

بهبود و رفع مشکلات و چالش‌های مرتبط با امنیت محاسبات ابری در شبکه مه

تاریخ دریافت: ۱۴۰۲/۰۳/۲۷

تاریخ پذیرش: ۱۴۰۲/۰۴/۱۸

کد مقاله: ۱۰۰۸۴

محمد مهدی سبحانی^۱

چکیده

احراز هویت دو طرفه که منجر به افزایش امنیت بیشتر ارتباط و کاهش جعل و فریب کاری و نیز استفاده از این روش که بر خلاف روشهای دیگر نیازی به احراز هویت مجدد ندارد می تواند دلیلی بر داشتن نوآوری در تحقیق باشد. هدف اصلی تحقیق حاضر بهبود و یا رفع مشکلات و چالش‌های مرتبط با امنیت در شبکه‌های مه می باشد. این پژوهش از نظر هدف جزء تحقیقات کاربردی می باشد. روش گردآوری اطلاعات روش های کتابخانه ای و میدانی می باشد که در بخش میدانی از ابزار پرسشنامه استفاده شده است. هدف از این پرسشنامه مقایسه سه روش ورود تکی گفته شده است. پیاده‌سازی مدل نیازمند یک محیط ابر خواهد بود که خود دارای سرورهایی برای احراز هویت، ارائه سرویس و عامل کاربر (مثلاً مرورگر وب) می باشد نتایج حاصل از تحقیق نشان داد که 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. و این می تواند باعث کاهش سربار حافظه و زمان شود. همچنین با استفاده از کلید رمزنگاری متقارن باعث کاهش ۳۶ درصدی سربار حافظه می شود.

واژگان کلیدی: کلود سیم، امنیت مه، ابر، محاسبات ابر، کلید رمز متقارن

۱- مقدمه

امروزه تاثیر فناوری اطلاعات و اینترنت بر زندگی مردم بر کسی پوشیده نیست. ادارات، سازمان ها و افراد جامعه نیازمند دسترسی سریع به اطلاعات و پردازش سریع اطلاعات هستند و این در حالی است که علاوه بر توجه به بحث سرعت در دسترسی و پردازش اطلاعات، افراد جامعه نیازمند امنیت اطلاعات و صرفه جویی در هزینه هم می باشد. (ورمقانی، ۱۳۹۸) از سوی دیگر پیشرفت علم حجم رو به گسترشی از داده ها و توان محاسباتی را ایجاد کرده است که برای انالیز آن ها ابر کامپیوتر هایی با توان پردازشی بالا مورد نیاز هستند که هزینه نگهداری و ارتقا بسیاری را بر عهده کاربر می گذارند. در این شرایط یکی از بهترین راهکارها استفاده از فناوری محاسبات ابری است تا با صرف کمترین هزینه و نیاز به کمترین حد مدیریت، بالاترین توان محاسباتی را برای کاربر تامین کنیم. (فرهادی، ۱۳۹۹) محاسبات ابری، مدل محاسباتی نوینی است که قابلیت دسترسی به منابع را با توجه به تقاضا تامین می کند، تاثیر قابل توجه این فناوری بر حوزه فناوری اطلاعات بسیاری از شرکت های معتبر نظیر مایکروسافت را بر ان داشته است که تلاش های بسیاری در جهت ارائه سرویس های قوی مبتنی بر ابر داشته باشند. استفاده از فناوری ابر خدمات مطمئن، با صرفه و پرسود را برای کاربر فراهم می کند. با این حال توجه به این نکته ضروری است که همیشه در کنار مزیت های هر طرح و فناوری جدید خطرات و نگرانی هایی وجود داشته است و آنچه در استفاده از این فناوری چالش بزرگی را ایجاد میکند بحث امنیت اطلاعات است. (بونومی، ۲۰۱۸) شبکه مه را می توان سناریویی دانست که در آن تعداد زیادی از دستگاه های بی سیم در همه جا حاضر و غیر متمرکز ارتباط برقرار می کنند. ارتباط بالقوه بین آن ها و شبکه برای انجام وظایف ذخیره سازی و پردازش بدون نیاز به شخص سوم است. شبکه مه با توانایی بالا در پردازش محلی، انالیز و ذخیره سازی داده ها در همکاری با فناوری ابر بسیاری از چالش ها را حل کرده و عکس العمل مناسبی را در برخورد با مسائل ایجاد کرده است. (بنابراین نیاز است تلاش های گسترده در جهت بهبود و رفع مشکلات و چالش های مرتبط با امنیت محاسبات ابری در شبکه مه صورت گیرد. (دی بریتو، ۲۰۱۷).

۲- پیشینه تحقیق

تا کنون تحقیقات کیفی و کمی بسیاری در این زمینه انجام شده است. در این تحقیقات از روش هایی متفاوتی مانند چارچوب FACE، بررسی الگوریتم های مانند RSA، SHA و ... استفاده شده است. روش به کار گرفته شده در این پژوهش استفاده از نرم افزار کلود سیم برای ارائه کلید رمز متقارن است. مثال هایی از پژوهش های انجام شده در این حوزه در ادامه آورده شده است. با این حال تاکنون مطالعه ای با هدف کاهش سربار حافظه توسط کلید رمز متقارن انجام نشده است در نتیجه میتوان استفاده از کلید رمز متقارن را به عنوان عامل نوآوری این پژوهش به حساب آورد.

نجات و همکاران در سال ۱۳۹۹ در مقاله ای مروری به بررسی مشکلات امنیتی در محاسبات ابری پرداختند. صدرالساداتی و همکاران در سال ۱۳۹۹ در مقاله ای بر مقوله رایانش ابری پرداخته و چالش های امنیتی مرتبط با این فناوری را مورد بررسی قرار دادند. رستمی یسار و همکاران در سال ۱۳۹۸ بررسی محاسبات لبه و مه را در تحقیقی بیان کرده که نتیجه تحقیقات آن ها حاکی از این مطلب بود که محاسبات لبه با صرفه جویی در ارتباطات IOT، کاهش پیچیدگی معماری سیستم و شبکه و کاهش تعداد نقاط نقص احتمالی در یک برنامه IoT موجب صرفه جویی در وقت و پول را موجب می شود.

ناماسادرا و همکاران در سال ۲۰۲۰ بهبود روش رمزگذاری مبتنی بر ویژگی نسبت به امنیت داده ها در محاسبات ابری را بررسی کردند. آن ها یک مدل کنترل دسترسی کارآمد و ایمن برای محیط رایانش ابری برای به اشتراک گذاری منابع و دانش با استفاده از رمزگذاری مبتنی بر ویژگی (ABE)، شبکه توزیع شده هش (DHT) و رمزگذاری زمان بندی شده بر اساس هویت ارائه کردند.

هایجان و همکاران در سال ۲۰۲۰ در تحقیقی تحت عنوان «بهبود امنیت اینترنت اشیا (IoT) با شبکه تعریف شده توسط نرم افزار» (SDN) به بررسی امنیت اشیا پرداختند. پیاده سازی و ارزیابی سیستم بیانگر این واقعیت بود که تکنیک پیشنهادی در برابر حملات سایبری مقاوم تر است.

۳- روش شناسی پژوهش

پژوهش حاضر از نظر هدف کاربردی می باشد. به منظور گردآوری اطلاعات لازم از ائین نامه های بین المللی، جدیدترین مقالات منتشر شده در ژورنال های معتبر جهانی و کتاب ها استفاده شد. ۲۷ درصد از افراد شرکت کننده در ارزیابی در مقطع کارشناسی، ۶۷ درصد از افراد در مقطع کارشناسی ارشد و ۶ درصد از افراد شرکت کننده دارای تحصیلات در مقطع دکتری بودند. ۹ نفر از این افراد از مهندسين نرم افزار، ۷ نفر متخصص در حوزه IT و فناوری اطلاعات و ۱۴ نفر از اساتید بودند. با مشورت با چندین متخصص و استاد در حوزه های کامپیوتر و بیوانفورماتیک معیارهای ارزیابی مشخص شدند پس از آن بر اساس معیارهای

مشخص شده پرسشنامه ای مشتمل بر دو بخش طراحی شد و در اختیار افراد قرار گرفت. بخش اول پرسشنامه شامل ۱۰ سوال بود که میزان آشنایی افراد با موضوع مورد مطالعه را مورد سنجش قرار میداد و بخش دوم مشتمل بر سوالاتی بود که سه روش ورود تکی سنتی، روش کربروس و روش ورود تکی با استفاده از زبان نشانه گذاری اثبات امنیت و مبتنی بر مه را مورد بررسی و مقایسه قرار داد. پایایی پرسشنامه با استفاده از ضریب الفای کرونباخ بررسی شد و برای ارزیابی روایی پرسشنامه از روش تحلیل عاملی استفاده شد. در این پژوهش کلید رمز متقارن درون سرآیند زبان نشانه گذاری اثبات امنیت قرار گرفت و به منظور محاسبات در شبکه‌های مه از نرم افزار کلود سیم استفاده شد.

۴- مدل پیشنهادی تحقیق

در جدول ۱ مراحل انجام مدل پیشنهادی در تحقیق حاضر به منظور احراز هویت ارائه‌دهنده هویت زبان نشانه گذاری اثبات امنیت ارائه شده است. روش کار به این صورت می باشد که درون سرآیند زبان نشانه گذاری اثبات امنیت، کلیدی (کلید رمز متقارن) 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. با توجه به این موضوع، مدلی ارائه خواهد شد که در آن احراز هویت ارائه‌دهنده هویت در نظر گرفته شود و امنیت آن نیز تامین گردد. و سربرار حافظه کاهش یابد.

جدول ۱- مدل احراز هویت ارائه‌دهنده هویت SAML

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

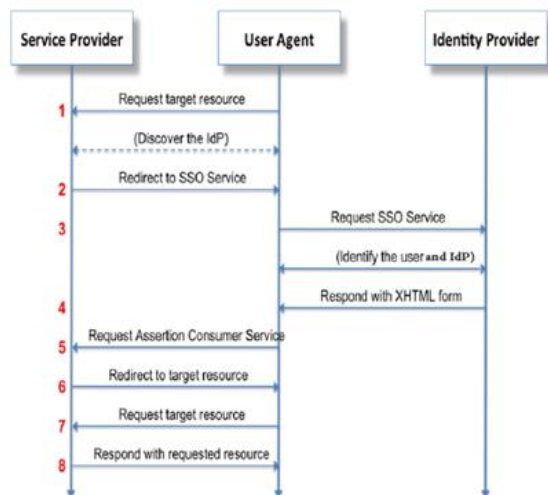
مدل بالا به منظور انجام ورود تکی با استفاده از زبان نشانه گذاری اثبات امنیت ارائه شده است. در این مدل فرض می‌شود که ارائه‌دهنده هویت، کلید رمز متقارن منحصر به فردی برای ارتباط با هر عامل کاربر که قصد ورود و احراز هویت دارد تولید می‌کند. به هر عامل کاربر نیز در هنگام ورود یک کلید رمز متقارن تخصیص داده می‌شود که هنگام ورود برای احراز هویت دو طرفه بین خود و ارائه دهنده 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 حل وجود دارد: راه حل اول استفاده از زمان انقضای طولانی‌تر است و راه حل دوم اینست که اگر عامل کاربر وارد شده باشد و زمان انقضا تمام و یا نزدیک به انقضا است، سرویس یک مهر زمان با زمان انقضای جدید صادر کند. در روش سنتی احراز هویت زبان نشانه گذاری اثبات امنیت 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 انجام می‌شود و این در صورتی است که هیچگونه اطلاعاتی از امنیت ارائه‌دهنده هویت در دست نیست.

۵- ارزیابی روش انجام مدل پیشنهادی

روش بهبود یافته احراز هویت کاربران توسط زبان نشانه گذاری 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 مسپرد 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 داده می‌شود. همراه با این پاسخ دو کلید منحصر به فرد نیز به عامل کاربر تخصیص داده می‌شود. 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 هویت مبادله می‌شود هر یک از طرفین با رمزگشایی اطلاعات توسط کلید خود می‌توانند به پاسخ و کلیدهای جاسازی شده 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 می‌شود 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

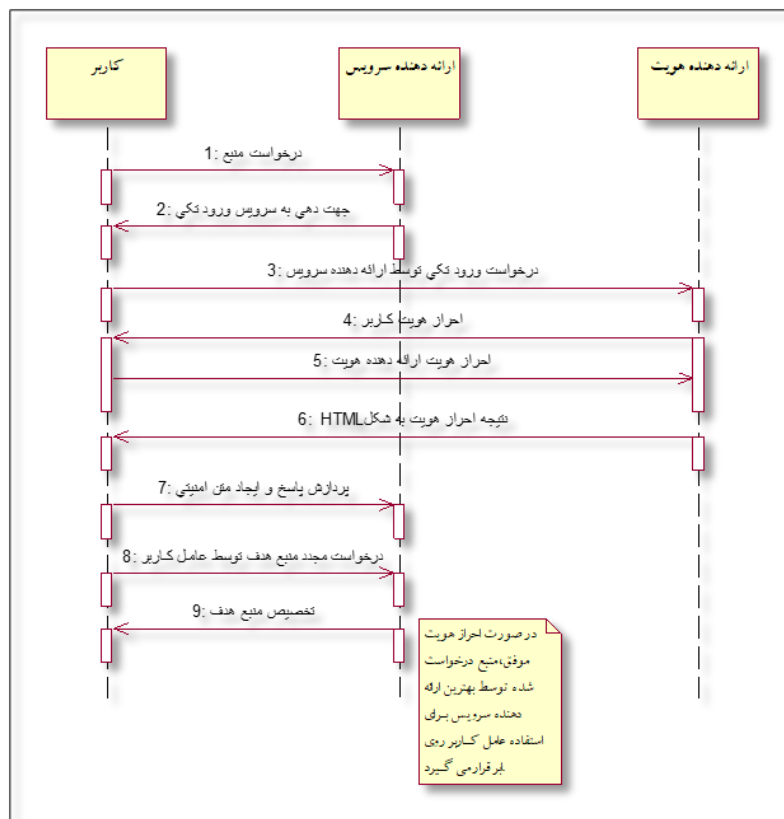
عامل کاربر بدون نیاز به استفاده از هر برنامه کاربردی خاصی می‌تواند به راحتی به آن دسترسی و از آن استفاده کند. و این می‌تواند باعث کاهش سربار حافظه و زمان شود. با توجه به شکل ۱، مراحل برای انجام فرایند احراز هویت ورود تکی به وب با استفاده از زبان نشانه‌گذاری اثبات امنیت دنبال می‌شود. در هنگام ورود عامل کاربر به محیط مه، 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 داده می‌شود. با توجه به همه این موارد گفته شده دو حالت وجود دارد که در ادامه توضیح داده شده‌اند:



شکل ۱- احراز هویت ورود تکی به وب با زبان نشانه‌گذاری اثبات امنیت [۶۱]

حالت اول: اگر کلید مبادله شده 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 انجام می‌شود و پس از طی مراحل فرایند سرویس یا سرویس‌های خواسته شده توسط عامل کاربر، توسط سرورهای ارائه‌دهنده سرویس به او داده می‌شود. همچنین مراحل انجام کار در نمودار توالی شکل ۲ آورده شده است.

حالت دوم: اگر کلید مبادله شده 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 کنند، فرایند برقرار نمی‌شود و اجازه ورود به کاربر داده نمی‌شود و بنابراین سرویس‌های درخواست شده 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 ۲ الگوریتم این فرایند را به تصویر کشیده‌است.



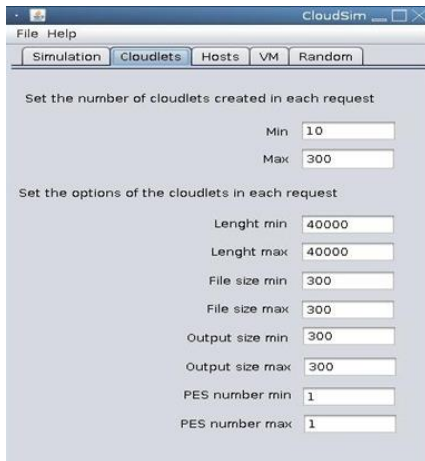
شکل ۲- الگوریتم مدل پیشنهادی

همان‌طور که مشاهده می‌شود کاربران در خارج از محدوده، از طریق اینترنت به عامل کاربر که خود می‌تواند شامل یک یا چند سرور باشد، دسترسی پیدا می‌کنند و عامل کاربر 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 تعریف شده است که کاربر در هنگام نیاز به دستیابی به یک سرویس به یکی از عامل‌های کاربر دسترسی پیدا می‌کند و با برقراری ارتباط با آن و در صورت احراز هویت موفق عامل کاربر برای سرور احراز هویت خاص، ارتباط برقرار می‌شود و سرورهای ارائه‌دهنده سرویس، سرویس درخواست شده را به عامل کاربر باز می‌گرداند. با توجه به محیط‌های آزمایشگاهی و امکانات و تجهیزات (خصوصاً شبکه) موجود و در دسترس، تنها مدل‌سازی این طرح امکان‌پذیر است و امکان پیاده‌سازی آن وجود ندارد. کاربران از طریق اینترنت و از نقاط مختلف به عامل‌های کاربری که در اطراف مه قرار دارند دسترسی پیدا می‌کنند. روند کار این‌گونه است که از هر عامل کاربری 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.

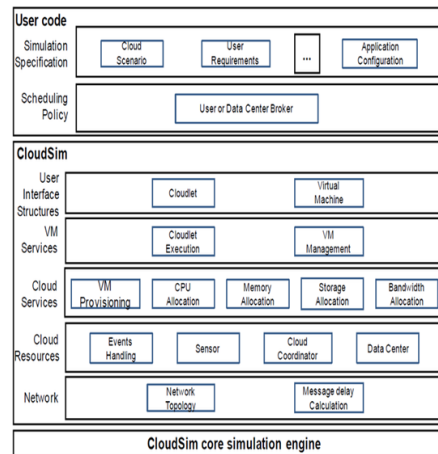
۶- انجام مدل پیشنهادی

از شبیه‌سازی ابر به نام کلود سیم^۱ به منظور شبیه‌سازی و نمایش منطق کار استفاده شده است. کلود سیم یک زبان مبتنی بر جاوا است و نیاز به نصب و اجرای برنامه‌های کاربردی نت بینز و JDK می‌باشد. کلود سیم یک چارپوب شبیه‌سازی گسترده و انعطاف‌پذیر است که مدل‌های یکپارچه را قادر به شبیه‌سازی می‌سازد. کلودسیم مثل بلوک‌های سازنده‌ای می‌ماند که با آن می‌توانید محیط مه شبیه‌سازی را ساخت. پیاده‌سازی این مدل نیازمند یک محیط مه می‌باشد که خود دارای سرورهایی برای احراز هویت، ارائه سرویس و عامل کاربر (مثلاً مرورگر وب) می‌باشد. نمای کلی پلت‌فرم کلود سیم در شکل ۳ آمده است. پس از اجرای نرم افزار ابتدا باید پارامترهای مورد نظر و خواسته شده توسط نرم افزار را تنظیم کرد. شکل ۴ تعدادی از این پارامترها را نشان می‌دهد. همان‌گونه که در بالا اشاره شد، شبیه ساز کلود سیم از زبان جاوا پشتیبانی می‌کند. نمای اولیه نرم افزار در حال اجرا در شکل ۵ نشان داده شده است. همچنین توابع و کتابخانه‌های کلود در شکل زیر نشان داده شده است.

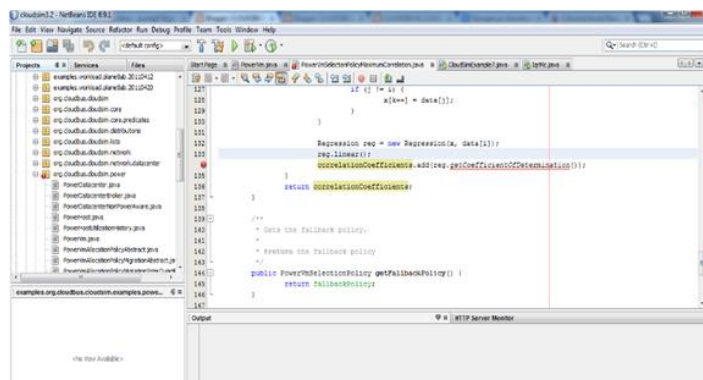
1- CloudSim



شکل ۴- محل تنظیم پارامترهای شبیه ساز کلود



شکل ۳- یک نمای کلی از پلت فرم نرم افزار کلود سیم



شکل ۵- نمای اولیه شبیه ساز کلود

۷- محاسبات ابر و امنیت داده‌ها

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 می‌گردند. در نتیجه در این سیستم‌ها امنیت به عنوان یک نگرانی عمده مورد توجه قرار می‌گیرد. معماری امنیتی باز^۱ چارچوب آزادی فراهم می‌کند که به راحتی در برنامه‌های کاربردی، برای جامعه معماری امنیتی یکپارچه شده است. کاربران نهایی از طریق اینترنت به عنوان یک نقطه ورودی به محیط مه دسترسی دارند که این ورودی باید امن باشد. 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^۲، TLS^۳ و IPSec^۴ استفاده کرد. مسأله دیگری که بین کاربران نهایی و مه باید امن باشد این است که هیچ یک از آنها نباید در ارتباط تصدیق بین کاربران و مه شوند. 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 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 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 قسمت بعد راهکارهایی آورده‌شده است که بعد از ارائه مدل بیان گردیده‌اند.

- 1- Open Security Architecture
- 2- Security Sockets Layer
- 3- Transport Layer Security
- 4- Internet Protocol Security

۸- بررسی امنیت مدل تحقیق

امنیت محاسبات مه 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 مه، 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 استفاده می‌شود. تمامیت در واقع اطمینان از اعتبار و کامل بودن اطلاعات است. تمامیت داده‌ها نه تنها بر درست بودن داده‌ها 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 پیشنهادی، استفاده از کلیدهای منحصر به فرد در برقراری ارتباط و همچنین رمزگذاری با الگوریتم‌های متقارن 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 در دسترس بودن سرورهای عامل کاربر 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 مه وجود دارد انجام می‌گیرد. همچنین عمل به‌روزرسانی سرور معیوب به سرعت توسط سرورهای پشتیبان موجود انجام می‌شود. در ادامه این فصل مدل پیشنهادی با نظرخواهی از ۳۲ متخصص ارزیابی شده و نتایج ارزیابی با استفاده از نمودارها و آزمون‌های آماری مورد تجزیه و تحلیل قرار گرفته است. در ادامه ابتدا روش ارزیابی مدل پیشنهادی توضیح داده شده است و سپس نتایج حاصل از ارزیابی، مورد تجزیه و تحلیل قرار گرفته است.

۹- بررسی روش پیشنهادی تحقیق

برای بررسی مدل با پرسشنامه 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 مه مطالعاتی داشتند توزیع گردید. پرسشنامه طراحی شده از دو بخش تشکیل شده است.

جدول ۲- مقایسه امتیازات دو روش انتخاب شده براساس معیارهای تعیین شده. (از روی پرسشنامه)

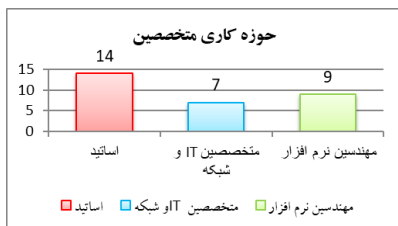
روش ورود تکی	روش سنتی	روش کربروس	روش دو طرفه
ردیف	ویژگی های مورد نظر		
۱	آمادگی اجرای هر روش	۱۳۶	۹۲
۲	راحتی آموزش و اطلاع رسانی به افراد	۱۲۵	۱۰۹
۳	سهولت یادگیری و قابل فهم بودن	۱۳۲	۱۱۰
۴	میزان تطابق با دانش روز دنیا	۶۰	۱۲۹
۵	صرفه جویی در زمان	۵۰	۱۳۱
۶	صرفه جویی در هزینه	۵۳	۱۳۰
۷	اهمیت به موضوع امنیت	۵۵	۱۲۹
۸	قدرت احراز هویت	۶۰	۱۲۷
۹	عدم نیاز به بخاطر سپردن نام‌های کاربری و رمز عبورهای متعدد	۵۲	۱۲۷
۱۰	سهولت و راحتی در استفاده	۱۱۸	۱۰۲
۱۱	امکان مدیریت دسترسی کاربران	۶۸	۱۲۰
۱۲	قابلیت استفاده هر روش در ورود تکی	۱۱۴	۱۰۲
۱۳	امکان و سهولت پیاده‌سازی هر روش	۱۲۶	۱۱۰
۱۴	میزان کارایی روش از همه لحاظ	۹۲	۱۲۷
میانگین امتیازات			
		۸۸/۶۴	۱۱۷/۵

قسمت اول پرسشنامه (که پرسشنامه شماره یک نامگذاری شد) شامل ۱۰ سؤال برای سنجش میزان آشنایی افراد با موضوع می‌باشد. در قسمت دوم پرسشنامه (که پرسشنامه شماره دو نامگذاری شد) با توجه به معیارهای مشخص شده، سه روش ورود تکی مورد بررسی و مقایسه قرار گرفته‌اند. روش اول ورود تکی به صورت سنتی است. ورود تکی سنتی نوعی ورود تکی است که با

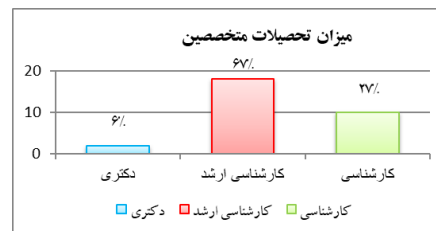
استفاده از آن، کاربر برای هر بار ورود و دسترسی به قسمت‌های مجاز، نیاز به وارد کردن نام کاربری و رمز عبور خود دارد. روش دوم، روش کربروس می‌باشد که در آن هر کاربر برای ورود تکی و استفاده از سرویس‌ها، هر بار باید برای هر سرور (سرور احراز هویت و ارائه‌دهنده سرویس) به صورت دو طرفه احراز هویت شود. روش سوم، ورود تکی با استفاده از زبان نشانه‌گذاری اثبات امنیت و مبتنی بر مه 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 نام کاربری و رمز عبور خود، امکان دسترسی به قسمت‌های مختلف و استفاده از امکانات مه را دارند. همچنین در ابتدای هر پرسشنامه، تحصیلات و شغل افراد پرسیده شده است. در جدول ۲ معیارهای انتخابی و امتیازات بدست‌آمده برای هر معیار پس از جمع‌آوری پرسشنامه‌ها آورده شده است. در ادامه از این نتایج برای ارزیابی و تجزیه و تحلیل روش استفاده شده است

۹-۱- اطلاعات توصیفی پاسخ دهندگان

اطلاعات فراوانی شرکت کنندگان در نمودارهای زیر آمده است.



شکل ۷- حوزه کاری افراد شرکت کننده در ارزیابی مدل پیشنهادی



شکل ۶- میزان تحصیلات افراد شرکت کننده در ارزیابی مدل پیشنهادی

۱۰- جایگزین کردن متغیرها در عامل‌ها

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 گرفته می‌شوند و بقیه عامل‌ها در گروه‌هایی شامل این عامل‌های معنی‌دار قرار می‌گیرند. برای این کار از نتایج جدول عاملی که در نرم‌افزار SPSS بدست‌آمده استفاده می‌گردد. در این مرحله دو جدول مورد بررسی قرار می‌گیرد. جدول ۳ 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 تعیین شده در تبیین واریانس متغیرهای مورد مطالعه است. در نتیجه نیازی به حذف هیچ سؤالی در پرسشنامه مورد نظر نیست. جدول ۴ 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 تبیین شده 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 ارائه شده است که مقادیر ویژه آنها بزرگتر از عدد یک باشند. ستون Rotation Sums of Squared Loadings مجموعه‌ی مقادیر عامل‌های استخراج شده بعد از چرخش را نشان می‌دهد. همان‌طور که مشخص است پنج عامل قابلیت تبیین واریانس‌ها را دارند. شکل ۸ تغییرات مقادیر ویژه را در ارتباط با عامل‌ها نشان می‌دهد. این نمودار برای تعیین تعداد بهینه مولفه‌ها به کار 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. 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 اعضای هر گروه مشخص می‌شود. با توجه به این جدول عامل اول در واریانس سؤالات ۴، ۵، ۶ و ۱۳ تاثیر بیشتری دارد. به همین ترتیب عامل دوم در واریانس سؤالات ۱۰، ۳، ۱۴، ۱۱ و ۸، عامل سوم در واریانس سؤالات ۱۱ و ۱۲، عامل چهارم در واریانس سؤالات ۴، ۷ و ۹ و در نهایت عامل پنجم در واریانس سؤالات ۱ و ۲ تاثیر بیشتری دارد. این پنج گروه در جدول ۶ آورده شده‌اند. 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 نتیجه ماتریس چرخیده‌شده مولفه‌ها و استفاده از پیشینه پژوهش می‌باشد.

جدول ۳- 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 ۴- مقدار ویژه و واریانس متناظر با عاملها

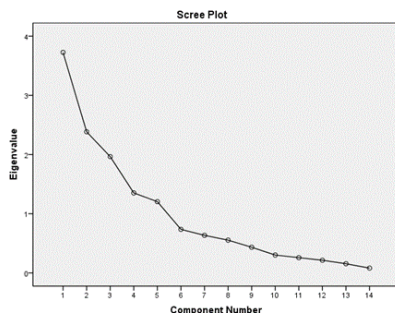
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative%	Total	% of Variance	Cumulative%	Total	% of Variance	Cumulative%
1	3.726	26.614	26.614	3.726	26.614	26.614	2.704	19.318	19.318
2	2.384	17.029	43.643	2.384	17.029	43.643	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	1.110	7.890	86.980	1.578	10.580	86.542
7	.635	4.533	85.719	1.055	7.006	93.540	1.497	9.680	97.245
8	.554	3.955	89.675	1.005	6.115	100.52	1.359	8.572	100.23
9	.434	3.097	92.772	0.098	5.740	110.35	1.256	7.256	110.48
10	.302	2.159	94.932	0.068	4.630	120.58	1.118	6.358	123.65
11	.258	1.844	96.776	0.042	3.350	130.74	1.006	5.987	135.87
12	.214	1.531	98.307	0.028	2.780	140.95	0.0086	4.365	140.58
13	.156	1.112	99.419	0.018	1.540	155.36	0.0064	3.256	158.69
14	.081	.581	100.000	0.006	0.008	168.62	0.0051	2.854	167.25

جدول ۵- ماتریس چرخیده شده 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 ۶- تجزیه معیارها به پنج گروه عاملی

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



شکل ۸- تغییرات مقادیر ویژه در ارتباط با عامل‌ها



شکل ۹- مقایسه امتیازات سه روش ورود تکی

در این پرسشنامه علاوه بر مدل پیشنهادی، دو روش ورود تکی سنتی و کربروس نیز مورد ارزیابی قرار گرفته‌اند تا بتوان نتایج حاصل از این ارزیابی را برای مقایسه سه روش به کار برد. در جدول ۲ امتیازات هر یک از سه روش گفته شده آورده شده بود. با توجه به این امتیازات، شکل ۹ نمودار حاصل از مقایسه سه روش را نشان می‌دهد. همان‌طور که در این شکل مشخص است، مدل پیشنهادی این پژوهش توانسته است بالاترین امتیاز را به دست آورد.

۱۱- مقایسه میانگین روش‌ها با آزمون فریدمن

در آزمون فریدمن فرض H_0 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 (H_1). در آزمون فریدمن اگر سطح پوشش آماره‌ی آزمون از پنج درصد کمتر باشد، فرض آماری H_0 رد شده و فرض آماری H_1 نتیجه گرفته می‌شود. نتایج جدول ۸ نشان می‌دهد که سطح پوشش آماره آزمون برابر $0/000$ می‌باشد که از $0/05$ کمتر است. در نتیجه فرض H_0 رد می‌شود و وجود تفاوت بین روش‌ها نتیجه گرفته می‌شود. میانگین رتبه‌ها در سه روش نیز در جدول ۷ ارائه شده است.

جدول ۸- نتیجه آزمون فریدمن برای امتیازات سه روش ورود تکی در SPSS

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

جدول ۷- نتیجه آزمون فریدمن میانگین رتبه‌ها در سه روش

	Mean Rank
Sonata	1.57
Kerberos	1.43
dotarafe	3.00

۱۱-۱ آزمون نرمال بودن

از آزمون کلموگروف-اسمیرنوف به منظور تعیین عادی یا نرمال بودن توزیع داده‌ها استفاده شده است. برای آزمون نرمال بودن فرض‌های آماری به صورت زیر تنظیم می‌شوند:

H_0 : توزیع داده‌های مربوط به هر یک از متغیرها نرمال است.

H_1 : توزیع داده‌های مربوط به هر یک از متغیرها نرمال نیست.

با توجه به خروجی‌های بدست آمده چنانچه در آزمون کلموگروف-اسمیرنوف، Sig. بیشتر از $0/05$ باشد می‌توان داده‌ها را با اطمینان بالایی نرمال فرض کرد. در غیر این صورت نمی‌توان گفت که توزیع داده‌ها نرمال است. جدول ۹ نتیجه انجام آزمون کلموگروف-اسمیرنوف را برای سه روش ورودتکی نشان می‌دهد. همان‌طور که در این جدول نشان داده شده است مقدار آماره توصیفی (Asymp. Sig.) بدست آمده از $0/05$ بیشتر است و در نتیجه فرض H_0 که نشان‌دهنده نرمال بودن توزیع داده‌ها می‌باشد، تایید می‌گردد.

جدول ۹- 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

۱۲- تحلیل واریانس برای مقایسه میانگین دو یا چند گروه

برای انجام تحلیل واریانس توزیع داده‌ها که در اینجا همان امتیازات هستند، باید جامعه نرمال باشند. از نتایج به دست آمده از آزمون کلموگروف-اسمیرونوف و با توجه به اثبات نرمال بودن توزیع داده‌ها در این آزمون، می‌توان نتیجه گرفت که تحلیل واریانس برای این پژوهش نتایج صحیحی تولید می‌کند. جدول ۱۰ 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 به دست آمده از تحلیل واریانس نیز می‌باشد، مجموع مربعات، میانگین مربعات و درجات آزادی آورده شده است. در این جدول با توجه به اینکه مقدار sig کوچک‌تر از ۰/۰۵ می‌باشد، می‌توان نتیجه گرفت 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 نشان می‌دهد. 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 نشان می‌دهد. در این جدول هر روش با یک عدد نشان داده شده است (ورود تکی سنتی با عدد یک، ورود تکی کربروس با عدد دو و ورود تکی با احراز هویت دو طرفه با عدد سه نشان داده شده‌اند).

جدول ۱۰- تایج 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	.9088	.0002
Total	26886.976	41	4777.39	10.1078	.0012

Levene Statistic	df1	df2	Sig.
54.588	2	39	.000

	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

۱۳- نتیجه گیری

نتایج حاصل از تحقیق نشان داد که مهم‌ترین مزیت استفاده از این مدل پیشنهادی در این تحقیق، احراز هویت دو طرفه عامل کاربر و ارائه‌دهنده هویت می‌باشد که منجر به افزایش امنیت بیشتر ارتباط می‌شود و جعل و فریب کاری نیز کاهش پیدا می‌کند. 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 را

تضمین می‌کند و از این پس ارائه‌دهنده هویت به عنوان یک لینک قوی در ارتباط و زنجیره امنیت این ارتباط در نظر گرفته می‌شود. مانند بیشتر سیستم‌های ورود تکی، سیستم‌های ورود تکی سازمانی برای کاهش زمانی که یک کاربر برای ورود اعتباراتش برای ورود به برنامه‌های کاربردی مختلف دارد، طراحی شده‌اند. این کار با استفاده از تکنیک پرکردن خودکار رمز عبورها برای کاربر انجام می‌شود، بنابراین آنها نیاز به وارد کردن دستی آنها ندارند. و این باعث کاهش سربار حافظه و زمان می‌شود. 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. و این می‌تواند باعث کاهش سربار حافظه و زمان شود. همچنین با استفاده از کلید رمزنگاری متقارن باعث کاهش سربار حافظه به میزان ۳۶ درصد می‌شود.

منابع

۱. فرهادی، میلاد و بختیاری، سعید، ۱۳۹۷، چالش‌ها در شبکه‌های مه، چهارمین کنفرانس ملی فناوری در مهندسی برق، کامپیوتر، تهران.
۲. شعبانی ابوذر، روستایی رسول، مروری بر رایانش مه، کاربردها و مقایسه آن با رایانش ابری، اولین کنفرانس ملی کامپیوتر و فناوری اطلاعات، صفحات ۴۷-۳۲، ۱۳۹۷.
۳. صدرالساداتی، سید محسن و کارگر، محمدجواد، ۱۳۹۲، چالش‌های امنیتی در رایانش ابری و ارائه راهکاری جهت بهبود امنیت آن در راستای توسعه خدمات عمومی دولت الکترونیک، همایش مهندسی کامپیوتر و توسعه پایدار با محوریت شبکه‌های کامپیوتری، مدل‌سازی و امنیت سیستم‌ها، مشهد، دوره ۱۲، شماره ۴، صص ۱۲۴-۱۳۵.
۴. رستمی یسار علی، حمدی مجید، فاطمی مقدم فراز، بررسی محاسبات لبه و مه، دو فصل‌نامه محاسبات و سامانه‌های توزیع شده، سال اول، شماره اول، صفحات ۵۸-۴۷، ۱۳۹۸.
۵. مؤذن محمد، احمدی حسین، سلامت ناصر، رایانش مه و اینترنت اشیاء، پنجمین کنفرانس بین‌المللی مهندسی برق و کامپیوتر با تأکید بر دانش بومی، صفحات ۳۳-۱۹، ۱۳۹۶.
۶. نجات، سیدحسن، ۱۳۹۹، بررسی مشکلات امنیتی در محاسبات ابری و راهکار بهبود امنیتی (مروری)، دهمین کنفرانس بین‌المللی فناوری اطلاعات، کامپیوتر و مخابرات، دوره ۱۶، شماره ۲، صص ۱۲-۲۴.
۷. ورمقانی، عباس و رسول روستایی، ۱۳۹۸، بررسی مسایل امنیتی و حریم شخصی محاسبات مه برای اینترنت اشیاء، دومین کنفرانس ملی تحقیقات کاربردی در مهندسی برق کامپیوتر و فناوری اطلاعات، شیراز، موسسه عالی علوم و فناوری.
8. Abeshu, A., Haftu, D., Reda, T., & Chilamkurti, N. Differential flow space allocation scheme in SDN based fog computing for IoT applications. *Journal of Ambient Intelligence and Humanized Computing*, 1(1),2021 .
9. E. Haleplidis, K. Pentikousis, S. Denazis, J. H. Salim, D. Meyer, and O. Koufopavlou,
10. Group, F. (n.d.). *Network Innovation through OpenFlow and SDN Principles and Design*
11. *Softwaredefined networking (sdn): Layers and architecture terminology*,
12. Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. I Resilience and survivability in communication networks : Strategies , principles , and survey of disciplines. *Computer Networks*, 44(.), 1215–1215. 2021
13. Nunes, B. A. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. A survey of software-defined networking: Past, present, and future of programmable networks.2020
14. Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. Software-defined networking: A comprehensive survey. 2021
15. Tank, G., Dixit, A., Vellanki, A., & Annapurna, D. *Software Defined Networks : TheNew Norm for Networks 2113–2115*. 2020
16. W. Stallings, «Sdn and openflow», *Acupuncture in Medicine*, vol. 11, no. 3, pp. 1–11,2021