویت استفاده می‌کنند، توسط این زبان اثبات نمی‌شود. تعیین این که داده‌ها از کجا استخراج شده و چه شناسه‌ای درخواست‌شده است را مشخص نمی‌کند. رد شدن از سیستم احراز هویت به اثبات زبان نشانه‌گذاری اثبات امنیت، اگر به درستی پیکربندی نشود، درب را به روی هکرها باز می‌کند. علاوه بر این، اگر یک اثبات نامعتبر باشد، ممکن است نتوان آنرا شناسایی کرد که بنابراین زبان نشانه‌گذاری اثبات امنیت هیچ استانداردسازی برای اثبات‌های XML امضا شده ارائه نمی‌دهد. این بدان معنی است که شما هیچ راهی برای بررسی و تایید اینکه گواهی از کجا آمده‌است، جایی که در آن ذخیره شده است، کسی که به آن دسترسی دارد و چگونگی دسترسی به کنترل و ثبت آن وجود ندارد. علاوه بر این، نمی‌توان مطمئن بود که چگونه شناسه ذخیره شده است، از چه پایگاه داده‌ای استخراج شده و امنیت آن پایگاه داده چگونه است.

زبان نشانه‌گذاری اثبات امنیت، مکانیزمی برای گزارش رویدادها ارائه نمی‌دهد. آخرین موردی که زبان نشانه‌گذاری اثبات امنیت انجام نمی‌دهد، اما مطلقاً برای امنیت و انطباق قوی لازم است، استانداردسازی و ثبت اجرا است. اگر حوادث در یک روش سازگار ثبت نشود، هیچ راهی برای بررسی انطباق اثبات‌ها با قوانین صنعت وجود ندارد. راه‌های زیادی برای پر کردن شکاف‌ها در سراسر زبان نشانه‌گذاری اثبات امنیت وجود دارد. یک راه برای مقابله با این مشکلات، استفاده از یک پلت‌فرم اجرای شناسه منحصر به فرد است. آنچه پلت‌فرم‌های اجرای شناسه انجام می‌دهند حرکت به داخل و نفوذ درون زبان نشانه‌گذاری اثبات امنیت است. با بکارگیری پلت‌فرم اجرای شناسه‌ی احراز هویت ایمن، یک احراز هویت پویا، دو عاملی داخلی و غیره در یک محیط ابری یک کار ساده است.

با یک پلت‌فرم اجرای شناسه منحصر به فرد احراز هویت امن، هنگامی که یک کاربر بر روی برنامه‌کاربردی کلیک می‌کند، برنامه از کاربر برای احراز هویت او و یا خودش سوال می‌پرسد. پلت‌فرم اجرای شناسه منحصر به فرد احراز هویت امن، احراز هویت را بررسی می‌کند و شناسه محلی را به یک اثبات زبان نشانه‌گذاری اثبات امنیت می‌دهد. همه این موارد در پشت صحنه انجام و در یک روش نامرئی دردسترس کاربران نهایی می‌باشد. پلت‌فرم اجرای شناسه احراز هویت امن، اولین پلت‌فرم منحصر به فرد صنعتی برای احراز هویت قوی یکپارچگی، ورود تکی، دسترسی و سرویس‌های مدیریت کاربر برای ابر، وب و برنامه‌های کاربردی شبکه اختصاصی مجازی[۲]است. این رویکرد منحصر به فرد، تضمین می‌کند که هر سازمان می‌تواند به راحتی به مقررات امنیتی و سازگاری با یک راه حل منحصر پایبند باشد که برای بدست آوردن الزامات امنیتی خاص پیکربندی شده‌اند.

---

[۱] SysAdmin, Audit, Networking, and Security

[۲] Virtual private network

ورود تکی رقابتی، احراز هویت و محصولات مدیریت شناسه، تنها یک تابع امنیتی- مانند احراز هویت، ورود تکی، دسترسی و مدیریت کاربر- ارائه می‌دهد و نمی‌تواند از ابر، وب و برنامه‌های‌کاربردی شبکه اختصاصی مجازی در یک پلت‌فرم واحد پشتیبانی کند. علاوه بر این، پلت‌فرم اجرای شناسهٔ احراز هویت امن، تنها نیازمند یک نمونه از احراز هویت کاربر است. از آن زمان به بعد، هر یک از برنامه‌های‌کاربردی پی‌درپی متصل به کاربر قادر به احراز هویت کاربر از طریق پلت‌فرم اجرای شناسه در پشت صحنه می‌باشد. با پلت‌فرم اجرای شناسه احراز هویت امن، احراز هویت قابل تنظیم است و هر برنامه‌کاربردی می‌تواند به‌طور مستقل و برای سطوح مناسب با دستور سیاست‌های سازمان پیکربندی شود. پلت‌فرم اجرای شناسه احراز هویت امن، هزینه‌های یکپارچه‌سازی را کاهش می‌دهد، امنیت را برای منابع متعدد (ابر، شبکه‌های اختصاصی مجازی، SaaS) افزایش، زمان استقرار را سریع و نرخ انطباق را افزایش می‌دهد. نتیجه نهایی این است که سازمان قادر به نفوذ در پلت‌فرم اجرای شناسه احراز هویت امن برای دسترسی به داخل سازمان، ابر، SaaS و ورود تکی وب در یک روش سالم، امن و متمرکز می‌باشد. همچنین سازمان به صورت همزمان، کنترل کاملی بر روی حساس‌ترین اطلاعات ارزشمند یعنی شناسه‌های کاربری افراد دارد. شکل ۹-۳ این فرایند را نشان می‌دهد [۵۰].

روش‌های ارائه شده هر یک دارای مزایا و معایبی می‌باشد که بسته به شرایط امکان استفاده یا عدم استفاده از هر یک را فراهم می‌کند. بعضی از روش‌ها مانند روش سنتی و ورود تکی کاهش‌یافته امنیت پایینی دارند. برخی دیگر مانند روش‌های ورود مبتنی بر ثبت نام و پر کردن فرم وقت گیر اند و زمان زیادی را برای ثبت‌نام و ورود کاربر می‌گیرند و برخی دیگر مانند کربوس، ورود تکی مبتنی بر کارت هوشمند یا بیومترک پیچیدگی زیاد و به تجهیزات و امکانات خاصی جهت پیاده‌سازی نیاز دارند، که امکان استفاده از آنها را مشکل می‌سازد. به علاوه اکثر این روش‌ها انعطاف‌پذیری کمی دارند و فقط می‌توان از آنها در شرایط خاصی استفاده کرد. در فصل بعدی روش ورود تکی مبتنی بر زبان شنانه‌گذاری اثبات امنیت ارائه می‌شود که تا حدودی برخی از این مشکلات و محدودیت‌ها را بر طرف می‌سازد.

۳-۱۶ نتیجه‌گیری

در این فصل ابتدا سیستم‌های ورود تکی و پس از آن هر یک از روش‌های ورود تکی به همراه مراحل کار هر یک مورد بررسی قرار گرفتند. در این فصل همچنین دو روش کربروس و پروتکل زبان نشانه‌گذاری اثبات امنیت به همراه مزایا و معایب هر یک، احراز هویت ورود تکی به وب با استفاده از زبان نشانه‌گذاری اثبات امنیت و فرایند انجام آن، سرویس‌های وب امنیتی، احراز هویت و سرویس‌های‌وب مجتمع، زبان نشانه‌گذاری اثبات امنیت و انواع نسخه‌های زبان نشانه‌گذاری اثبات امنیت بیان شد. در نهایت و پس از بیان نحوه پیاده‌سازی روش‌های ورود تکی، مزایای احراز هویت ورود تکی، زبان نشانه‌گذاری اثبات امنیت و خطاهای رایج آن ارائه‌شد.

در جدول ۳-۱ مقایسه‌ای بین روش‌های ارائه‌شده در این فصل، انجام‌شده است. این مقایسه به‌طور کلی از منظر دو معیار امنیت و احراز هویت انجام‌شده است. در پایان این فصل مبحث امنیت در محاسبات ابری مورد مطالعه قرار گرفت تا با کمک آن بتوان روی روش‌های برقراری امنیت در مدل پیشنهادی این پایان‌نامه کار کرد. با توجه به این مدل‌ها و با استفاده از نتایج به دست‌آمده، در مدل پیشنهادی سعی بر این است که از روش‌هایی که برای ارتباط قسمت‌های مختلف موضوع در این مدل‌ها استفاده شده است، الگوبرداری شود.

در ادامه و در فصل بعد مدل پیشنهادی ارائه می‌گردد. مدل پیشنهادی اصلاح شدهٔ روش زبان نشانه‌گذاری اثبات امنیت است که فرایند احراز هویت را بهبود می‌دهد. مدل پیشنهادی برخی معایب زبان نشانه‌گذاری اثبات امنیت را بهبود و کارایی مدل قبلی را بهبود می‌بخشد. مدل و مراحل انجام روش پیشنهادی در فصل بعد به طور کامل توضیح داده شده است.

جدول ۳-۱: مقایسه تعدادی از روش‌های ورود تکی

معیارهای مقایسه مدل ها	مبتنی بر ابر	انعطاف پذیری	امنیت
ورود تکی مبتنی بر کوکی	✓	X	✓
ورود تکی مبتنی بر کربروس	✓	X	✓
ورود تکی مبتنی بر درخواست	✓	X	✓
ورود تکی مبتنی بر کارت هوشمند	✓	X	✓
ورود تکی کاهش یافته	✓	✓	X
ورود تکی بین چند دامنه	✓	✓	✓
ورود تکی مبتنی بر جلسه	✓	X	✓
مدل پیشنهادی برای احراز هویت و ورود تکی	✓	X	✓

فصل چهارم
روش اصلاح شده پیشنهادی برای ورود تکی با استفاده از زبان نشانه‌گذاری اثبات امنیت

٤-١ مقدمه

فناوری‌های جدیدی برای ارائه چارچوب‌های استاندارد برای ورود تکی به اینترنت پدید آمده‌اند. این فناوری‌ها هنوز نسبتاً جدید هستند اما فرصت‌هایی برای سادگی فرایند نگهداری اعتبارات در مکان‌های چندگانه و برای عبور اعتبارات بین سازمان‌ها وجود دارد. زبان نشانه‌گذاری اثبات امنیت قدیمی‌ترین پروتکل احراز هویت مجتمع است که بیشترین سازگاری را دارد که قابلیت احراز هویت مجتمع سازمان را اثبات می‌کند. زبان نشانه‌گذاری اثبات امنیت تمایل به نشان‌دادن و تظاهر به یک مدل برای یک زمان طولانی را دارد. زبان نشانه‌گذاری اثبات امنیت به عنوان یک ابزار مهم در ذخیره امنیت سازمان بکار می‌رود. دلیل اصلی که پروژه‌های زبان نشانه‌گذاری اثبات امنیت شکست می‌خورند به این دلیل است که یا هزینه تاخیر آنها زیاد است یا پیاده‌سازی آنها می‌تواند پیچیده باشد و منابع آموزش‌دیده در زبان نشانه‌گذاری اثبات امنیت یک چالش می‌باشند. بسیاری از نگرانی‌ها با یک انجمن یا مجتمع‌سازی ورود تکی، موضوعات مدیریتی، مانند نیاز برای اطمینان برای برنامه های کاربردی که به‌طور مستقیم توسط زبان نشانه‌گذاری اثبات امنیت نظارت نشده‌اند وجود دارد. این موضوعات در چارچوب‌های بزرگ‌تر مانند کتابخانه و سرویس‌های وب مجتمع و شیبوه[1]نظارت می‌شوند. این چارچوب‌ها برای نمایش سه بخش صنعت شامل جنبه کسب‌وکار، تکنولوژی و آموزش در نظر گرفته می‌شوند.

سیستم‌های ورود تکی اینترنت نگرانی‌های حفظ حریم خصوصی شامل خطرات ردیابی کاربر و ارتباط اکانت یا فاش‌سازی اطلاعات برای ارائه‌دهندگان سرویس را ایجاد می‌کند. نگرانی دیگر، نگرانی‌های عملیاتی از جمله مقیاس‌پذیری، میزان تحمل شکست و تهاجم می‌باشد. هنگام ارزیابی راه حل‌های زبان نشانه‌گذاری اثبات امنیت، باید با در نظر گرفتن همه‌ی موارد مورد مطالعه سازمان، نیاز برای یکپارچه‌سازی با زیرساخت‌های موجود و اتصال به همه‌ی استانداردهای شناسه تضمین شود. امروزه راه حل‌های زبان نشانه‌گذاری اثبات امنیت بالغ و کاملتر شده و پیاده‌سازی ورود تکی به اینترنت مبتنی بر زبان نشانه‌گذاری اثبات امنیت به سرعت انجام می‌گیرند.

٤-٢ مدل پیشنهادی برای احراز هویت زبان نشانه‌گذاری اثبات امنیت در ورود تکی وب

مراحل انجام کار مدل پیشنهادی برای احراز هویت ارائه‌دهنده هویت زبان نشانه‌گذاری اثبات امنیت در جدول ۳-۱ آمده است. با توجه به این موضوع، در فصل بعد مدلی ارائه خواهد شد که در آن احراز هویت ارائه‌دهنده هویت در نظر گرفته شود و امنیت آن نیز تامین گردد. بدین صورت که درون سرآیند اثبات زبان نشانه‌گذاری اثبات امنیت، کلیدی تعبیه می‌شود که در هنگام فرایند ورود تکی و احراز هویت کاربر بین ارائه‌دهنده هویت و عامل کاربر مبادله شود و فرایند احراز هویت به صورت دو طرفه انجام شود.

---

[1] Shibboleth

جدول ٤-١: مدل احراز هویت ارائه‌دهنده هویت SAML

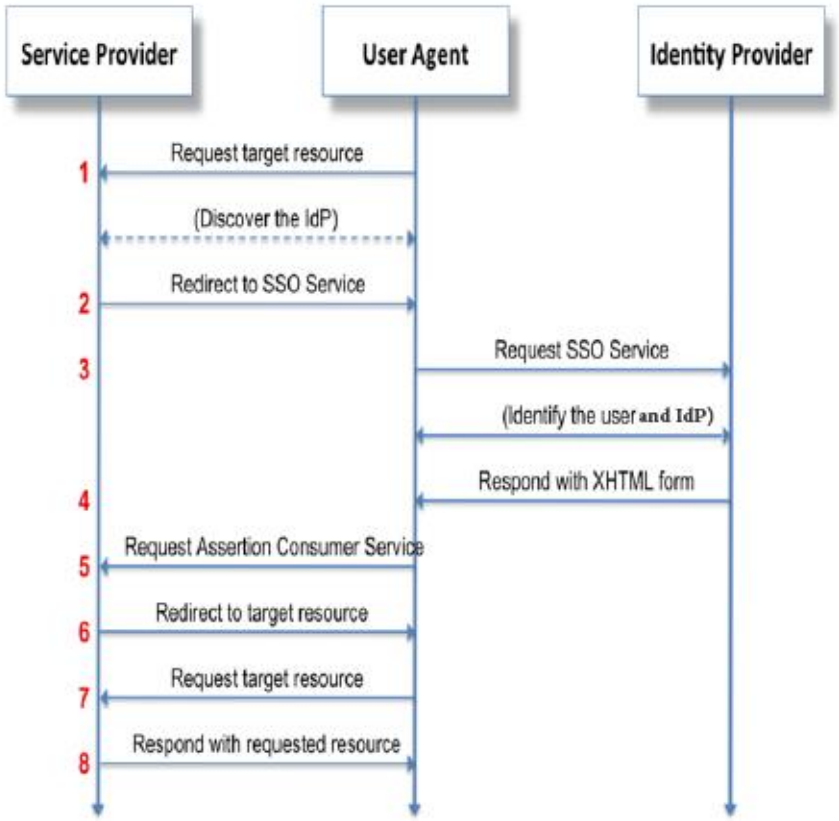
مراحل انجام کار	شرح فعالیت
گام ۱	عامل کاربر منبع هدف را از ارائه‌دهنده سرویس درخواست می‌کند.
گام ۲	ارائه‌دهنده سرویس، بهترین ارائه‌دهنده هویت کاربر را مشخص می‌کند و عامل کاربر را به سرویس ورود تکی در ارائه‌دهنده هویت مسیردهی مجدد می‌کند.
گام ۳	عامل کاربر یک درخواست برای سرویس ورود تکی به ارائه‌دهنده هویت ارسال می‌کند.
گام ۴	فرایند احراز هویت (دو طرفه) عامل کاربر و ارائه‌دهنده هویت انجام‌می‌شود
گام ۵	سرویس ورود تکی، درخواست و پاسخ را با یک متن شامل یک فرم XHTML اعتبارسنجی می‌کند.
گام ۶	عامل کاربر درخواست وپاسخ را به ارائه‌دهنده سرویس ارسال می‌کند.
گام ۷	ارائه‌دهنده سرویس، پاسخ را پردازش می‌کند و در صورت معتبر بودن، اجازه دسترسی را به عامل کاربر می‌دهد و عامل کاربر را مجدداً به منبع هدف جهت‌دهی می‌کند.
گام ۸	عامل کاربر مجدداً منبع هدف را در ارائه‌دهنده سرویس درخواست می‌کند.
گام ۹	در صورت احراز هویت موفق و برقراری ارتباط، ارائه‌دهنده سرویس منبع را به عامل کاربر باز می‌گرداند.

برای انجام ورود تکی با استفاده از زبان نشانه‌گذاری اثبات امنیت مدل ۴-۱ ارائه‌شده است. در این مدل، عامل کاربر از طریق استاندارد زبان نشانه‌گذاری اثبات امنیت، اقدام به ورود تکی به ابر می‌نماید و سرویس‌های مورد نیاز خود را درخواست و پس از احراز هویت و ورود موفقیت‌آمیز به وب، از آنها استفاده‌می‌کند. در این مدل فرض‌می‌شود که ارائه‌دهنده هویت، کلید منحصر به فردی برای ارتباط با هر عامل کاربر که قصد ورود و احراز هویت دارد تولیدمی‌کند. به هر عامل کاربر نیز در هنگام ورود یک کلید تخصیص داده‌می‌شود که هنگام ورود برای احراز هویت دو طرفه بین خود و ارائه‌دهنده هویت مبادله می‌شود. این کلید تا پایان کار و تا هنگام خروج تکی، نزد دو طرف باقی خواهد ماند. همچنین برای امنیت بیشتر فرایند، می‌توان از یک مهر زمان استفاده کرد که در صورت منقضی‌شدن مهر زمان، اجازه ورود به عامل کاربر داده نشود. همچنین برای مقابله با منقضی‌شدن زمان، دو راه حل وجود دارد: راه حل اول استفاده از زمان انقضای طولانی‌تر است و راه حل دوم اینست که اگر عامل کاربر وارد شده‌باشد و زمان انقضا تمام و یا نزدیک به انقضا است، سرویس یک مهر زمان با زمان انقضای جدید صادر کند.

٤-٣ مراحل انجام مدل پیشنهادی

همان‌طور که در روش سنتی احراز هویت زبان نشانه‌گذاری اثبات امنیت مشاهده شد تنها عامل کاربر احراز هویت می‌شود و امنیت ارائه‌دهنده سرویس نیز تامین می‌شود. این فرایند همیشه با فرض امن و مطمئن بودن ارائه‌دهنده هویت، آغاز و مبادله اطلاعات انجام‌می‌شود و این درصورتی است که هیچگونه اطلاعاتی از امنیت ارائه‌دهنده هویت در دست نیست. روش بهبود یافته احراز هویت کاربران توسط زبان نشانه‌گذاری اثبات امنیت در ورود تکی وب به این صورت است که عامل کاربر یک سرویس را از ارائه‌دهنده سرویس درخواست می‌کند. ارائه‌دهنده سرویس، بهترین ارائه‌دهنده هویت کاربر را مشخص می‌کند و عامل کاربر را به سرویس ورود تکی در ارائه‌دهنده هویت مسیردهی مجدد می‌کند. ارائه‌دهنده سرویس یک اثبات هویت از ارائه‌دهنده هویت درخواست می‌کند. در این مرحله احراز هویت دو طرفه بین عامل کاربر و ارائه‌دهنده هویت توسط کلیدهای منحصر به فردی که بین آنها مبادله می‌شود انجام می‌گیرد. بدین صورت که عامل کاربر اطلاعات را با کلید خود امضا می‌کند، اطلاعات در ارائه‌دهنده

هویت خوانده می‌شود و عامل کاربر اعتبارسنجی می‌شود، در صورتی که عامل کاربر معتبر بود، پاسخ به عامل کاربر برگشت داده‌می‌شود. همراه با این پاسخ دو کلید منحصر به فرد نیز به عامل کاربر تخصیص داده می‌شود.



شکل ٤-1: احراز هویت ورود تکی به وب با زبان نشانه‌گذاری اثبات امنیت [۴].

این دو کلید به صورت تصادفی و خودکار توسط یک تولیدکننده کلید منحصر، ایجاد و ساخته می‌شوند. پس از اینکه کلیدها ایجاد شدند، توسط یکی از الگوریتم‌های رمزگذاری، رمزگذاری می‌شوند و سپس در سرآیند اثبات زبان نشانه‌گذاری اثبات امنیت جاسازی می‌شوند. ارائه‌دهنده هویت یک نسخه از این کلیدها را به طور امن به ارائه‌دهنده سرویس که عامل کاربر را به او جهت‌دهی کرده است ارسال می‌کند و همان کلیدها را نیز به عامل کاربر تخصیص می‌دهد. هنگامی که اثبات بین عامل کاربر و ارائه‌دهنده حویت مبادله می‌شود هر یک از طرفین با رمزگشایی اطلاعات توسط کلید خود می‌توانند به پاسخ و کلیدهای جاسازی‌شده دسترسی یابند. عامل کاربر اطلاعات را دریافت و با کلید خود رمزگشایی و این کلیدها را دریافت می‌کند. پس از رمزگشایی، عامل کاربر به درخواست اثبات ارائه‌دهنده سرویس پاسخ می‌دهد. همراه با این پاسخ ارائه‌دهنده سرویس برای اجازه دسترسی عامل کاربر به سرویس‌ها، دو کلید از عامل کاربر درخواست می‌کند. عامل کاربر دو کلیدی که توسط ارائه‌دهنده هویت به وی تخصیص داده شده بود را به ارائه‌دهنده سرویس نشان می‌دهد. در صورتی که این دو کلید با دو کلیدی که بین ارائه‌دهنده هویت و ارائه‌دهنده سرویس مبادله شده است یکسان باشد، عامل کاربر نیز برای ارائه‌دهنده سرویس و ارائه‌دهنده هویت احراز هویت شده است و براساس این اثبات و پاسخ، ارائه‌دهنده سرویس می‌تواند یک تصمیم کنترل دسترسی ایجاد کند. سپس عامل کاربر مجدداً سرویس مورد نظر را درخواست و اجازه دسترسی به سرویس‌ها به عامل کاربر داده شود و در نهایت با اعتبارسنجی موفق عامل کاربر، ارائه‌دهنده سرویس، منبع یا سرویس مورد نظر را به عامل کاربر باز می‌گرداند.

بر اساس این مدل، فرایند احراز هویت به صورت دو طرفه انجام می‌شود و هم عامل کاربر خود را برای ارائه‌دهنده هویت و سرویس و هم ارائه‌دهنده هویت و سرویس خود را برای عامل کاربر احراز هویت می‌کنند. مزیت این مدل نسبت به مدل‌های قبلی این است که احراز هویت دو طرفه است که احتمال احراز هویت اشتباه یا جعلی توسط یک ارائه‌دهنده هویت جعلی را کاهش و امنیت را بالا می‌برد. همچنین مدل احراز هویت ساده و در هر مکانی که امکان دسترسی به اینترنت وجود داشته باشد عامل کاربر بدون نیاز به استفاده از هر برنامه کاربردی خاصی می‌تواند به راحتی به آن دسترسی و از آن استفاده کند. با توجه به شکل ۴-۱، مراحل شکل ۴-۲ برای انجام فرایند احراز هویت ورود تکی به وب با استفاده از زبان نشانه‌گذاری اثبات امنیت دنبال می‌شود.

گام یک: عامل‌کاربر یک سرویس را از ارائه‌دهنده‌سرویس درخواست می‌کند. در واقع، عامل‌کاربر وارد ابر می‌شود و منبع هدف را از ارائه‌دهنده‌سرویس درخواست می‌کند (به عنوان مثال ورود به صفحه اصلی یک سایت).

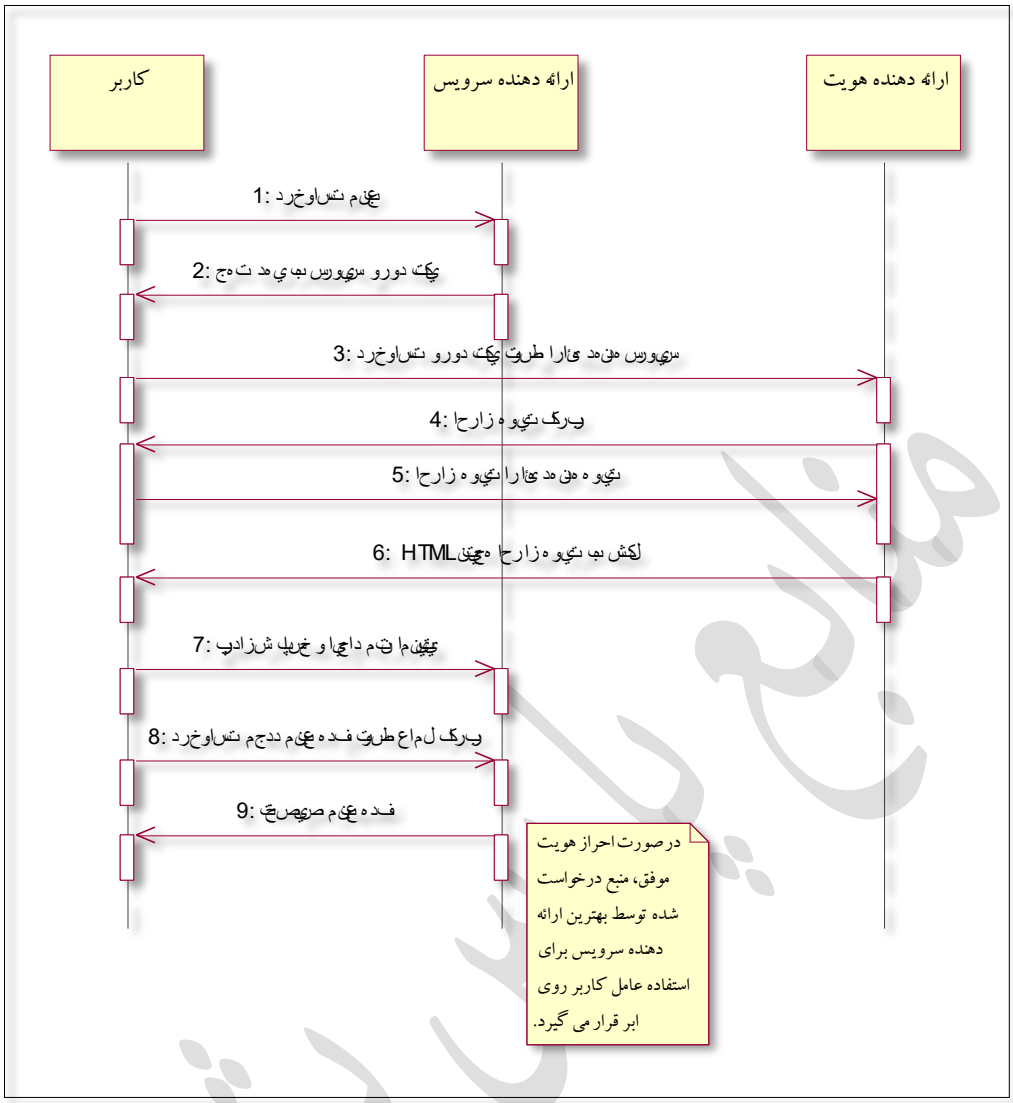
گام نهم: در صورتی احرازهویت با موفقیت انجام شود و ارتباط به درستی برقرار گردد، منبع درخواست‌شده توسط عامل‌کاربر روی ابر قرار می‌گیرد و مناسب‌ترین ارائه‌دهنده‌سرویس منبع را به عامل کاربر باز می‌گرداند.

شکل ٤-۲: مراحل انجام فرایند احراز هویت ورود تکی به وب با استفاده از زبان نشانه‌گذاری اثبات امنیت.

در هنگام ورود عامل کاربر به محیط ابر، درخواست به ارائه‌دهنده سرویس ارسال می‌شود. ارائه‌دهنده سرویس درخواست را به بهترین ارائه‌دهنده هویت ارسال می‌کند. سرور احراز هویت، عامل کاربر را احراز هویت می‌کند، همچنین با کلیدی که بین خود و عامل کاربر مبادله می‌کند، خود نیز برای عامل کاربر احراز هویت می‌شود که در صورت موفقیت‌آمیز بودن این فرایند اجازه ورود و تبادل اطلاعات به عامل کاربر داده‌می‌شود. با توجه به همه این موارد گفته شده دو حالت وجود دارد که در ادامه توضیح داده شده‌اند:

حالت اول: اگر کلید مبادله‌شده بین عامل کاربر و سرور احراز هویت با یکدیگر منطبق باشند و بتوانند یکدیگر را به درستی احراز هویت کنند، هیچ مشکلی وجود ندارد و ارتباط بین عامل کاربر و سرور احراز هویت برقرار و تبادل اطلاعات انجام‌می‌شود و پس از طی مراحل فرایند سرویس یا سرویس‌های خواسته‌شده توسط عامل کاربر، توسط سرورهای ارائه‌دهنده سرویس به او داده‌می‌شود. همچنین مراحل انجام کار در نمودار توالی شکل ۴-۳ آورده شده است.

حالت دوم: اگر کلید مبادله‌شده بین عامل کاربر و سرور احراز هویت با یکدیگر منطبق نباشد و عامل کاربر یا سرور احراز هویت، هر یک نتوانند دیگری را احراز هویت کند، فرایند برقرار نمی‌شود و اجازه ورود به کاربر داده نمی‌شود و بنابراین سرویس‌های درخواست‌شده به او تعلق نمی‌گیرد. در این حالت سرور ارائه‌دهنده سرویس با توجه به درخواست دریافت شده از عامل کاربر، پیامی را به او بازمی‌گرداند. شکل ۴-۳ الگوریتم این فرایند را به تصویر کشیده‌است.



شکل ٤-۳: نمودار توالی مدل پیشنهادی.

همان‌طور که مشاهده می‌شود کاربران در خارج از محدوده، از طریق اینترنت به عامل‌کاربر که خود می‌تواند شامل یک یا چند سرور باشد، دسترسی پیدا می‌کنند و عامل‌کاربر با سرورهای ارائه‌دهنده سرویس و احراز هویت ارتباط برقرار می‌کند. در واقع، کاربر به‌طور مستقیم با سرورهای ارائه‌دهنده سرویس و احراز هویت در ارتباط نیست. عامل کاربر دارای آدرس‌های IP از پیش تعریف‌شده است که کاربر در هنگام نیاز به دستیابی به یک سرویس به یکی از عامل‌های‌کاربر دسترسی پیدا می‌کند و با برقراری ارتباط با آن و در صورت احراز هویت موفق عامل‌کاربر برای سرور احراز هویت خاص، ارتباط برقرار می‌شود و سرورهای ارائه‌دهنده سرویس، سرویس درخواست‌شده را به عامل‌کاربر باز می‌گرداند. با توجه به محیط‌های آزمایشگاهی و امکانات و تجهیزات (خصوصاً شبکه) موجود و در دسترس، تنها مدل‌سازی این طرح امکان پذیر است و امکان پیاده‌سازی آن وجود ندارد. کاربران از طریق اینترنت و از نقاط مختلف به عامل‌های‌کاربری که در اطراف ابر قرار دارند دسترسی پیدا می‌کنند. روند کار این‌گونه است که از هر عامل‌کاربری که وجود دارد سه نسخه در دسترس است که در صورت خراب یا هک شدن یکی از آنها، به راحتی می‌توان آنها را به‌روزرسانی یا از دیگری استفاده کرد.

٤-٤ شبیه‌سازی مدل پیشنهادی

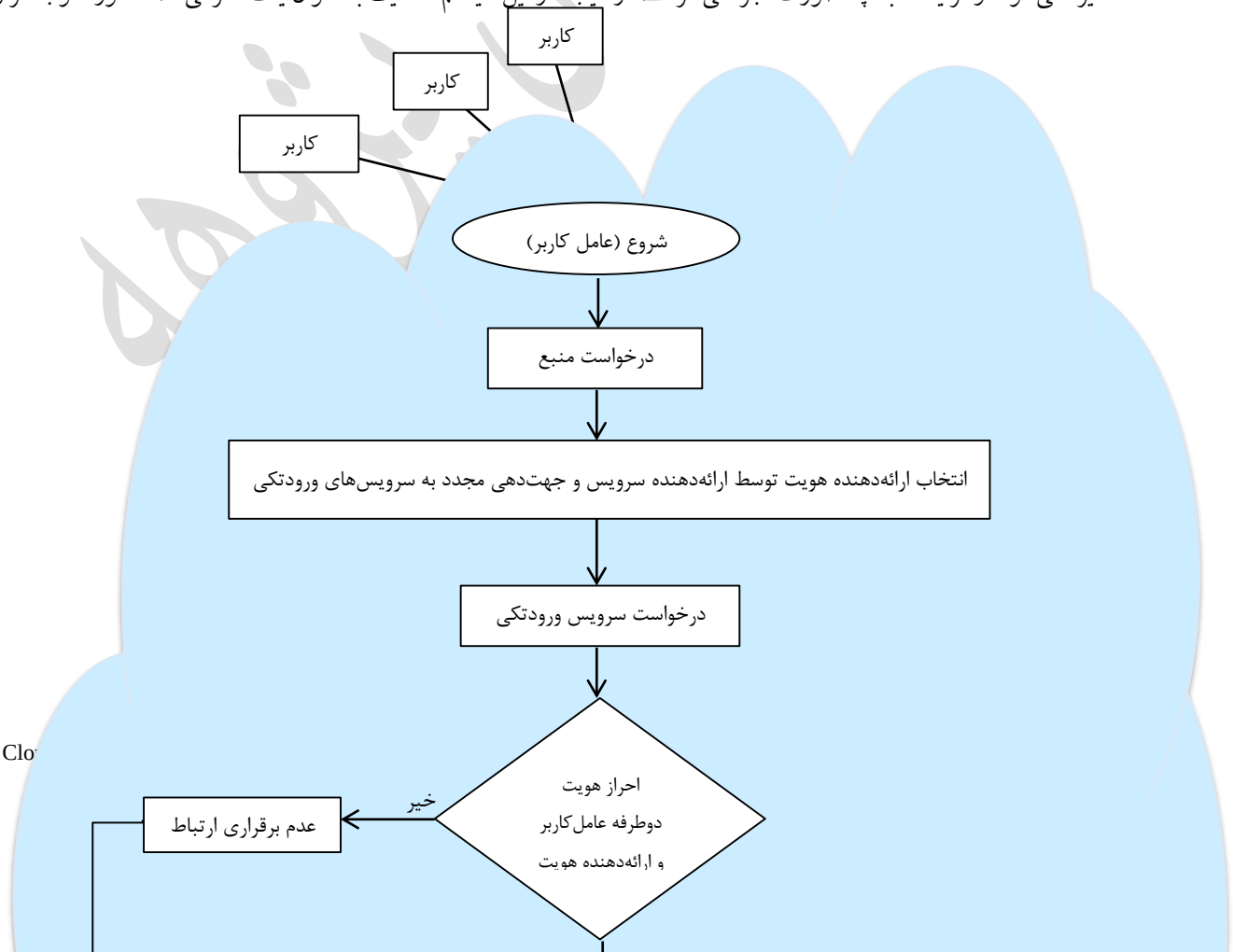
پیاده‌سازی این مدل نیازمند یک محیط ابر می‌باشد که خود دارای سرورهایی برای احراز هویت، ارائه سرویس و عامل کاربر (مثلاً مرورگر وب) است. برای شبیه‌سازی و نمایش منطق کار از شبیه‌سازی ابری به نام کلود سیم[1]استفاده شده است. کلود سیم یک زبان مبتنی بر جاوا است و نیاز به نصب و اجرای برنامه‌های کاربردی نت بینز[2] و JDK می باشد. کلود سیم یک چارپوب شبیه‌سازی گسترده و انعطاف‌پذیر است که مدل‌های یکپاچه را قادر به شبیه‌سازی و آزمایش زیرساخت‌های محاسبات ابری موجود و سرویس‌های مدیریت می‌سازد. چارچوب شبیه‌سازی ویژگی‌های جدیدی ارائه می‌دهد. برخی از این ویژگی‌های جدید در زیر ذکر شده‌اند:

- پشتیبانی برای مدل‌سازی و تعمیر زیرساخت محاسبات ابری در مقیاس بزرگ،
- یک پلت فرم خود شمول برای مدل‌سازی مراکز داده، سرویس‌های واسط، زمان‌بندی و سیاست‌های تخصیص منبع،
- قابلیت ماشین مجازی با هدف ایجاد و مدیریت سرویس‌های مجازی‌شده میزبان، مستقل و چندگانه روی مراکز داده،
- انعطاف‌پذیری برای تعویض اشتراک زمان و فضا بین تخصیص پردازنده مرکزی برای سرویس‌های مجازی شده.

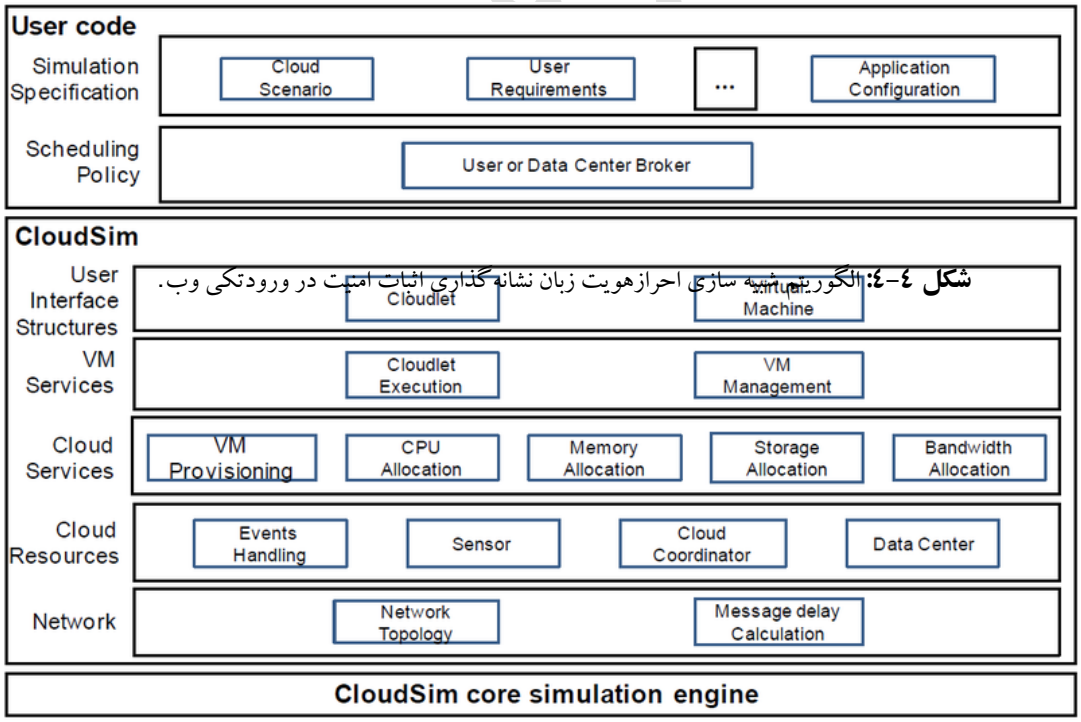
نمای کلی پلت‌فرم کلود سیم در شکل ۴-۵ آمده است. پس از اجرای نرم افزار ابتدا باید پارامترهای مورد نظر و خواسته‌شده توسط نرم افزار را تنظیم کرد. شکل ۴-۶ تعدادی از این پارامترها را نشان می‌دهد. همانگونه که در بالا اشاره شد، شبیه ساز کلود سیم از زبان جاوا پشتیبانی می کند. نمای اولیه نرم افزار در حال اجرا در شکل ۴-۷ نشان داده شده است. همچنین توابع و کتابخانه‌های کلود در شکل زیر نشان داده شده است.

٤-٥ مدل امنیت داده‌ها در محاسبات ابر

با توجه به نیاز مدل پیشنهادی و مباحث امنیتی مورد مطالعه قرارگرفته، برای بررسی امنیت باید به این نکته اشاره کرد که در محاسبات متمرکز، کنترل کامل بر روی داده‌ها و فرایندها وجود دارد، اما در محاسبات مجازی مشتریان نمی‌دانند که داده‌ها در کجا ذخیره می‌شوند و فرایندها به چه صورت اجرا می گردند. در نتیجه در این سیستم‌ها امنیت به عنوان یک نگرانی عمده مورد توجه قرار

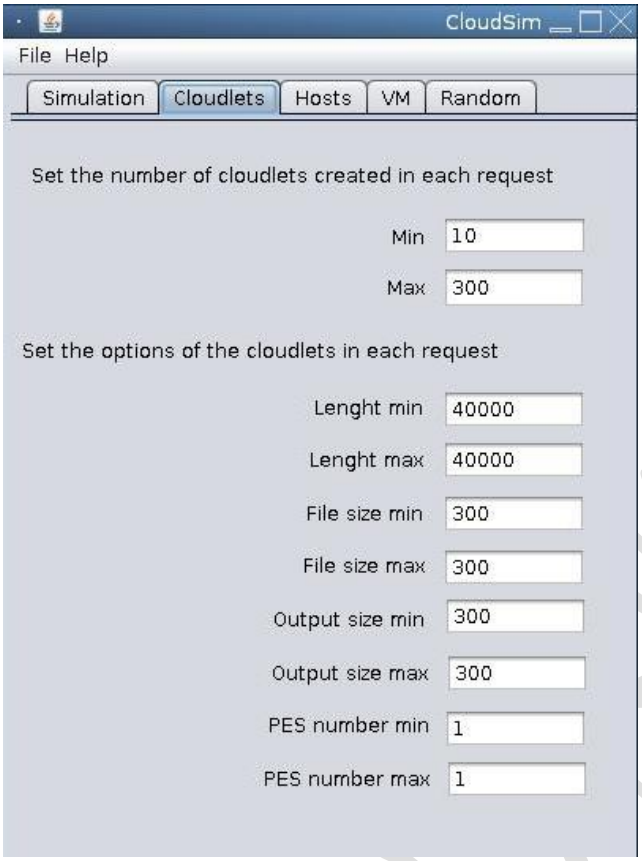


[1] Clo

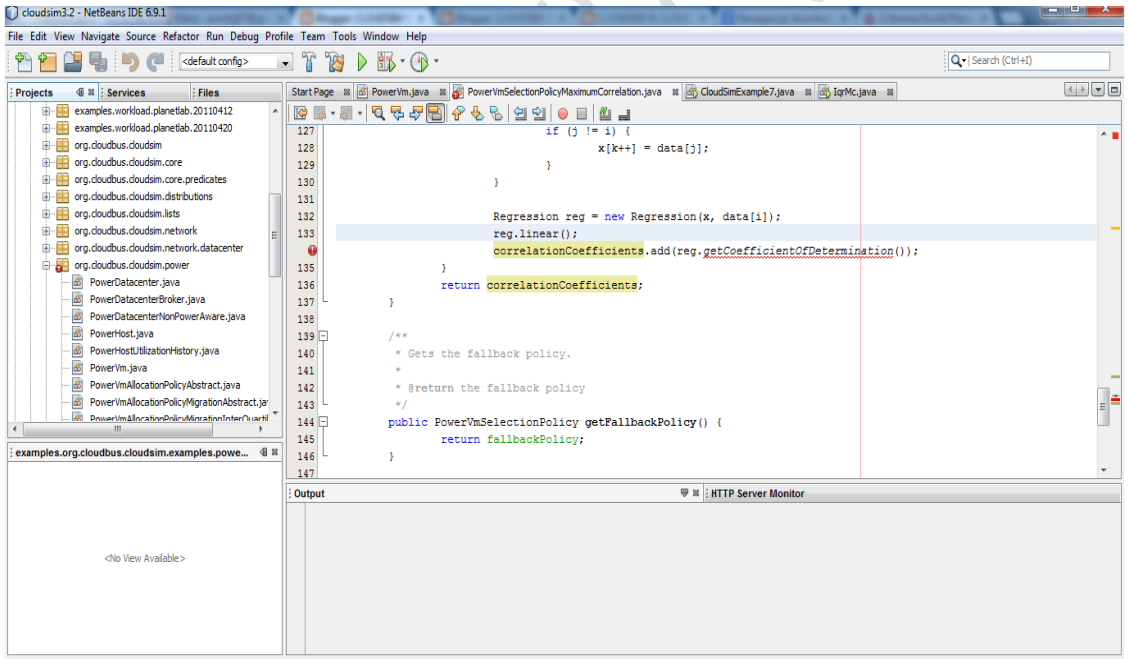


شکل ٤-٤: الگوریتم شبیه سازی احرازهویت زبان نشانه‌گذاری اثبات امنیت در ورودتکی وب.

شکل ٤-٥: یک نمای کلی از پلت‌فرم نرم افزار کلود سیم.



شکل ٤-٦: محل تنظیم پارامترهای شبیه ساز کلود.



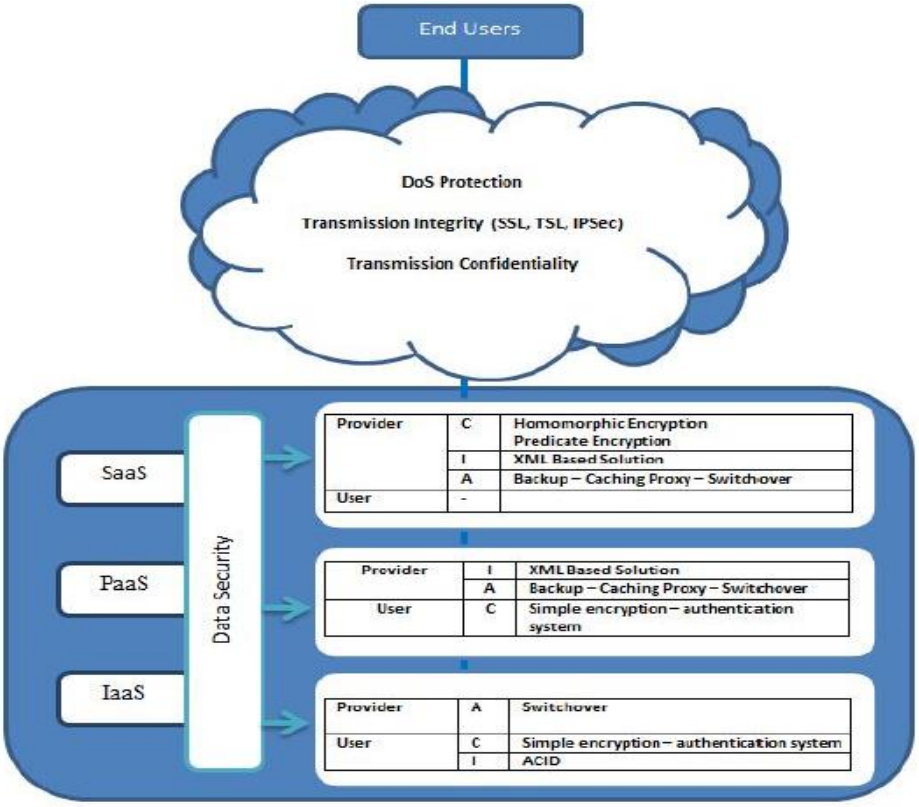
شکل ٤-٧: نمای اولیه شبیه ساز کلود.

می‌گیرد. معماری امنیتی باز[۱]چارچوب آزادی فراهم می‌کند که به راحتی در برنامه‌های کاربردی، برای جامعه معماری امنیتی یکپارچه شده است. در [۱۰]، اجزایی از معماری‌های محاسبات ابری همراه با توصیف عناصر وجود دارد که آن را امن می‌سازد. در

[۱] Open Security Architecture

[۲] Denial-of-Service

این مقاله، مدل به یک مدل جدید برای امنیت داده‌ها در محاسبات ابر افزایش یافته است. در مدل ارائه شده، تمام تکنیک‌هایی که برای حفاظت از داده‌ها در تمام سطوح از محیط‌های ابر از دسترسی‌های ناامن مفید هستند به طور خلاصه بیان شده‌اند. روش‌های مختلفی برای حفاظت از انواع مختلف ارائه‌دهندگان سرویس ابر در شکل ۴-۸ در جزئیات شرح داده شده است.



شکل ٤-٨: مدل امنیت داده در محاسبات ابری [۵۱].

کاربران نهایی از طریق اینترنت به عنوان یک نقطه ورودی به محیط ابر دسترسی دارند که این ورودی باید امن باشد. ورود قوی برای دسترسی به ابر برای ارائه‌دهنده ابر سودمند است اما به ضرر کاربران است. این مدل باید امنیت روی کاربران نهایی و در ابرهای یکسان را تضمین کند. ابر نیاز به ایمن سازی برای هر کاربر با مقاصد مخرب دارد که ممکن است برای به دست آوردن دسترسی به اطلاعات و یا از کار انداختن یک سرویس تلاش کند. به همین دلیل، ابر باید شامل حفاظت انکار (رد) سرویس[۲] باشد. استفاده از پهنای باند بیشتر و قدرت محاسباتی بهتر روش خوبی است که ابر از آن استفاده می‌کند. پس از ورود به ابر، باید به انتقال داده بین کاربران و ارائه‌دهنده ابر توجه شود. یک راه حل مناسب، رمزگذاری داده‌ها قبل از ارسال آنها توسط کاربران است. برای ارسال داده‌ها می‌توان از تکنیک‌های انتقال، همچون SSL[۱] TLS[۲] و IPSec[۳] استفاده کرد. مسأله دیگری که بین کاربران نهایی و ابر باید امن باشد این است که هیچ یک از آنها نباید در ارتباط تصدیق بین کاربران و ابر شنود شوند. همین مکانیسم‌های ذکرشده می‌توانند محرمانه بودن را تضمین کنند. ارائه‌دهندگان ابر مسئولیت اصلی برای حفاظت از داده‌ها، به منظور حفظ یکپارچگی داده‌ها را بر عهده دارند. همچنین در مورد در دسترس بودن داده‌ها هر یک از ارائه‌دهندگان سرویس مسئولیت استفاده از تکنیک‌های خاص برای تامین منابع را بر عهده دارند.

مدل ارائه‌شده در این پایان‌نامه می‌تواند در دسته ابرهای عمومی و خصوصی مورد استفاده قرار گیرد. این مدل همچنین از مجموعه مدل‌های SaaS می‌باشد. در نتیجه بررسی امنیت این مدل‌ها از اهمیت ویژه‌ای برخوردار است. در مدل SaaS، کاربر اقدام به خرید اشتراک محصول نرم‌افزاری می‌کند، اما برخی یا تمام داده‌ها و کدها جای دیگری قرار دارند و مشتریان می‌توانند به این

---

[۱] Security Sockets Layar [۲] Transport Layer Security [۳] Internet Protocol Security

خدمات از طریق اینترنت دسترسی داشته‌باشند. در این مدل، برنامه‌های کاربردی می‌توانند با یک رابط کاربر به‌طور کامل در شبکه اجرا شوند. در SaaS، کاربران به شدت باید به ارائه‌دهندگان ابر از لحاظ امنیت تکیه کنند. همچنین ارائه‌دهندگان برای محرمانه بودن، یکپارچگی و در دسترس بودن خدمات خود مسئول هستند و کاربران هیچ مسئولیتی در این موارد ندارند. در مدل ارائه‌شده در این پایان‌نامه نیز این مسئله مطرح است و استاندارد زبان نشانه‌گذاری اثبات امنیت مسئول حفظ امنیت در هنگام برقراری ارتباط می‌باشد که باید محرمانه بودن، یکپارچگی و در دسترس بودن آنرا تضمین کند. برای تضمین این موارد، در مدل پیشنهادی این پایان‌نامه، در فصل‌های بعد راهکارهایی آورده‌شده است که بعد از ارائه مدل بیان گردیده‌اند.

برای امنیت داده‌ها سه موضوع محرمانه بودن داده‌ها، تمامیت و درستی داده‌ها و در دسترس بودن داده‌ها در محاسبات ابری مطرح شده و مورد بررسی قرار گرفته‌است. محرمانه بودن برای جلوگیری از افشای اطلاعات به افراد و یا سیستم‌های غیرمجاز استفاده می‌شود. تمامیت در واقع اطمینان از اعتبار و کامل‌بودن اطلاعات است. تمامیت داده نه تنها بر درست بودن داده تاکید دارد، بلکه قابل اتکا و اعتماد بودن آنرا نیز شامل می‌شود. همچنین در دسترس بودن به معنای اطمینان از مسئولیت سیستم برای ارائه، ذخیره‌سازی و پردازش اطلاعات زمانی که دسترسی به آنها مورد نیاز است و توسط کسانی که به آنها نیاز دارند، می‌باشد. در مدل SaaS هر سه جنبه گفته‌شده بر عهده ارائه‌دهندگان ابر می‌باشد [۵۱].

٦-٤ نتیجه‌گیری

پس از جمع‌بندی و تجزیه و تحلیل این بررسی‌ها مشاهده می‌شود که مدل پیشنهادی تقریباً تمام حالت‌های ورود و مسائل امنیتی آن را پوشش می‌دهد و می‌توان از آن برای ورود تکی با امنیت بیشتر استفاده نمود. این مدل می‌تواند در ورودهای تکی مبتنی بر اینترنت براساس زبان نشانه‌گذاری مبتنی بر اثبات مورد استفاده قرار گیرد. با استفاده از این مدل می‌توان ورود تکی کاربران را مدیریت کرد، در حالی که افراد درخواست‌کننده سرویس فقط با یکبار احراز هویت و بدون صرف هزینه یا وقت به راحتی وارد شوند و سرویس خود را دریافت نمایند. در فصل بعد مسئله بسیار مهم امنیت مورد بررسی قرار می‌گیرد و چند کاری که در این زمینه در مدل پیشنهادی در نظر گرفته شده بررسی می‌گردد. همچنین در فصل بعد مزایا، معایب و مشکلات احتمالی بررسی، برای حل آنها و کارهای آینده پیشنهاداتی ارائه‌شده است.

فصل پنجم
بررسی مدل پیشنهادی و نتیجه‌گیری

۵-۱ مقدمه

با توجه به پیشرفت تکنولوژی و فراگیرشدن استفاده از محاسبات ابری، نیاز به انجام کارها با استفاده از این امکانات بیشتر احساس می‌شود. دولت‌ها از این فناوری جدید و نوظهور برای ارائه بهتر و بهینه‌تر خدمات خود استفاده می‌کنند. در این پایان‌نامه، یک سیستم برای بهبود امنیت ورود تکی به اینترنت با استفاده از زبان نشانه‌گذاری اثبات امنیت مبتنی بر ابر پیشنهاد شده است. این مدل یک سیستم کاربرپسند با استفاده از تکنولوژی رایانش ابری فراهم می‌کند. این مدل باعث صرفه‌جویی زیادی در هزینه و زمان برای کاربران می‌شود. در این فصل مدل پیشنهادی مورد بررسی قرارگرفته و مزایا و مشکلاتی که پیش‌بینی می‌شود وجود داشته باشند، بیان شده است. همچنین سعی شده است برای رفع این مشکلات پیشنهاداتی ارائه شود که بدون شک به کار بیشتری نیاز دارند.

۵-۲ بررسی مدل پیشنهادی از نظر امنیت

بدون شک مهم‌ترین موضوعی که در پردازش ابری مطرح است و توجه همه را به خود جلب کرده است، موضوع امنیت است. امنیت محاسبات ابری یکی از مهم‌ترین موضوعاتی است که در حال حاضر وجود دارد و توانسته است این فناوری جدید را به چالش بکشد و توجه کارشناسان را بیش از پیش به خود جلب کند. همان‌طور که پیش از این نیز بیان شد برای نشان‌دادن امنیت مدل با توجه به ویژگی‌های ابر، سه موضوع محرمانه بودن داده‌ها، تمامیت و درستی داده‌ها و در دسترس بودن داده‌ها است که باید در نظر گرفته شود. محرمانه بودن برای جلوگیری از افشای اطلاعات به افراد و یا سیستم‌های غیرمجاز استفاده‌می‌شود. تمامیت در واقع اطمینان از اعتبار و کامل‌بودن اطلاعات است. تمامیت داده‌ها نه تنها بر درست‌بودن داده‌ها تاکید دارد، بلکه قابل اتکا و اعتمادبودن آنرا نیز شامل می‌شود. همچنین در دسترس بودن به معنای اطمینان از مسئولیت سیستم برای ارائه، ذخیره‌سازی و پردازش اطلاعات زمانی که دسترسی به آنها مورد نیاز است و توسط کسانی که به آنها نیاز دارند، می‌باشد. در مدل پیشنهادی، استفاده از کلیدهای منحصر به فرد در برقراری ارتباط و همچنین رمزگذاری و امضای اطلاعات با کلیدهای منحصر به فرد محرمانه بودن و تمامیت و درستی داده‌ها را تضمین می‌کند. استفاده از کلیدهای منحصر به فرد برای هر کاربری که وارد می‌شود امنیت این مدل را تضمین می‌کند و باعث افزایش آن می‌شود.

یک روش برای در دسترس بودن، گرفتن پشتیبان از اطلاعات دریافتی می‌باشد. در این مدل تنها نیاز به دردسترس بودن سرورهای عامل‌کاربر و احراز هویت است. در سیستم‌های ورود تکی از هر سرور کاربر و احراز هویت چندین نسخه وجود دارد که در صورت خرابی یا سرقت و هک یکی از این سرورها، ارتباط‌ها به نسخه‌های موجود این سرورها متصل می‌شود و دسترسی‌ها و امکان ورود کاربران از سرورهای چندگانه موجود دیگری که در ابر وجود دارد انجام می‌گیرد. همچنین عمل به‌روزرسانی سرور معیوب به سرعت توسط سرورهای پشتیبان موجود انجام می‌شود.

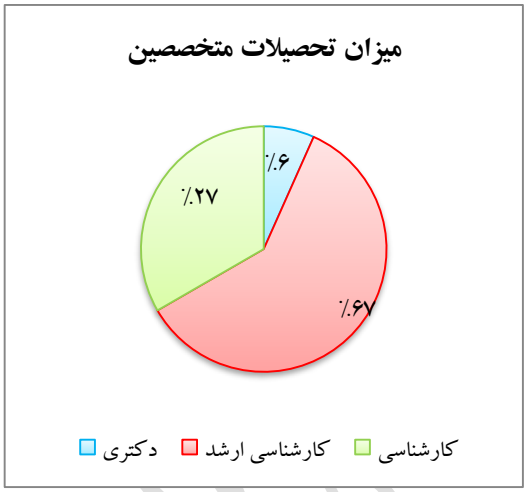
۵-۳ بررسی و ارزیابی مدل پیشنهادی

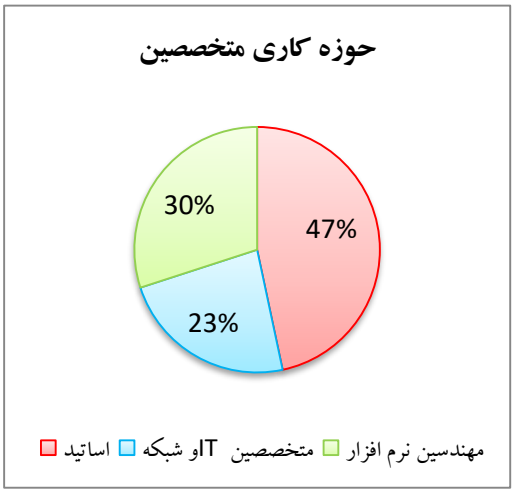
در ادامه این فصل مدل پیشنهادی با نظرخواهی از ۳۲ متخصص ارزیابی‌شده و نتایج ارزیابی با استفاده از نمودارها و آزمون‌های آماری مورد تجزیه‌وتحلیل قرارگرفته‌است. در ادامه ابتدا روش ارزیابی مدل پیشنهادی توضیح داده‌شده است و سپس نتایج حاصل از ارزیابی، مورد تجزیه‌وتحلیل قرارگرفته‌است.

۵-۳-۱ روش ارزیابی مدل

برای ارزیابی مدل پیشنهادی با مشورت چند متخصص و استاد کامپیوتر و انفورماتیک، معیارهایی برای ارزیابی مشخص گردید. با توجه به این معیارها پرسشنامه‌ای طراحی شد و در بین تعدادی از اساتید و دانشجویانی که در زمینه رایانش ابری مطالعاتی داشتند توزیع گردید. پرسشنامه طراحی‌شده از دو بخش تشکیل شده است. قسمت اول پرسشنامه (که پرسشنامه شماره یک نامگذاری شد) شامل ۱۰ سئوال برای سنجش میزان آشنایی افراد با موضوع می‌باشد. در قسمت دوم پرسشنامه (که پرسشنامه شماره دو نامگذاری شد) با توجه به معیارهای مشخص‌شده، سه روش ورود تکی مورد بررسی و مقایسه قرارگرفته‌اند. روش اول ورود تکی به صورت سنتی است. ورود تکی سنتی نوعی ورود تکی است که با استفاده از آن، کاربر برای هر بار ورود و دسترسی به قسمت‌های مجاز، نیاز به وارد کردن نام‌کاربری و رمز عبور خود دارد. روش دوم، روش کربروس می‌باشد که در آن هر کاربر برای ورود تکی و استفاده از سرویس‌ها، هر بار باید برای هر سرور (سرور احراز هویت و ارائه‌دهنده سرویس) به صورت دو طرفه احراز هویت شود. روش سوم، ورود تکی با استفاده از زبان نشانه‌گذاری اثبات امنیت و مبتنی بر ابر می‌باشد که در این روش، کاربران با استفاده از زبان نشانه‌گذاری اثبات امنیت اقدام به ورود می‌نمایند و تا زمانی که از محیط خارج نشوند بدون نیاز به وارد کردن مجدد نام‌کاربری و رمز عبور خود، امکان دسترسی به قسمت‌های مختلف و استفاده از امکانات ابر را دارند. همچنین در ابتدای هر پرسشنامه، تحصیلات و شغل افراد پرسیده شده است. نمونه‌ای از پرسشنامه‌ی طراحی‌شده، در پیوست آخر این پایان‌نامه آورده شده است. پس از طراحی پرسشنامه و انتخاب مدل‌هایی که باید مقایسه شوند، پرسشنامه‌ها در اختیار ۳۲ متخصص قرار گرفت. شکل ۵ ۳ تحصیلات و حوزه کاری متخصصین را مشخص می‌کند.

هدف از این پرسشنامه مقایسه سه روش ورود تکی گفته شده‌است. برای این منظور، مهمترین معیارها در ورود تکی انتخاب شده‌اند. این معیارها در سئوالاتی در پرسشنامه گنجانده و برای هر یک از این معیارها گزینه‌های بسیار زیاد، زیاد، متوسط، کم و بسیار کم در نظر گرفته شده‌است. متخصصین با توجه به سه روش ورود تکی مطرح شده، میزان برآورده‌شدن هر معیار را تعیین کرده‌اند. در این پرسشنامه برای هر یک از گزینه‌های بسیار زیاد، زیاد، متوسط، کم و بسیار کم به ترتیب وزن‌های ۵، ۴، ۳، ۲ و ۱ در نظر گرفته شده است. همچنین اگر متخصصین در مورد یک معیار نظر نداشته باشند یا مخالف یک معیار باشند، برای آن معیار وزن صفر در نظر گرفته شده است. با توجه به اینکه تعداد افرادی که پرسشنامه را پر کرده‌اند، ۳۰ نفر می‌باشند، حداکثر امتیازی که هر معیار در هر روش می‌تواند بدست‌آورد ۱۵۰ می‌باشد (همه افراد گزینه بسیار زیاد را برای یک معیار انتخاب کرده‌باشند). همچنین حداقل امتیاز صفر می‌باشد (همه افراد با یک معیار مخالف باشند). در جدول ۵-۱ معیارهای انتخابی و امتیازات بدست‌آمده برای هر معیار پس از جمع‌آوری پرسشنامه‌ها آورده شده است. در ادامه از این نتایج برای ارزیابی و تجزیه‌وتحلیل روش استفاده‌شده است.





شکل ۵-۱: میزان تحصیلات و حوزه کاری افراد شرکت کننده در ارزیابی مدل پیشنهادی.

جدول ۵- ۱: مقایسه امتیازات دو روش انتخاب شده براساس معیارهای تعیین‌شده. (از روی پرسشنامه)

ردیف	روش ورود تکی ویژگی های مورد نظر	روش سنتی	روش کربروس	روش دو طرفه
۱	آمادگی اجرای هر روش	۱۳۶	۸۶	۹۲
۲	راحتی آموزش و اطلاع رسانی به افراد	۱۲۵	۷۶	۱۰۹
۳	سهولت یادگیری و قابل فهم بودن	۱۳۲	۹۱	۱۱۰
۴	میزان تطابق با دانش روز دنیا	۶۰	۸۹	۱۲۹
۵	صرفه جویی در زمان	۵۰	۸۸	۱۳۱
۶	صرفه جویی در هزینه	۵۳	۸۳	۱۳۰
۷	اهمیت به موضوع امنیت	۵۵	۹۶	۱۲۹
۸	قدرت احراز هویت	۶۰	۸۳	۱۲۷
۹	عدم نیاز به بخاطر سپردن نام‌های کاربری و رمز عبورهای متعدد	۵۲	۹۱	۱۲۷
۱۰	سهولت و راحتی در استفاده	۱۱۸	۷۹	۱۰۲
۱۱	امکان مدیریت دسترسی کاربران	۶۸	۸۶	۱۲۰
۱۲	قابلیت استفاده هر روش در ورود تکی	۱۱۴	۸۳	۱۰۲
۱۳	امکان و سهولت پیاده‌سازی هر روش	۱۲۶	۷۹	۱۱۰
۱۴	میزان کارایی روش از همه لحاظ	۹۲	۹۱	۱۲۷
	میانگین امتیازات	**۸۸/٦٤**	**۸۵/۷۹**	**۱۱۷/۵**

۵-۳-۲ تعیین پایایی و روایی پرسشنامه

در این پایان‌نامه برای ارزیابی مدل پیشنهادی از روش پرسشنامه استفاده‌شده است. برای استفاده از نتایج یک پرسشنامه باید کیفیت پرسشنامه مورد بررسی قرار گیرد. به‌طور کلی می‌توان گفت یک پرسشنامه خوب باید از ویژگی‌های مطلوبی مانند عینیت، سهولت اجرا، عملی‌بودن، سهولت تغییر و تفسیر، روایی و پایایی برخوردار باشد تا به نتایج درستی منجر شود [۵۲]. در بین این ویژگی‌ها، روایی و پایایی از اهمیت بیشتری برخوردار هستند و در این پایان‌نامه مورد توجه قرارگرفته‌اند. برای تعیین پایایی یا قابلیت اعتماد پرسشنامه از روش آلفای کرونباخ و برای تعیین روایی یا اعتبار آن از تحلیل عاملی استفاده‌شده است.

۵-۳-۳ تعیین پایایی پرسشنامه طراحی‌شده برای ارزیابی مدل پیشنهادی

در بررسی پایایی، هدف این است که بدانیم ابزار اندازه‌گیری در شرایط یکسان تا چه اندازه نتایج یکسانی به‌دست می‌دهد. به بیان دیگر، اگر ابزار اندازه‌گیری را در یک فاصله زمانی کوتاه چندین بار به یک گروه واحدی از افراد بدهیم، آیا نتایج حاصل نزدیک به هم خواهد بود یا نه؟ برای اندازه‌گیری پایایی غالباً از شاخصی به نام «ضریب پایایی» استفاده‌می‌کنیم. دامنه ضریب پایایی از صفر تا ۱+ است. ضریب پایایی صفر معرف عدم پایایی و ضریب پایایی یک معرف پایایی کامل است که پایایی کامل واقعاً به ندرت دیده‌می‌شود.

برای محاسبه ضریب پایایی ابزار اندازه‌گیری (پرسشنامه)، شیوه‌های مختلفی به‌کار برده‌می‌شود. در این پایان‌نامه از روش آلفای کرونباخ استفاده‌شده است. ضریب آلفای کرونباخ برای سنجش میزان تک بعدی بودن نگرش‌ها، قضاوت‌ها، عقاید و سایر مقولاتی که اندازه‌گیری آنها آسان نیست به‌کار می‌رود. در واقع می‌خواهیم ببینیم تا چه حد برداشت پاسخگویان از سؤالات یکسان بوده‌است. هر قدر شاخص آلفای کرونباخ به یک نزدیک‌تر باشد، همبستگی درونی بین سؤالات بیشتر و در نتیجه پرسش‌ها همگن‌ترخواهند بود. کرونباخ ضریب پایایی ۴۵ درصد را کم، ۷۵ درصد را متوسط و قابل قبول و ضریب ۹۵ درصد را زیاد پیشنهاد معرفی کرده است. همچنین در بسیاری از منابع، مقادیر به‌دست آمده بالای ۰/۷ در این آزمون، مطلوب تلقی شده‌اند. بدیهی است درصورت پایین بودن مقدارآلفا، بایستی بررسی شود که با حذف کدام پرسش‌های پرسشنامه مقدارآن را می‌توان افزایش داد [۵۳].

در این پایان‌نامه برای محاسبه ضریب آلفای کرونباخ از نرم‌افزار SPSS استفاده‌شده است. در جدول ۵-۲ میزان ضریب آلفای کرونباخ برای پرسشنامه‌ی طراحی‌شده برای ارزیابی مدل پیشنهادی این پایان‌نامه، آورده‌شده است. جدول سمت راست، خلاصه پردازش مورد و تعداد پرسشنامه‌های لحاظ‌شده در ارزیابی را نشان می‌دهد و جدول سمت چپ ضریب آلفا را به ازای معیارهای مورد بررسی نشان می‌دهد.

جدول ۵-۲: محاسبه ضریب آلفای کرونباخ برای پرسشنامه طراحی‌شده.

Case Processing Summary

		N	%
Cases	Valid	30	100.0
	Excluded[a]	0	.0
	Total	30	100.0

Reliability Statistics

Cronbach's Alpha	N of Items
.753	14

همان‌طور که در جدول ۵-۲ مشخص است ضریب آلفای کرونباخ برای پرسشنامه‌ی طراحی‌شده برای ارزیابی مدل پیشنهادی ورود تکی با احراز هویت دو طرفه توسط زبان نشانه‌گذاری اثبات امنیت برابر ۰/۷۵۳ می‌باشد که بیانگر این نکته است که پرسشنامه مورد نظر پایایی قابل قبولی دارد. اطلاعات دیگری که از روش آلفای کرونباخ می‌توان به‌دست آورد در جداول ۵-۳ و ۵-۴ آورده‌شده است. جدول ۵-۳ میانگین و انحراف معیار استاندارد را برای هر یک از معیارهای موجود در پرسشنامه نشان می‌دهد. جدول ۵-۴

همبستگی بین متغیرها و ضریب آلفای کرونباخ پس از حذف هر سئوال را نشان می‌دهد. در واقع از این جدول هنگامی استفاده می‌شود که ضریب آلفای بدست‌آمده کوچک است و نیاز به حذف سئوال‌هایی است که این مقدار را کاهش داده‌اند.

جدول ۵-۳: میانگین و انحراف معیار استاندارد برای هر یک از معیارهای موجود در پرسشنامه.

	Mean	Std. Deviation	N
v1	3.50	.509	30
v2	3.63	.669	30
v3	3.67	.802	30
v4	4.23	.679	30
v5	4.50	.509	30
v6	4.33	.479	30
v7	4.30	.596	30
v8	4.23	.568	30
v9	4.23	.568	30
v10	3.40	.675	30
v11	4.00	.587	30
v12	3.73	.691	30
v13	3.67	.802	30
v14	4.23	.728	30

جدول ۵-٤: همبستگی بین متغیرها و ضریب آلفای کرونباخ پس از حذف هر سئوال.

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
v1	52.17	16.971	.453	.733
v2	52.03	16.033	.494	.725
v3	52.00	16.207	.352	.742
v4	51.43	16.668	.360	.739
v5	51.17	16.489	.576	.722
v6	51.33	16.713	.557	.725
v7	51.37	17.757	.202	.754
v8	51.43	17.289	.321	.743
v9	51.43	17.220	.336	.742
v10	52.27	16.340	.427	.732
v11	51.67	17.747	.209	.753
v12	51.93	17.444	.209	.756
v13	52.00	17.379	.165	.765
v14	51.43	15.013	.635	.707

٤-۳-۵ تعیین روایی پرسشنامه طراحی‌شده برای ارزیابی مدل پیشنهادی

روایی تعیین‌می‌کند که پرسشنامه تهیه‌شده تا چه حد مفهوم خاص مورد نظر را اندازه می‌گیرد. به عبارت دیگر، روایی به ما می‌گوید که آیا پرسشنامه مفهوم واقعی (آنچه مد نظر بوده‌است) را اندازه‌گیری می‌کند یا نه؟ در این پژوهش برای سنجش روایی پرسشنامه از تحلیل عاملی استفاده‌شده است. هدف از تحلیل عاملی خلاصه‌کردن متغیرها در تعدادی عامل است. در واقع تحلیل عاملی، از میان متغیرهای آزمون (سئوالات پرسشنامه)، آنهایی که تاثیر بیشتری بر واریانس دارند را انتخاب‌کرده و طبق همبستگی سایر متغیرها با عامل‌های انتخابی، گروه‌هایی تشکیل می‌دهد. متغیرهایی که در یک گروه قرار می‌گیرند وابستگی مطلوبی با یکدیگر دارند.

قبل از انجام تحلیل عاملی، باید نتایج پرسشنامه ارزیابی شوند تا تعیین گردد آیا برای اجرای تحلیل عاملی مناسب هستند یا خیر. برای انجام این کار از ضریب KMO استفاده می‌شود که مقدار آن همواره بین صفر و یک در نوسان است. مقادیر کوچک KMO بیانگر آن است که همبستگی بین زوج متغیرها نمی‌تواند توسط متغیرهای دیگر تبیین شود، بنابراین کاربرد تحلیل عاملی متغیرها ممکن است قابل توجیه نباشد. در صورتی که مقدار KMO کمتر از ۰/۵ باشد داده‌ها برای تحلیل عاملی مناسب نخواهند

بود [۵۴]. برای اطمینان از مناسب‌بودن داده‌ها برای تحلیل عاملی از آزمون کرویت بارتلت نیز استفاده‌می‌شود. آزمون بارتلت این فرضیه که ماتریس همبستگی‌های مشاهده‌شده متعلق به جامعه‌ای با متغیرهای ناهمبسته است را می‌آزماید. برای آنکه یک مدل عاملی مفید و دارای معنا باشد، لازم است متغیرها همبسته باشند، در غیر اینصورت دلیلی برای تبیین مدل عاملی وجود ندارد. در آزمون بارتلت اگر sing کوچکتر از ۰/۵ باشد، تحلیل عاملی برای شناسایی ساختار مناسب است [۵۲]. جدول ۵-۵ نتایج حاصل از آزمون KMO و بارتلت را برای پرسشنامه طراحی‌شده برای ارزیابی مدل پیشنهادی نشان می‌دهد.

جدول ۵-۵: نتایج حاصل از آزمون KMO و بارتلت

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.505
Bartlett's Test of Sphericity	Approx. Chi-Square	171.570
	Df	91
	Sig.	.000

با توجه به اطلاعات بدست‌آمده در جدول ۵-۵، مشخص می‌گردد ضریب KMO برابر ۰/۵۰۵ می‌باشد که از مقدار ۰/۵ بیشتر است. همچنین مقدار sing آزمون بارتلت صفر شده است که از ۰/۵ کوچک‌تر می‌باشد. در نتیجه استفاده از روش تجزیه عاملی برای پرسشنامه‌ی طراحی‌شده برای ارزیابی مدل پیشنهادی این پایان‌نامه مناسب می‌باشد.

۵-۳-۵ استخراج عامل‌ها

همان‌طور که در بخش‌های قبل گفته‌شد هدف تحلیل عاملی خلاصه‌کردن متغیرها در تعدادی عامل است. یکی از روش‌های استخراج عامل‌ها، روش تجزیه مولفه‌های اصلی است. در روش تجزیه مولفه‌های اصلی، عامل‌هایی که بیشترین مقدار واریانس را در بین دیگر عامل‌ها دارند، استخراج می‌شوند. در واقع در این روش یک مقدار ویژه برای عامل‌ها محاسبه می‌گردد. سپس عامل‌هایی که مقدار ویژه آنها بیشتر از یک باشد، به عنوان عامل‌های معنی‌دار در نظر گرفته‌می‌شوند و بقیه عامل‌ها در گروه‌هایی شامل این عامل‌های معنی‌دار قرار می‌گیرند. برای این‌کار از نتایج جدول عاملی که در نرم‌افزار SPSS بدست‌آمده استفاده می‌گردد. در این مرحله دو جدول مورد بررسی قرار می‌گیرد. جدول ۵-۶ میزان اشتراک متغیرها یا واریانس کل با میزان اشتراک عاملی متغیرها را نشان می‌دهد. Initial گویای تمامی اشتراک‌های قبل از استخراج است، بنابراین تمامی آنها برابر یک هستند. در ضمن همان‌گونه که مشاهده می‌شود همه میزان اشتراک‌ها بعد از استخراج بالاتر از ۰/۵ هستند که این بیانگر توانایی عامل‌های تعیین‌شده در تبیین واریانس متغیرهای مورد مطالعه است. در نتیجه نیازی به حذف هیچ سئوالی در پرسشنامه مورد نظر نیست. جدول ۵-۷ مقدار ویژه و واریانس متناظر با عامل‌ها را نشان می‌دهد. در ستون Initial Eigenvalues مقادیر ویژه اولیه برای هر یک از عامل‌ها در قالب مجموع واریانس تبیین‌شده برآورد می‌شود. پایین بودن این مقدار برای یک عامل به این معنی است که آن عامل نقش اندکی در تبیین واریانس متغیرها داشته‌است. در ستون Extraction Sums of Squared Loadings واریانس تبیین‌شده‌ی عامل‌هایی ارائه‌شده است که مقادیر ویژه آنها بزرگتر از عدد یک باشند. ستون Rotation Sums of Squared Loadings مجموعه‌ی مقادیر عامل‌های استخراج‌شده بعد از چرخش را نشان می‌دهد [۵۵]. همان‌طور که مشخص‌است پنج عامل قابلیت تبیین واریانس‌ها را دارند.

شکل ۵-۴ تغیرات مقادیر ویژه را در ارتباط با عامل‌ها نشان می‌دهد. این نمودار برای تعیین تعداد بهینه مولفه‌ها به‌کار می‌رود. با توجه به این نمودار مشاهده می‌شود که از عامل ششم به بعد تغییرات مقدار ویژه کم می‌شود. پس می‌توان شش عامل را به عنوان عوامل مهم که بیشترین نقش را در تبیین واریانس داده‌ها دارند، استخراج کرد. همچنین رابطه میان هر متغیر با عامل‌های استخراجی در جدول ۵-۸ آورده شده است. هر متغیر در گروه عاملی قرار می‌گیرد که با آن عامل همبستگی بالای داشته‌باشد. با توجه به

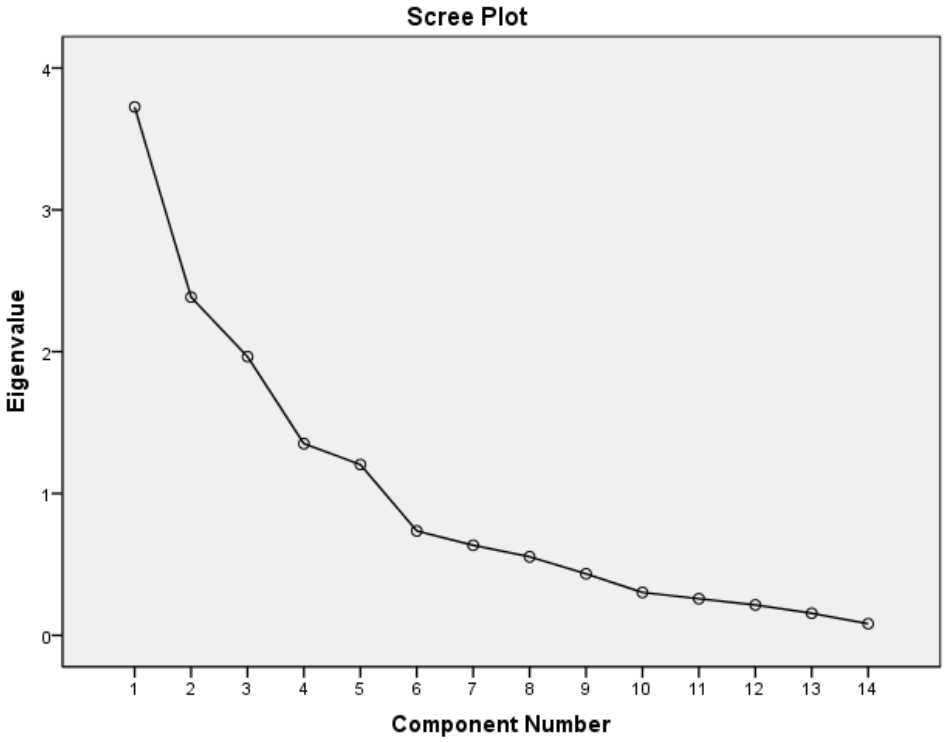
تحلیل عاملی پنج عامل شناسایی شد و با توجه به جدول ۵-۸ اعضای هر گروه مشخص می‌شود. با توجه به این جدول عامل اول در واریانس سئوالات ۴، ۵ ، ۶ و ۱۳ تاثیر بیشتری دارد. به همین ترتیب عامل دوم در واریانس سئوالات ۳ ،۱۰ و ۱۴، عامل سوم در واریانس سئوالات ۸، ۱۱ و ۱۲، عامل چهارم در واریانس سئوالات ۴، ۷ و ۹ و در نهایت عامل پنجم در واریانس سئوالات ۱ و ۲ تاثیر بیشتری دارد. این پنج گروه در جدول ۵-۹ آورده‌شده‌اند. لازم به ذکر است که در تحلیل عاملی می‌توان طبق پیشینه موضوع گروه‌ها را تغییر داد [۵۲]. به عنوان مثال معیار میزان تطابق با دانش روز دنیا که در گروه چهار قرار گرفته‌است به گروه پنج منتقل می‌شود. در واقع جدول ۵-۹ نتیجه ماتریس چرخیده‌شده مولفه‌ها و استفاده از پیشینه پژوهش می‌باشد.

جدول ۵-٦: میزان اشتراک متغیرها قبل و بعد از استخراج عامل‌ها.

	Initial	Extraction
v1	1.000	.781
v2	1.000	.736
v3	1.000	.661
v4	1.000	.753
v5	1.000	.800
v6	1.000	.763
v7	1.000	.814
v8	1.000	.804
v9	1.000	.752
v10	1.000	.865
v11	1.000	.798
v12	1.000	.779
v13	1.000	.705
v14	1.000	.619

جدول ۵-۷: مقدار ویژه و واریانس متناظر با عامل‌ها.

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.726	26.614	26.614	3.726	26.614	26.614	2.704	19.318	19.318
2	2.384	17.029	43.643	2.384	17.029	43.643	2.515	17.964	37.282
3	1.965	14.034	57.677	1.965	14.034	57.677	1.864	13.314	50.596
4	1.351	9.650	67.327	1.351	9.650	67.327	1.851	13.224	63.820
5	1.204	8.600	75.927	1.204	8.600	75.927	1.695	12.107	75.927
6	.736	5.259	81.187						
7	.635	4.533	85.719						
8	.554	3.955	89.675						
9	.434	3.097	92.772						
10	.302	2.159	94.932						
11	.258	1.844	96.776						
12	.214	1.531	98.307						
13	.156	1.112	99.419						
14	.081	.581	100.000						



شکل ۵-۲: تغیرات مقادیر ویژه در ارتباط با عامل‌ها.

جدول ۵-۸: ماتریس چرخیده‌شده مولفه‌ها.

	Component				
	1	2	3	4	5
v1	.207	.191	-.119	.044	.828
v2	.066	.420	.110	.036	.736
v3	-.146	.732	.159	.125	.249
v4	.535	-.243	.069	.521	.363
v5	.827	.178	.259	.132	-.020
v6	.847	.115	.104	.043	.140
v7	.111	-.101	-.070	.886	.044
v8	-.015	.320	.734	.395	-.084
v9	-.148	.419	.275	.691	-.031
v10	.126	.886	-.092	-.187	.145
v11	.284	.020	.842	-.090	-.027
v12	.486	.401	-.545	.056	-.287
v13	.676	-.153	-.275	-.231	.309
v14	.354	.636	.147	.154	.210

جدول ۵-۹: تجزیه معیارها به پنج گروه عاملی

گروه	معیارها
آمادگی اجرای هر روش	آمادگی اجرای هر روش، امکان و سهولت پیاده‌سازی هر روش، صرفه جویی در هزینه
سهولت یادگیری و قابل فهم بودن	صرفه جویی در زمان، قدرت احراز هویت، امکان مدیریت دسترسی کاربران و قابلیت استفاده هر روش در ورود تکی
صرفه جویی در زمان	میزان تطابق با دانش روز دنیا
راحتی آموزش و اطلاع رسانی به افراد	سهولت یادگیری و قابل فهم بودن، سهولت و راحتی در استفاده و کارایی کلی روش
میزان تطابق با دانش روز دنیا	راحتی آموزش و اطلاع رسانی به افراد، اهمیت به موضوع امنیت و عدم نیاز به بخاطر سپردن نام‌های کاربری و رمز عبورهای متعدد

٦-٤-٥ ارزیابی مدل پیشنهادی

پس از اثبات روایی و پایایی پرسشنامه، مشخص شد که پرسشنامه‌ی طراحی‌شده برای ارزیابی مدل پیشنهادی این پایان‌نامه شرایط لازم را داشته و قادر است مدل پیشنهادی را به‌درستی ارزیابی کند. در این پرسشنامه علاوه بر مدل پیشنهادی، دو روش ورود تکی سنتی و کربروس نیز مورد ارزیابی قرارگرفته‌اند تا بتوان نتایج حاصل از این ارزیابی را برای مقایسه سه روش به‌کار برد. در جدول ۵-۱ امتیازات هر یک از سه روش گفته‌شده آورده شده بود. با توجه به این امتیازات، شکل ۵-۵ نمودار میله‌ای حاصل از مقایسه سه روش را نشان می‌دهد. همان‌طور که در این شکل مشخص است، مدل پیشنهادی این پژوهش توانسته است بالاترین امتیاز را به‌دست آورد.

شکل ۵. ۳: مقایسه امتیازات سه روش ورود تکی.

٧-٤-٥ آزمون فریدمن برای مقایسه میانگین روش‌ها

آزمون فریدمن یک آزمون ناپارامتری، معادل آنالیز واریانس با اندازه‌های تکراری (درون‌گروهی) است که از آن برای مقایسه میانگین رتبه‌ها در بین K متغیر (گروه) استفاده‌می‌شود. در آزمون فریدمن فرض H۰ مبتنی بر یکسان بودن میانگین رتبه‌ها در بین گروه‌ها است. رد شدن فرض صفر به این معنی است که در بین گروه‌ها حداقل دو گروه با هم اختلاف معنی دارند (H۱). در این پایان‌نامه، این آزمون با توجه به اطلاعات جدول ۵-۱ که امتیازات معیارهای مختلف در سه روش ورود تکی سنتی، ورود تکی کربروس و ورود تکی با احراز هویت دو طرفه را نشان می‌دهد، انجام‌شده است. در آزمون فریدمن اگر سطح پوشش آماره‌ی آزمون از پنج درصد کمتر باشد، فرض آماری H۰ رد شده و فرض آماری H۱ نتیجه گرفته می‌شود. نتایج آزمون انجام شده در نرم‌افزار SPSS مورد تجزیه و تحلیل قرار گرفته است و اطلاعات بدست آمده در جدول ۵-۱۰ آورده‌شده است. با توجه به جدول ۵-۱۰ (جدول سمت چپ) مشاهده می‌گردد که سطح پوشش آماره آزمون برابر ۰/۰۰۰ می‌باشد که از ۰/۰۵ کمتر است. در نتیجه فرض H۰ رد می‌شود و وجود تفاوت بین روش‌ها نتیجه گرفته‌می‌شود. همچنین جدول سمت راست میانگین رتبه‌ها در سه روش را نشان می‌دهد.

جدول ۵-۱۰: نتیجه آزمون فریدمن برای امتیازات سه روش ورود تکی در SPSS.

	Mean Rank
Sonata	1.57
Kerberos	1.43
dotarafe	3.00

N	30
Chi-Square	46.828
df	2
Asymp. Sig.	.000

۵-٤-۸ آزمون کلموگروف-اسمیرونوف

برای بررسی عادی یا نرمال‌بودن توزیع داده‌های استفاده‌شده، از آزمون کلموگروف- اسمیرونوف استفاده‌می‌شود. هنگام بررسی نرمال‌بودن داده‌ها، فرض صفر نرمال‌بودن توزیع داده‌ها را در سطح خطای ۵ درصد تست می‌کند. بنابراین اگر آماره آزمون بزرگتر مساوی ۰/۰۵ بدست آید، در این صورت دلیلی برای رد فرض صفر مبتنی بر اینکه داده نرمال است، وجود نخواهد داشت. به عبارت دیگر، توزیع داده‌ها نرمال خواهد بود. برای آزمون نرمال‌بودن فرض‌های آماری به صورت زیر تنظیم می‌شوند:

H۰: توزیع داده‌های مربوط به هر یک از متغیرها نرمال است.

H۱: توزیع داده‌های مربوط به هر یک از متغیرها نرمال نیست.

با توجه به خروجی‌های بدست‌آمده چنانچه در آزمون کلموگروف-اسمیرونوف، .Sig بیشتر از ۰/۰۵ باشد می‌توان داده‌ها را با اطمینان بالایی نرمال فرض کرد. در غیر این صورت نمی‌توان گفت که توزیع داده‌ها نرمال است. جدول ۵-۱۱ نتیجه انجام آزمون کلموگروف- اسمیرونوف را برای سه روش ورودتکی نشان می‌دهد. همان‌طور که در این جدول نشان‌داده‌شده است مقدار آماره توصیفی (Asymp. Sig.) بدست‌آمده از ۰/۰۵ بیشتر است و در نتیجه فرض H۰ که نشان‌دهنده نرمال‌بودن توزیع داده‌ها می‌باشد، تایید می‌گردد.

جدول۵-۱۱: نتیجه آزمون کلموگروف- اسمیرونوف برای امتیازات سه روش ورود تکی در SPSS.

		Dt
N		30
Normal Parameters[a,b]	Mean	55.6667
	Std. Deviation	4.37338
Most Extreme Differences	Absolute	.099
	Positive	.099
	Negative	-.077
Kolmogorov-Smirnov Z		.543
Asymp. Sig. (2-tailed)		.930

۵-٤-۹ تحلیل واریانس

تحلیل واریانس برای مقایسه میانگین دو یا چند گروه استفاده‌می‌شود. برای انجام تحلیل واریانس توزیع داده‌ها که در اینجا همان امتیازات هستند، باید در جامعه نرمال باشند. از نتایج به‌دست‌آمده از آزمون کلموگروف-اسمیرونوف و با توجه به اثبات نرمال‌بودن توزیع داده‌ها در این آزمون، می‌توان نتیجه گرفت که تحلیل واریانس برای این پژوهش نتایج صحیحی تولیدمی‌کند. جدول ۵-۱۲ نتایج تحلیل واریانس برای مقایسه میانگین‌های سه روش ورود تکی سنتی، ورود تکی کربروس و ورود تکی با احراز هویت دو طرفه را نشان می‌دهد. این خروجی شامل سه جدول است. در جدول اول، که مهمترین خروجی بدست‌آمده از تحلیل واریانس نیز می‌باشد، مجموع مربعات، میانگین مربعات و درجات آزادی آورده‌شده است. در این جدول با توجه به اینکه مقدار sig کوچک‌تر از ۰/۰۵ می‌باشد، می‌توان نتیجه‌گرفت که میانگین روش‌ها با یکدیگر برابر نمی‌باشند (در این جدول اگر مقدار sig کمتر از ۰/۰۵ باشد، نشان‌دهنده اختلاف میانگین روش‌ها است). جدول دوم همگنی واریانس را نشان‌می‌دهد. در این جدول اگر sig بزرگ‌تر از ۰/۰۵ باشد، واریانس نمونه‌ها همگن است. با توجه به مقدار sig در جدول، نتیجه گرفته می‌شود که واریانس نمونه‌ها ناهمگن است. جدول سوم میانگین هر یک از روش‌های ورود تکی را نشان‌می‌دهد. در این جدول هر روش با یک عدد نشان‌داده‌شده است (ورود تکی سنتی با عدد یک، ورود تکی کربروس با عدد دو و ورود تکی با احراز هویت دو طرفه با عدد سه نشان‌داده‌شده‌اند).

جدول ۵-۱۲: نتایج تحلیل واریانس برای ارزیابی امتیازات سه روش ورود تکی در SPSS.

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	8617.905	2	4308.952	9.199	.001
Within Groups	18269.071	39	468.438		
Total	26886.976	41			

Levene Statistic	df1	df2	Sig.
54.588	2	39	.000

Model

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
1	14	88.64	34.709	9.276	68.60	108.68	50	136
2	14	85.79	5.632	1.505	82.53	89.04	76	96
3	14	117.50	12.996	3.473	110.00	125.00	92	131
Total	42	97.31	25.608	3.951	89.33	105.29	50	136

۵-۵ مزایای و نتایج بدست‌آمده از مدل پیشنهادی

مهمترین مزیت استفاده از این مدل، احراز هویت دو طرفه عامل کاربر و ارائه‌دهنده هویت است که باعث امنیت بیشتر ارتباط و کاهش جعل و فریب کاری می‌شود. به عبارت دیگر با احراز هویت دوطرفه، علاوه بر ارائه‌دهنده هویت، عامل کاربر نیز از هویت ارائه‌دهنده هویت آگاه می‌شود و ارائه‌دهنده هویت نیز خود را به عامل کاربر اثبات می‌کند. در واقع عامل کاربر با ارائه‌دهنده هویت خاص و معتبر مرتبط و فرایند احراز هویت را انجام می‌دهد.

با توجه به مشکل پروتکل زبان نشانه گذاری اثبات امنیت که چگونگی امنیت سرور وب ارائه‌دهنده هویت را مشخص نمی‌کند و هیچ کار و تلاشی به منظور بررسی کیفیت ارائه‌دهنده هویت انجام نمی‌دهد و اینکه هیچ چیز برای تضمین سازگاری ارائه‌دهنده هویت با قوانین صنعت و تعیین چگونگی اشکالات سرور وب ارائه‌دهنده هویت وجود ندارد و همچنین اینکه خود ارائه‌دهنده هویت می‌تواند لینک ضعیفی در زنجیره امنیتی شما ایجاد کند و زبان نشانه‌گذاری اثبات امنیت هیچ راهی برای شناختن آن ندارد، مدل پیشنهادی با احراز هویت دو طرفه و با احراز هویت ارائه‌دهنده هویت، امنیت سرور ارائه‌دهنده هویت تضمین می‌شود و از این پس ارائه‌دهنده هویت به عنوان یک لینک قوی در ارتباط و زنجیره امنیت این ارتباط در نظر گرفته می‌شود. همچنین سایر مزایای استفاده از مدل پیشنهادی در جدول ۵-۱۳ آورده‌شده‌اند.

جدول ۵-۱۳: مزایای استفاده از مدل پیشنهادی.

ردیف	شرح مزیت
۱	باعث جلوگیری از اتلاف وقت کاربران برای احراز هویت‌های مجدد، هنگام ورود می‌شود.
۲	باعث کاهش هزینه کاربران می‌شود.
۳	باعث می‌شود ارائه‌دهنده هویت به عنوان یک لینک قوی در زنجیره امنیتی درنظر گرفته شود (امنیت ارائه‌دهنده‌هویت تضمین می‌شود).
۴	باعث شناسایی سرور ارائه‌دهنده‌هویت خاصی که یک کاربر خاص را احراز هویت می‌کند می‌شود.
۵	با پیکر بندی مناسب سیستم احراز هویت، امکان هک‌شدن را به شدت کاهش می‌دهد.
۶	امکان شناسایی اثبات‌های نامعتبر را فراهم می‌کند.
۷	مرجع صدور شناسه و گواهی (تاییدیه هویت)، محل ذخیره و نگهداری، میزان و نوع دسترسی و امنیت را مشخص می‌کند.

٦-٥ مشکلات احتمالی و راه حل‌های پیشنهادی

با توجه به فراهم نبودن بسترهای پیاده‌سازی این روش در کشورهای جهان سوم و بالا بودن هزینه پیاده‌سازی آن برای سازمان‌ها، در این حالت می‌توان از همان روش سنتی استفاده کرد با این تفاوت که اطلاعات کاربر برای دسترسی ثبت شوند که نیاز به احراز هویت‌های مکرر و مجدد در هنگام ورود و استفاده از منابع مورد نیاز نباشد. مشکل دیگری که وجود دارد اینست که گزارش رویدادها در زبان نشانه‌گذاری اثبات امنیت در جایی ثبت نمی‌شود که این مشکل با بکارگیری یک سیستم گزارش‌گیری حل می‌شود. موضوع دیگری که به عنوان یک مشکل اساسی مطرح است، عدم وجود مکانیزم‌های احراز هویت استاندارد است (مثلاً نوع احراز هویتی که سازمان‌ها یا شرکت‌ها استفاده می‌کنند، یکپارچه نیستند)، که با تدوین یک پروتکل جهانی می‌توان یک استانداردسازی و یکپارچه‌سازی سراسری برای استفاده و احراز هویت با استفاده از زبان نشانه‌گذاری اثبات امنیت ایجاد کرد که همه سازمان‌ها، شرکت‌ها و نهادها برای یکپارچه‌سازی از این پروتکل خاص پیروی کنند. موضوع دیگری که وجود دارد مدیریت و دسترسی کاربران است که فرایند بسیار مهمی است. این موضوع می‌تواند با تعاریف خاصی از سطح دسترسی و شرایطی که برای هر کاربر در نظر گرفته می‌شود به طور مناسبی مرتفع می‌گردد.

با توجه به این که موضوع امنیت و احراز هویت دو موضوع بسیار مهم و اساسی در دسترسی و استفاده از خدمات وب و رایانش ابری است، همچنان نیازمند بررسی و کارهای بیشتری در این زمینه می‌باشد که می‌تواند به عنوان کارهای آینده مورد توجه قرار گیرد. همچنین با توجه به اینکه زبان نشانه‌گذاری اثبات امنیت، امنیت فرم‌های وب را تضمین نمی‌کند، برای استفاده از رایانش ابری و ورود تکی در صفحات وب و ورود اعتبارات کاربران موضوع امنیت فرم‌ها باید در نظر گرفته شود. این موضوع با نیازمند دانستن چگونگی ساخته‌شدن صفحات وب است چرا که به عنوان یک نقطه ضعف در هنگام هک کردن درنظر گرفته می‌شوند.

٧-٥ پیشنهادات

با توجه به حرکت جهان به سمت محاسبات ابری و پیشرفت‌های جهانی و عمومی و فراگیر آن با مناسب سازی بسترهای اجرا و پیاده سازی این تکنولوژی امکان استفاده بیشتر و بهینه‌تر از این فناوری وجود دارد که جای بحث و تأمل و کارهای فروان است.

منابع و مآخذ

[1] Prepared by the Cloud Security Alliance *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, United States Copyright Act , December 2009.
[2] TaheriMonfared A *Securing the IaaS Service Model of Cloud Computing Against Compromised Components*, Norwegian University of Science and Technology, June 2011.
[3] Kumaz P, Sehgal K, Chauhan S, Gupta K and Diwakar M "Effective Ways of Secure, Private and Trusted Cloud Computing", *IJCSI International Journal of Computer Science Issues*, Vol 8, Issue 3, No 2, May 2011.
[4] LEWIS D and LEWIS E "Web Single Sign-On Authentication using SAML", *IJCSI International Journal of Computer Science Issues*, Vol 2, 2009.
[5] Ragouzis N "Security Assertion Markup Language (SAML) V2.0 Technical Overview", Feb. 2007.
[6] Cantor S "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005.
[7] Wang J, Zhao Y, Jiang S and Le J "Providing privacy preserving in Cloud computing", *International Conference on Test and Measurement*, pp 213-216, 2009.
[8] Saltzer H *Protection and the control of information sharing in multics*, ACM, 17(7):388–402, 1974.
[9] Stanoevska-Slabeva k and Wozniak K, *principal cloud*,
[10] Chen Y, Paxson V and Katz K "What's New About Cloud Computing Security", *Electrical Engineering and Computer Sciences University of California at Berkeley*, Technical Report No. UCB/EECS-2010-5, January 20, 2010.
[11] http://www.iranianlearn.com/article6119.html.
[12] http://xen.org/products/xenhyp.html.
[13] Karger P "Securing virtual machine monitors—what is needed", *Keynote address*, ASIACSS 2009.
[14] Feinleib H *A Technical History of National CSS*, Computer History Museum, April 2005.
[15] "Cloud Computing Security Considerations", *Department of Intelligence and Security of Australian Government*, April 2011.
[16] Delgado V *Exploring the limits of cloud computing*, Master of Science Thesis Stockholm, Sweden, 2010.
[17] Miller M "Using WS-Security and SAML for Internet Single Sign On", *20th Computer Science Seminar, SA3-T4-1*, 2005.
[18] Jøsang A Security Usability Principles for Vulnerability Analysis and Risk Assessment, *Annual Computer Security Applications Conference*, 2007 (ACSAC'07).
[19] "Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration", *Jerichio Forum* [tm], Version 1.0, April 2009.
[20] Provos N *Safe Browsing* (Google Online Security Blog), June 2012.
[21] Jansen W and Grance T *Guidelines on Security and Privacy in Public Cloud Computing*, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, December 2011.
[22] http://www.schneier.com/blog/archives/2010/06/data_at_rest_vs.html.
[23] Winkler R *Cloud Computer Security Techniques and Tactics*, in the United States of America, 2011.
[24] "Security Assertion Markup Language (SAML) 2.0", *OASIS Standard*, July 2005.
[25] Kemp J "Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0." *OASIS SSTC*, January 2005.
[26] "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", *OASIS Standard*, March 2005.

[27] Box D "Simple Object Access Protocol (SOAP) 1.1.", *World Wide Web Consortium Note*, May 2000.
[28] Meyer C, Feldmann F and Schwenkpaper J "Sometimes it's better to be STUCK", *Horst Gortz Institute for IT-Security*, Ruhr-University Bochum, 2011.
[29] Cantor S "Bindings for the OASIS Security Assertion Markup Language (SAML)V2.0." *OASIS SSTC*, March 2005.
[30] Aarts R "Liberty Reverse HTTP Binding for SOAP Specification Version 1.0.", *Liberty Alliance Project*, 2003.
[31] "Introduction to Security Assertion Markup Language (SAML) and SAML Support in IBM WebSphere Application Server Version 7.0 Fix Pack 7", *IBM WebSphere Web Services Security Development*, Software Group, November, 2009.
[32] Monzillo R "OASIS Web Services Security: SAML2.0 Token Profile 1.0".
[33] Morgan M "Interactions between Shibboleth and local-site web sign-on services", April 2001.
[34] "Leveraging SAML for Federated Single Sign-on", *PistolStar, Inc. dba PortalGuard*, PO Box 1226 Amherst, NH 03031 USA, 2012.
[35] http://www.pistolstar.com/SSO.html.
[36] Somorovsky J, Mayer A, Schwenk J, Kampmann M and Jensen M, "On Breaking SAML: Be Whoever You Want to Be", *Sec2 project of the German Federal Ministry of Education and Research (BMBF, FKZ: 01BY1030)*, 2012.
[37] http://en.wikipedia.org/wiki/Claims-based_identity.
[38] Shadfar S "Smart Card-Based Identity and Access Management", *Schlumberger Information Solutions*, 2004.
[39] F L Podio and Dunn J "Biometric Authentication Technology:From the Movies to Your Desktop", 2002.
[40] http://en.wikipedia.org/wiki/NT_LAN_Manager.
[41] http://docs.oracle.com/cd/E19575-01/820-3746/6nf8qcveh/index.html.
[42] "Kerberos White Paper", Hewlett-Packard Development Company, L.P, *Trademark of Intel Corporation in the U.S,* 2005.
[43] Schneier B "Sharing a Secret: How Kerberos Works", *Cryptography: Protocols, Algorithms and Source Code in C*, 1995.
[44] the MIT Kerberos Consortium, "Why is Kerberos a credible security solution?", *the United States Government*, 2008.
[45] http://howto.caspio.com/getting-started/password-protection/password-protection-1-of-3-lookup-and-authentication-tables.
[46] Ping Identity, SAML101 (White Paper), Ping Identity Corporation, 2012.
[47] http://saml.xml.org/advantages-saml
[48] http://en.wikipedia.org/wiki/SAML_2.0.
[49] http://www.gluu.org/blog/tag/saml.
[50]"SAML Alone Is Not Secure", SECUREAUTH (Whitepaper), *8965 Research Drive*, Suite 200, Irvine, CA 92618, 2011.
[51] Ajoudanian Sh and Ahmadi M R “A Novel Data Security Model for Cloud Computing”, *IACSIT*, April, 2012.
[۵۲] شفیعی ثابت ا ر "ارائه یک مدل بهبود یافته برای ساخت ایمن برنامه کاربردی وب"، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، موسسه آموزش عالی صنعتی فولاد فولادشهر، پاییز ۹۲.
[53] http://hr-vojdani.blogfa.com/post/261, accessed January 1, 2214.
[۵۴] فرشادفرع اصول و روش‌های آماری چند متغیره، انتشارات طاق بستان، دانشگاه رازی، کرمانشاه، ۱۳۸۰.
[۵۵] زارع چاهوکی م ع روش‌های تحلیل چند متغیره در نرم افزار SPSS ، دانشگاه تهران، پاییز ۱۳۸۹.

پیوست‌ها

پیوست: پرسشنامه طراحی شده برای ارزیابی مدل پیشنهادی

پرسشنامه شماره یک

موضوع پایان‌نامه: بهبود امنیت ورودتکی با استفاده از زبان نشانه‌گذاری اثبات امنیت

نام و نام‌خانوادگی:

عنوان شغل: محل خدمت:

رشته تحصیلی: تحصیلات:

توضیحات پیرامون پژوهش

مفهوم محاسبات ابری:

تعریف موسسه ملی استاندارد و فناوری ایالات متحده از محاسبات ابری: "محاسبات ابری یک مدل برای دسترسی مناسب شبکه بر اساس تقاضا، به یک انبار مشترک از منابع محاسباتی قابل پیکربندی (به عنوان مثال، شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و خدمات) است که می‌تواند به سرعت و با حداقل تلاش مدیریت و با تعامل ارائه‌دهنده‌سرویس، تولید و منتشر شود".

محاسبات ابری در حقیقت به معنای تبدیل پردازش و منابع پردازشی از یک محصول به یک سرویس است. در این مدل منابع بر روی یک سرور اصلی تحت شبکه قرار می‌گیرند و سیستم‌ها و سایر تجهیزات تنها نیاز به اتصال به شبکه دارند و از ابزار فراهم‌شده بر روی شبکه استفاده‌کنند. در مدل محاسبات ابری، بسیاری از موارد مانند پردازش، نرم‌افزارها، دسترسی به داده و فضای ذخیره‌سازی بر روی ارائه‌دهنده ابر قرار دارند و کاربران ابری نیازی به دانستن مکان دقیق ذخیره‌سازی اطلاعات و نحوه کار سیستم ندارند و حتی سیستم مورد استفاده آنها در این مدل نیازی به داشتن فضای وسیع جهت ذخیره‌سازی اطلاعات ابری نخواهند داشت.

زبان نشانه‌گذاری اثبات امنیت

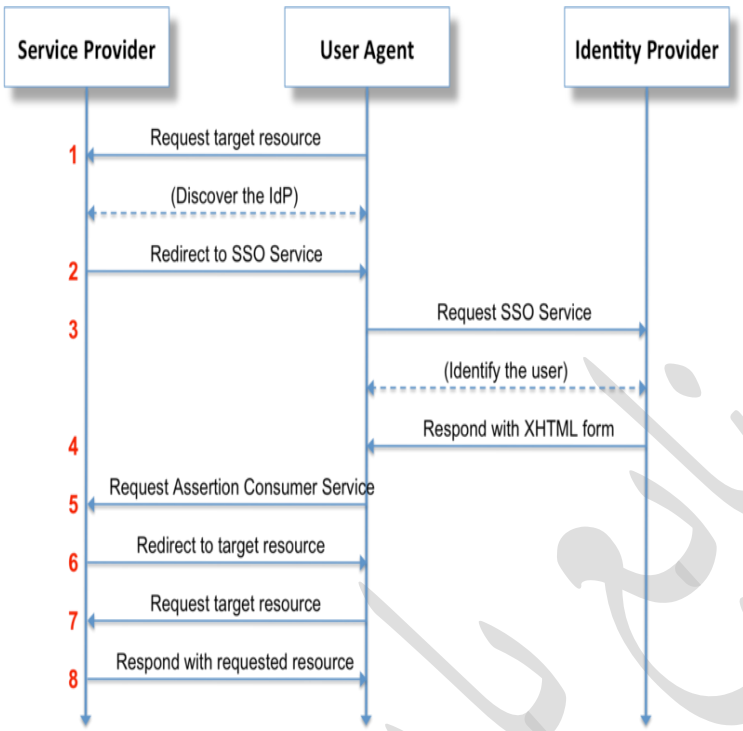
زبان نشانه‌گذاری اثبات امنیت یک استاندارد مبتنی بر زبان نشانه‌گذاری توسعه‌پذیر برای ورودتکی مرورگر وب است و توسط کمیته فنی سرویس‌های امنیت سازمان گسترش استانداردهای اطلاعات ساختاریافته[۳۵] برای تبادل اطلاعات ایمن بین بخش‌های مختلف تعریف شده است. زبان نشانه‌گذاری اثبات امنیت پیچیده است و تنها شرکت‌های بزرگ می‌توانند هزینه سنگین استفاده و پیاده‌سازی زبان نشانه‌گذاری اثبات امنیت را توجیه کنند.

مدل پیشنهادی برای ورودتکی

مدلی پیشنهادی برای ورودتکی با استفاده از زبان نشانه‌گذاری اثبات امنیت به این صورت عمل می‌کند که عامل کاربر از طریق استاندارد زبان نشانه‌گذاری اثبات امنیت اقدام به ورودتکی به ابر می‌نماید و سرویس‌های مورد نیاز خود را درخواست و پس از احراز هویت و ورود موفقیت‌آمیز به وب، از آنها استفاده می‌کند. در این مدل فرض می‌شود که ارائه‌دهنده هویت، کلید منحصر به فردی برای ارتباط با هر عامل کاربر که قصد ورود و احراز هویت دارد تولید می‌کند. به هر عامل کاربر نیز در هنگام ورود یک کلید تخصیص داده می‌شود که هنگام ورود برای احراز هویت دو طرفه بین خود و ارائه‌دهنده هویت مبادله می‌شود. این کلید تا پایان کار و تا هنگام خروج تکی، نزد دو طرف باقی خواهد ماند. همچنین برای امنیت بیشتر فرایند می‌توان از یک مهر زمان استفاده کرد که در صورت منقضی شدن مهر زمان، اجازه ورود به عامل کاربر داده نشود. همچنین برای مقابله با منقضی شدن زمان، دو راه

[3] Organization for the Advancement of Structured Information Standards

حل وجود دارد: راه حل اول استفاده از زمان انقضای طولانی‌تر است و راه حل دوم اینست که اگر عامل کاربر وارد شده‌باشد و زمان انقضا تمام و یا نزدیک به انقضا است، سرویس یک مهر زمان با زمان انقضای جدید صادر کند.



مراحل انجام کار به صورت زیر است:

گام یک: عامل‌کاربر یک سرویس را از ارائه‌دهنده سرویس درخواست می‌کند. در واقع، عامل‌کاربر وارد ابر می‌شود و منبع هدف را از ارائه‌دهنده سرویس درخواست می‌کند (به عنوان مثال ورود به صفحه اصلی یک سایت).

گام دوم: درخواست به ارائه‌دهنده‌سرویس فرستاده‌می‌شود و ارائه‌دهنده‌سرویس، بهترین ارائه‌دهنده‌هویت کاربر را مشخص و عامل‌کاربر را به سرویس ورودتکی در ارائه‌دهنده‌هویت مسیردهی مجدد می‌کند.

گام سوم: پس از جهت‌دهی مجدد درخواست منبع هدف با عامل‌کاربر، عامل‌کاربر درخواست را برای بدست‌آوردن دسترسی به سرویس ورودتکی به ارائه‌دهنده‌هویت ارسال می‌کند.

گام چهارم: فرایند احراز هویت دو طرفه عامل کاربر و ارائه‌دهنده هویت انجام می‌شود. ارائه‌دهنده‌سرویس یک اثبات هویت از ارائه‌دهنده هویت درخواست می‌کند. عامل‌کاربر اطلاعات را با کلید خود امضا می‌کند، اطلاعات در ارائه‌دهنده هویت خوانده‌می‌شود و عامل‌کاربر اعتبارسنجی می‌شود. در صورتی که عامل‌کاربر معتبر بود، پاسخ به عامل‌کاربر برگشت داده‌می‌شود. عامل‌کاربر اطلاعات را با کلید خود رمزگشایی می‌کند. پس از رمزگشایی، در صورتی که احراز هویت ارائه‌دهنده هویت موفقیت‌آمیز باشد، به اثبات هویت درخواست‌شده توسط ارائه‌دهنده‌سرویس پاسخ داده‌می‌شود.

گام پنجم: سرویس ورودتکی، درخواست و پاسخ را با یک متن شامل یک فرم XHTML اعتبارسنجی می‌کند. بر اساس این اثبات، ارائه‌دهنده سرویس می‌تواند یک تصمیم کنترل دسترسی ایجاد کند یا حتی قبل از تحویل اثبات هویت به ارائه‌دهنده سرویس، ارائه‌دهنده هویت ممکن است برخی اطلاعات (از قبیل نام‌کاربر ی و رمز عبور) را از عامل‌کاربر درخواست کند، به عبارت دیگر عامل‌کاربر را احراز هویت کند.

گام ششم: عامل کاربر یک درخواست به سرویس مصرف‌کننده اثبات در ارائه‌دهنده سرویس ارسال می‌کند. ارائه‌دهنده سرویس اثبات را خوانده و اطلاعات آن استخراج می‌شود. سپس از نتیجه اثبات برای ادامه فرایند استفاده‌می‌شود.

گام هفتم: پس از اینکه سرویسِ‌مصرف‌کننده اثبات در ارائه‌دهنده سرویس پاسخ را پردازش کرد، در صورت تایید، یک متن امنیتی در ارائه‌دهنده سرویس ایجاد می‌شود و عامل‌کاربر را مجدداً به منبع هدف جهت‌دهی می‌کند.

گام هشتم: پس از جهت‌دهی مجدد عامل‌کاربر به منبع هدف توسط ارائه‌دهنده سرویس، عامل‌کاربر مجدداً منبع هدف را در ارائه‌دهنده سرویس درخواست می‌کند.

گام نهم: در صورتی احراز هویت با موفقیت انجام شود و ارتباط به درستی برقرار گردد، منبع درخواست‌شده توسط عامل‌کاربر روی ابر قرار می‌گیرد و مناسب‌ترین ارائه‌دهنده سرویس منبع را به عامل کاربر باز می‌گرداند.

بررسی مدل پیشنهادی از نظر امنیت

بدون شک مهم‌ترین موضوعی که در محاسبات ابری مطرح است و توجه همه را به خود جلب کرده است، موضوع امنیت است. امنیت محاسبات ابری یکی از مهم‌ترین موضوعاتی است که در حال حاضر وجود دارد و توانسته‌است این فناوری جدید را به چالش بکشد و توجه کارشناسان را بیش از پیش به خود جلب کند.

برای نشان دادن امنیت مدل با توجه به ویژگی‌های ابر، سه موضوع محرمانه بودن داده‌ها، تمامیت و درستی داده‌ها و در دسترس بودن داده‌ها است که باید در نظر گرفته شود. در مدل پیشنهادی، استفاده از کلیدهای منحصر به فرد در برقراری ارتباط و همچنین رمزگذاری و امضای اطلاعات با کلیدهای منحصر به فرد محرمانه بودن و تمامیت و درستی داده‌ها را تضمین می‌کند. استفاده از کلیدهای منحصر به فرد برای هر کاربری که وارد می‌شود امنیت این مدل را تضمین می‌کند و باعث افزایش آن می‌شود. گرفتن پشتیبان از اطلاعات دریافتی، در دسترس بودن را تضمین می‌کند. در این مدل تنها نیاز به دردسترس بودن سرورهای عامل کاربر و احراز هویت است. در سیستم‌های ورودتکی از هر سرور کاربر و احراز هویت جندین نسخه وجود دارد که در صورت خرابی یا سرقت و هک یکی از این سرورها، ارتباط‌ها به نسخه‌های موجود این سرورها متصل می‌شود و دسترسی ها و امکان ورود کاربران از سرورهای چندگانه موجود دیگری که در ابر وجود دارد انجام می‌گیرد. همچنین عمل به‌روزرسانی سرور معیوب به سرعت توسط سرورهای پشتیبان موجود انجام می‌شود.

۱- تا چه حد با محاسبات ابری (Cloud Computing) آشنایی دارید؟

زیاد　　تاحدودی　　آشنایی ندارم

۲- تا چه حد با زبان نشانه‌گذاری اثبات امنیت آشنایی دارید؟

زیاد　　تاحدودی　　آشنایی ندارم

۳- آیا زیرساخت‌های پیاده‌سازی این روش وجود دارد؟

بله　　خیر

۴- آیا شما حاضر به استفاده از این مدل هستید؟

بله　　خیر

۵- آیا به این روش اعتماد دارید؟

بله　　خیر

۶- آیا تمایلی به استفاده از این روش به جای روش‌های موجود دارید؟

بله　　خیر

۷- آیا امکان احراز هویت نادرست در این روش وجود دارد؟

بله　　خیر

۸- میزان آشنایی شما با خدمات ورودتکی به وب چقدر است؟

زیاد تاحدودی آشنایی ندارم

۹- احراز هویت این روش تا چه میزان مطمئن است؟

زیاد کم

۱۰- لطفا اگر پیشنهاد یا نظری در مورد هر سوال و مدل پیشنهادی دارید در پایان ذکر کنید. قطعاً نظرات شما باعث بهبود این کار خواهد شد.

پرسشنامه شماره دو

توضیحات در مورد سه روش‌های ورودتکی:

۱- روش ورودتکی سنتی

در این روش به هر کاربر یک نام‌کاربری و رمز عبور تخصیص داده‌می‌شود. کاربر برای هر بار ورود به وب، باید نام‌کاربری و رمز عبور خود را وارد نماید. علاوه بر این کاربر برای دسترسی به هر سرویس باید مجدداً و به صورت مجزا احراز هویت شود. در این روش کاربر نیاز به، به‌خاطر سپردن تعداد زیادی نام‌کاربری و رمز عبور برای ورود و استفاده از خدمات و برنامه‌های‌کاربردی وب دارد.

۲- روش کربروس

کربروس، کاربر را قادر به ورود درون پنجره‌های دامنه حساب‌هایش می‌کند و سپس ورودتکی را برای برنامه‌های‌کاربردی داخلی آنها محیا می‌کند. کربروس برای اتصال کاربر، به یک مرکز توزیع کلید نیاز دارد. کاربران خودشان را برای سرویس‌ها (مثلاً سرورهای وب) احراز هویت می‌کنند. ابتدا برای مرکز توزیع کلید احراز هویت می‌شوند، سپس بلیط‌های سرویس رمزگذاری شده از مرکز توزیع کلید را برای یک سرویس خاص که قصد استفاده از آن را دارند درخواست می‌کنند که به طور خودکار در همه مرورگرهای مهم با استفاده از SPNEGO (مکانیزم مذاکره GSSAPI محافظت‌شده و ساده) رخ می‌دهد. در واقع در کربروس، برای برقراری ارتباط و تبادل اطلاعات، هم کاربر و هم ارائه‌دهندگان سرویس باید خود را برای دیگری احراز هویت کنند (احراز هویت دو طرفه بین تمام بخش‌ها انجام می‌گیرد).

۳- ورودتکی مبتنی بر زبان نشانه‌گذاری اثبات امنیت (احراز هویت دو طرفه)

ورودتکی مبتنی بر زبان نشانه‌گذاری اثبات امنیت برای ورودتکی عامل کاربران جهت عدم تکرار استفاده از نام‌های‌کاربری و رمز عبورهای متعدد مورد استفاده قرار می‌گیرد. مشکل ورودتکی زبان نشانه‌گذاری اثبات امنیت این است که سرور ارائه‌دهنده‌هویت برای عامل کاربر احراز هویت نمی‌شود. در مدل پیشنهادی (ورودتکی دو طرفه با استفاده از زبان نشانه‌گذاری اثبات امنیت) به عامل کاربر و سرور ارائه‌دهنده‌هویت یک کلید منحصربه‌فرد تخصیص می‌دهد که هنگام برقراری ارتباط، اطلاعات را امضا و رمزگذاری می‌کند که سرور ارائه‌دهنده‌هویت خاص، عامل کاربر را با کلید خود احراز هویت می‌کند و عامل کاربر نیز سرور ارائه‌دهنده‌هویت را احراز هویت می‌کند.

روش‌های ورودتکی	روش سنتی					روش کربروس					احراز هویت دو طرفه				
ویژگی‌های مورد نظر	بسیار زیاد	زیاد	متوسط	کم	بسیار کم	بسیار زیاد	زیاد	متوسط	کم	بسیار کم	بسیار زیاد	زیاد	متوسط	کم	بسیار کم
آمادگی اجرای هر روش															
راحتی آموزش و اطلاع رسانی به افراد															
سهولت یادگیری و قابل فهم بودن															
میزان تطابق با دانش روز دنیا															
صرفه جویی در زمان															
صرفه جویی در هزینه															
اهمیت به موضوع امنیت															
قدرت احراز هویت															
عدم نیاز به بخاطر سپردن نام‌های‌کاربری و رمز عبورهای متعدد															
سهولت و راحتی در استفاده															
امکان مدیریت دسترسی کاربران															
قابلیت استفاده هر روش در ورود تکی															
امکان و سهولت پیاده سازی هر روش															
میزان کارایی روش از همه لحاظ															

Foolad Institute of Technology

Department of Mechanical Engineering

Information Security Enhancement in Cloud Computing with SAML Standard

A Thesis

Submitted in partial fulfillment of the requirements for the degree of Master of Science

By

Rasool Daneshmand

Evaluated and Approved by the Thesis Committee, on December 16, 2014

Dr. Shohreh Ajoudanian (Supervisor)

Dr. Mohammad Davarpanah Jazi (Advisor)

Dr. Mohammad Ali Montazeri (Examiner)

Department Graduate Coordinator

Information Security Enhancement in Cloud Computing with SAML Standard

Rasool daneshmand

Daneshmand1989@yahoo.com

Department of

Foolad Institute of Technology, Fooladshahr, Isfahan, Iran

Degree: M.Sc.

Dr.Ajoudanian, Shajoudanian@yahoo.com

Abstract

The world of internet and computers are becoming more complex and evolving every day. One of the products of evolution, is cloud computing. Due to this, the sensitivity of data and information privacy seriously as a major concern for organizations becomes. Companies for provide Web-based services the special attention to application service providers (ASP) or software as a service (SaaS), which reduces costs and providing specific applications and focused on the users. This approach the complexity of the design, installation, configuration, deployment and support of the system by internal sources eliminates that offers many benefits to organizations.

Recently, organizations from the central authentication resources use for Web-based applications and portals for the greater part of its internal. The authentication single sign on, when properly configured to create a strong security means that users don't need remember and remembering passwords for different systems. Also makes easily user's manage and audit. Using the standard for information authentication exchange on the Internet, we can solve this problem. Security Assertion Markup Language, an XML-based and secure solution for exchange of user's information between identity provider (organization) and service provider (ASP or SaaS) are provided. Security Assertion Markup Language Standard defined rules and syntax for the exchange of information, yet flexible and permit customized data transfer to the external service provider.

In this project we tried to improve the single sign on systems and special for single sign on with using Security Assertion Markup Language by using the advantagees of the cloud computing and single sign on. To do so, at first we review the basic concepts and definitions including cloud computing, Security Assertion Markup Language, authentication and Single Sign On. A short survey was done about authentication ways in order to provide a better and more complete model, that was tailored to develop a authentication model using Security Assertion Markup Language and based cloud computing. Also, some of the presented models for each of the above topics and combination of this concepts was investigated. By combining above methods and information, a model was suggested and implemented for Single Sign on based on cloud computing with using , Security Assertion Markup Language in order to help the Single Sign on in the user's authentication process. Finally, after mentioning the advantages of the proposed model, possible problems of the model was discussed and some suggestions has been made for solving these problems that can be subject to future works.

Key Words

Information security in cloud computing, SAML in cloud computing.