دانشگاه آزاد اسلامی

واحد بندرعباس

دانشکده: فنی و مهندسی

پایان‌نامه برای دریافت درجه کارشناسی ارشد (M.Sc.)

رشته: کامپیوتر گرایش :نرم‌فزار

عنوان:

استفاده از سیستم فازی جهت ارزیابی اعتماد امنیت گرا و غیر امنیت گرا در رایانش ابری

استاد راهنما:

دکتر محمد شایسته

استاد مشاور:

دکتر هدایت الله دلاکی

نگارنده:

میثم سالاری

بهار ۱۴۰۰

H

به نام خدا

معاونت پژوهش و فن‌آوری

منشور اخلاق پژوهش

با یاری از خداوند سبحان و اعتقاد به اینکه عالم محضر خداست و همواره ناظر بر اعمال انسان و به منظور پاسداشت مقام بلند دانش و پژوهش و نظر به اهمیّت جایگاه دانشگاه در اعتلای فرهنگ و تمدن بشری، ما دانشجویان و اعضاء هیأت علمی واحدهای دانشگاه آزاد اسلامی متعهد می‌گردیم اصول زیر را در انجام فعالیت‌های پژوهشی مد نظر قرار داده و از آن تخطّی نکنیم:

۱-اصل حقیقت‌جویی: تلاش در راستای پیجویی حقیقت و وفاداری به آن و دوری از هر گونه پنهان‌سازی حقیقت.

۲-اصل رعایت حقوق: التزام به رعایت کامل حقوق پژوهشگران و پژوهیدگان (انسان، حیوان و نبات) و سایر صاحبان حق.

۳-اصل مالکیت مادی و معنوی: تعهد به رعایت کامل حقوق مادی و معنوی دانشگاه و کلیه‌ی همکاران پژوهش.

٤-اصل منافع ملّی: تعهد به رعایت مصالح ملّی و در نظر داشتن پیشبرد و توسعه کشور در کلیه‌ی مراحل پژوهش.

٥-اصل رعایت انصاف و امانت: تعهد به اجتناب از هر گونه جانبداری غیرعلمی و حفاظت از اموال، تجهیزات و منابع در اختیار.

٦-اصل رازداری: تعهد به صیانت از اسرار و اطلاعات محرمانه افراد، سازمان‌ها و کشور و کلیه‌ی افراد و نهادهای مرتبط با تحقیق.

۷-اصل احترام: تعهد به رعایت حریم‌ها و حرمت‌ها در انجام تحقیقات و رعایت جانب نقد و خودداری از هر گونه حرمت‌شکنی.

۸-اصل ترویج: تعهد به رواج دانش و اشاعه‌ی نتایج تحقیقات و انتقال آن به همکاران علمی و دانشجویان به غیر از مواردی که منع قانونی دارد.

۹-اصل برائت: التزام به برائت‌جویی از هر گونه رفتار غیر حرفه‌ای و اعلام موضع نسبت به کسانی که حوزه‌ی علم و پژوهش را به شائبه‌های غیرعلمی می‌آلایند.

نا م و نام خانوادگی: میثم سالاری

تاریخ و امضاء

تقديم به آنانكه هرگز تسليم سختي‌هاي زندگي نمي‌شوند.

درود و سلام به شهدای عزیزی که دنیا را آزمودند و
راه نیک علم را برایمان روشن نمودند،
وسپاس فراوان از استادان عزیزم که در این راه ،
راهنما و دلسوز ما بودند،
و تشکر از خانواده خوبم که یار همیشگی ام بودند.

فهرست مطالب

فهرست جدول ها و نمودارها

فهرست شکل ها

چکیده

در رایانش ابری، اعتماد، به عنوان یک راه حل برای بالا بردن امنیت، توجه زیادی از محققان را به خود جلب کرده است. این مقوله یکی از مهمترین روش‌ها برای بهبود قابلیت اطمینان منابع محاسباتی فراهم شده در محیط ابر بوده و نقش مهمی را در محیط‌های تجاری ابر بر عهده دارد. همچنین، اعتماد یکی از موانع اصلی رشد و به کارگیری رایانش ابری توسط صنعت فناوری‌اطلاعات است، به این دلیل که ساز و کار قابل اطمینان و پربازده‌ای برای ارزیابی آن وجود ندارد. اعتماد، برآورد توانایی منبع ابر در کامل کردن یک کار در محیط‌های توزیع شده بر اساس اعتبار، هویت و دسترس‌پذیری است، که این به کاربر در انتخاب سرویس مناسب بر روی زیرساخت ابر ناهمگن کمک می‌کند. در این پژوهش، یک مدل اعتماد بر اساس معیارهای امنیتی سنجیده شده توسط خبرگان حوزه‌ی رایانش ابری ارائه داده‌ایم. نتایج شبیه‌سازی نشان می‌دهد که رویکرد پیشنهادی ما با در نظر گرفتن معیارهای کیفیت سرویس، قابل اعتمادترین سرویس در محیط ابر را انتخاب می‌نماید، همچنین نسبت به مدل‌های مشابه مزایای بیشتری دارد.

کلمات کلیدی: رایانش ابری، امنیت، اعتماد، منطق‌فازی

فصل اوّل:

کلّیات تحقیق

۱-۱. مقدمه

در حال حاضر محاسبات ابری یک موضوع مورد توجه در عرصه‌ی پژوهشی و همچنین در عرصه‌ی سازمانی می‌باشد، زیرا محاسبات ابری دارای ویژگی‌های خوبی مانند: پایین بودن مقدار سرمایه‌گذاری، فراهم آوردن سرویس‌های قابل اتکا، نگهداری آسان، قابلیت انعطاف‌پذیری و قابلیت گسترش سریع می‌باشد. اما اگر بخواهیم به راستی محاسبات ابری را پیاده‌سازی نماییم، باید به تدریج آن را در عرصه‌های آکادمیک، قانونی و نهادی بهبود ببخشیم. در این رابطه، مسئله اعتماد یکی از بزرگترین موانع برای توسعه‌ی محاسبات ابری می‌باشد. در اینجا دو حالت وجود دارد: اعتماد کاربران به فراهم‌کننده‌ی پردازشات ابری و اعتماد فراهم‌کننده‌ی پردازشات ابری به کاربران و مشتریان خود، که ما سعی می‌نماییم حالت اوّل را با توجه به اهمیّتی که در نزد کاربران دارد، بررسی نماییم.

بنابراین، در محاسبات ابری، اعتماد متقابل کاربران و فراهم‌کنندگان سرویس نیاز است به طوری که هیچکدام قابل چشم‌پوشی نمی‌باشد، برای مثال، زمانی که کاربران کنترل و مدیریت داده‌ها و ابزار را در محیط ابری از دست می‌دهند، نگرش آنها نسبت به سرویس‌های ابری به سمت بی‌اعتمادی سوق پیدا می‌کند، که این امر شامل ریسک در رابطه با افشای داده‌ها، امنیت مکان ذخیره‌سازی داده‌ها، داده‌های سرمایه‌گذاری شده، از دست دادن داده‌ها، انقطاع سرویس و از بین رفتن فراهم‌کننده‌ی محاسبات ابری می‌باشد، اما محاسبات ابری می‌تواند هزینه‌های مربوط به عملیات محاسبه را کاهش داده و در عین حال کارایی آن را بهبود ببخشد، بنابراین خیلی از کشورها منابع لازم را برای سرمایه‌گذاری در محاسبات ابری فراهم می‌نمایند.

اگر بخواهیم فرض کنیم که کاربران به فراهم‌کنندگان سرویس اعتماد کرده و می‌خواهند داده‌ها و پردازشات روزانه‌شان را در اختیار آنها قرار دهند، لازمه‌ی این فرض در توسعه‌ی کامل محاسبات ابری یافت می‌شود. در نتیجه پاسخ به این سؤال که: "آیا کاربران می‌توانند به فراهم‌کنندگان سرویس، اعتماد نمایند یا خیر ؟" خیلی مهم است و این موضوع اصلی پژوهش اغلب پژوهشگران می‌باشد. در محاسبات ابری به دلیل دسترسی مستقیم کاربران به نرم‌افزار و سیستم عامل و حتی محیط برنامه‌نویسی و زیرساخت‌های شبکه که به وسیله فراهم‌کننده‌ی سرویس ابری فراهم می‌شود)، احتمال خرابی و اثرات آن برای این سیستم‌ها در مقایسه با خرابی‌های احتمالی از طرف کاربران فعلی اینترنت خیلی بیشتر و بدتر می‌باشد. لذا برآورد اعتماد در استفاده از سرویس‌های ابری چه از لحاظ امنیتی و چه از لحاظ غیرامنیتی، بسیار حائز اهمیّت بوده و تأثیر به سزایی در شفافیت ارائه‌ی

خدمات این نوع سرویس‌ها خواهد داشت. البته، در این پژوهش در برخی موارد، به علّت خوانایی بهتر جملات، از رایانش ابری به عنوان محاسبات ابری نیز نام برده‌ایم که هر دو دارای یک معنا و مفهوم هستند.

۱-۲. بیان مسئله

رایانش ابری به عنوان یک سبک محاسباتی جدید در اواخر سال ۲۰۰۷ پا به عرصه وجود نهاد. در واقع این مفهوم تعمیمی است بر روی بحث تغییر بر حسب نیاز که می‌گوید در حالی که نیازهای کاربران تغییر می‌کند ارائه‌دهنده می‌بایست سخت‌افزار، نرم‌افزار و سرویس‌های مرتبط با آن نیاز را تأمین نماید. امروزه با توسعه سریع اینترنت غالباً نیاز کاربران از طریق اینترنت به تحقق می‌رسد و همین امر پایه و اساس رایانش ابری را شکل داده است. بدین منظور برای کاربران بالقوه سؤالاتی پیش می‌آید نظیر اینکه آیا می‌توان به سرویس‌های ابری اعتماد نمود؟ یا اساس اعتماد در رایانش ابری چیست؟ شاید ویژگی‌های یک سرویس ابری در مرحله‌ی اوّل مورد قضاوت قرار گیرد که کاربران بر چه اساس باید به ویژگی‌های مفید ادعا شده توسط ارائه‌دهندگان سرویس‌های ابری باور داشته باشند؟ پاسخ به اینگونه سؤالات برای گسترش روزافزون استفاده از سرویس‌های ابری ضروری است. به همین منظور جهت ارزیابی میزان اعتماد در استفاده از رایانش ابری و افزایش آن در بین کاربران مختلف ناگزیر باید چالش‌های مختلفی را مورد بررسی قرار داد که مهمترین آن امنیت است. از آنجا که کاربران این محیط از محل دقیق داده‌های خود و از کدهایی که روی داده‌های آنها اجرا می‌شود اطلاع ندارند و همچنین صحت، سازگاری و جامعیت داده‌ها باید تا سطح بالایی تضمین شود، لذا لازم است معیاری برای سنجش و ارزیابی عوامل مختلف به دست آورد تا با استفاده از آن قابلیت اعتماد که از مسائل مطرح در حوزه‌ی رایانش ابری است را افزایش داد، زیرا اعتماد را می‌توان به عنوان یک عامل تأثیرگذار در انتخاب یک سرویس خاص توسط کاربر دانست.(شیخ و دکتر کمار، ۲۰۱۵)

از سوی دیگر، پردازش‌ابری بستری را فراهم می‌نماید که ثابت شده است نسبت به سایر ارائه‌دهندگان سرویس بر روی شبکه از نظر هزینه به‌صرفه می‌باشد و قابلیت اتکا، قابلیت گسترش و قابلیت انعطاف‌پذیری بالایی دارد. برای مثال یک برنامه به جای صرف هزینه‌ی زیاد برای خرید و نصب به صورت یک ابر در اختیار یک کاربر قرار می‌گیرد. چالش مهمی که در اینجا مطرح می‌شود این است که آیا سازمان‌هایی که این سرویس‌ها را ارائه می‌دهند نیز می‌توانند به کاربرانی که درخواست سرویس دادند اعتماد کنند؟ یا آیا می‌توان چارچوبی برای مدیریت این اعتماد برای دو طرف بیان کرد؟ مدیریت اعتماد یکی از بحث‌های داغ و چالشی در زمینه‌ی پردازش ابری می‌باشد. قابلیت اعتماد در خیلی از سیستم‌ها مورد توجه می‌باشد و شامل ویژگی‌های مهمی همچون قابلیت‌اطمینان، امنیت و مواردی دیگر می‌باشد. در این زمینه، اعتماد به عنوان یک

سرویس را می‌توان مطرح نمود که یک پروتکل جدید برای بازخورد اعتماد و حفظ حریم خصوصی کاربران ارائه می‌نماید. (یان و ژانگ، ۲۰۱٤)

البته شناسایی مواردی که به نظر کاربران رایانش ابری مهمترین معیارهای مؤثر بر کیفیت خدمات به شمار می‌آید بسیار حائز اهمیت می‌باشد. بدین جهت ناگزیر باید به تعیین و سنجش معیارهایی که سبب افزایش رضایت کاربران می‌گردد پرداخت تا با شناسایی نقاط قوت و ضعف و ارتقاء کیفیت آنها قادر به پاسخگویی به انتظارات فزاینده‌ی آنها بود.

مسئله‌ای که در این راستا با توجه به مطالب فوق می‌توان مطرح نمود این است که، معیارهای تأثیرگذار بر رضایت کاربران و در راستای آن افزایش اعتماد آنها در استفاده از سرویس‌های ابری چیست؟ و در نهایت چگونه می‌توان به کمک منطق‌فازی، میزان اعتماد در استفاده از سرویس‌های ابری را ارزیابی نمود؟ که در این راستا می‌توان با بهره‌گرفتن از معیارهای امنیتی به عنوان ورودی‌های منطق‌فازی به این امر مهم دست یافت. این معیارها به کمک پرسشنامه‌ی دیمتل و پاسخ‌دهی حداقل ۵۰ نفر از افراد خبره، شناسایی و مقداردهی می‌شوند. البته باید عنوان نمود که یک فرد خبره، فردی است که بر حسب نیاز مدل‌های اعتماد در رایانش ابری، اطلاعات کافی درباره‌ی امنیت، ساختار، زیرساخت، استانداردها و توافقات سطح سرویس در سرویس‌های ابری داشته باشد.

۳-۱. فرضیه‌های تحقیق

۱. ارزیابی میزان اعتماد در استفاده از سرویس‌های ابری به کمک منطق‌فازی دارای دقت بالایی است.
۲. تأثیرات معیارهای امنیت در رایانش ابری بر روی یکدیگر در ارزیابی اعتماد نیز اثر دارد.

۱-٤. اهداف و انگیزه‌های تحقیق

تکامل رایانش ابری بر پایه‌ی اینترنت نیازمند اعتماد و امنیت به عنوان چالش‌های اصلی است که باید حل شود. عملیات تجاری مرسوم شامل متن‌های قانونی مناسب با امضاها و اعتماد طرف‌ها به یکدیگر است. در رایانش ابری بر پایه اینترنت نیاز شدیدی به ایجاد اعتماد بین تأمین‌کنندگان خدمات و کاربران است. ساز و کار مناسب مدیریت اعتماد، زیان کاربران و زیان تأمین‌کنندگان خدمات را نیز کاهش می‌دهد. ساز و کارهای موجود اعتماد مانند اعتبارسنجی و اعطای مجوز برای رایانش ابری مناسب نیست. همچنین، همیشه قابلیت اطمینان مؤثری را ارائه نکرده است. مثلاً مشتریان Salesforce.com در تاریخ ۱۲ فوریه ۲۰۰۸ به مدت ٦ ساعت قادر به دریافت خدمات نبودند و سه روز بعد خدمات Amazon EC2، به مدت ۳ ساعت دچار وقفه شدند. در این پایان‌نامه قصد داریم یک مدل اعتماد جدید بر اساس معیارهای امنیتی در سطح رایانش ابری به

کمک منطق‌فازی را ارائه دهیم که شامل سنجش اثر معیارهای امنیت بر یکدیگر و به تناسب آن بر میزان اعتماد کاربران در سطح رایانش ابری است.

۱-۵. تعاریف واژه‌ها

۱-۵-۱. رایانش ابری

محاسبات ابری یک مدل سرویس‌دهی است که در آن امکانات محاسباتی و ذخیره‌سازی مانند پردازنده، حافظه، پهنای باند و نرم‌افزارهای گوناگون به صورت برخط، تحت شبکه، با دسترسی سریع و آسان و به صورت فراوان و انعطاف‌پذیر در اختیار کاربران قرار می‌گیرد. در این مدل، شرکت‌هایی اقدام به فراهم کردن امکانات محاسباتی و ذخیره‌سازی در سطح وسیع کرده و در اختیار کاربران قرار می‌دهند. برای استفاده از این سرویس‌ها، کاربران لازم است که داده‌های خود را بر روی محیط فیزیکی فراهم‌کننده‌ی محاسبات ابری ذخیره نمایند. در این صورت کاربران دیگر کنترل فیزیکی بر روی داده‌های خود ندارند و این فراهم‌کننده‌ی محاسبات ابری است که این داده‌ها را تحت کنترل خود دارد. در این شرایط لازم است که کاربران به یک فراهم‌کننده‌ی محاسبات ابری اعتماد کنند تا بتوانند با خیال راحت داده‌های خود را بر روی مرکز داده‌های فراهم‌کننده ذخیره کرده و از سرویس‌های او استفاده نمایند. اکنون می‌بایست کاربران بدانند چه خطراتی داده‌های آنان را تهدید کرده و با اطمینان از رفع این خطرات از سرویس‌های محاسبات ابری استفاده نمایند. در این شرایط، این خطرات هستند که اعتماد کاربران را به مدل محاسبات ابری خدشه‌دار می‌نمایند. همچنین، فراهم‌کنندگان محاسبات ابری نیز می‌بایست از این خطرات آگاهی داشته باشند تا با در نظر گرفتن آنها و تلاش در راستای کاهش و رفع این خطرات گام برداشته تا بتوانند اعتماد کاربران در استفاده از سرویس‌های مورد نظرشان را جلب نمایند.(رشیدی، ۱۳۹۱)؛ لذا این تحقیق به منظور افزایش اعتماد در خصوص استفاده از خدمات و سرویس‌های ابری، چالش‌های پیش رو را بررسی و نسبت به بازخورد میزان اعتماد از طریق ارزیابی میزان اعتماد تأکید دارد.

۱-۵-۲. اعتماد

۱-۲-۵-۱. مفهوم اعتماد

اعتماد و اعتبار ریشه در علوم اجتماعی دارند که ماهیت و رفتار جامعه‌ی بشری را مطالعه می‌کنند. اعتماد در مورد "اطمینان" و تضمین این است که افراد، داده‌ها، موجودیت‌ها، اطلاعات یا فرایندها به صورت مورد انتظار عمل یا رفتار خواهند کرد.(رابینسون و والری، ۲۰۱۰)؛ از جنبه‌ی دیگر، اعتماد به عنوان یک حالت ذهنی، که شامل انتظار، باور و تمایل برای ریسک کردن است، تعریف می‌گردد. از این رو، اعتماد یک عامل

سرنوشت‌ساز در رایانش ابری به شمار می‌رود. در شرایط کنونی، اعتماد به شدت به قضاوت کاربران ابر در مورد اعتبار تأمین‌کنندگان ابری وابسته است.(شیملال و دیپک، ۲۰۱٤)

اعتماد می‌تواند به عنوان یک موجودیت مبتنی بر قابلیت اطمینان و باور راسخ مبتنی بر ویژگی موجودیت تعریف گردد. اعتماد باور راسخ در توانایی یک موجودیت برای عمل کردن به همان گونه‌ی مورد انتظار است، که این باور راسخ یک مقدار ثابت مرتبط با موجودیت نیست اما تقریباً زیر سلطه‌ی رفتار موجودیت قرار داده می‌شود و تنها در محدوده‌ی یک زمینه معین در زمان مفروض به کار برده می‌شود.(عزالدین و مهسوران، ۲۰۰۲)

این بدین معنا است که باور راسخ مقدار پویایی است که به موقع تغییر می‌کند. بر اساس نظر گراندیسون، اعتماد عمل جمع‌آوری، تدوین، تحلیل و ارزیابی دلیل مرتبط با شایستگی، درستی امنیت و قابلیت اعتماد با هدف انجام تخمین و تصمیم در ارتباط با رابطه‌ی اعتماد است.(گراندیسون و سلومان، ۲۰۰۲)

بنابراین اعتماد نتیجه‌ی پیشرفت به سوی امنیت یا تأمین اهداف حریم خصوصی است. تحقیقات اخیر در مورد امنیت ابر، اعتماد را به عنوان یکی از مسائل بحرانی شناسایی کرده است. اعتماد به طور رسمی به صورت رابطه‌ای تعریف می‌شود که در آن یک موجودیت به موجودیت دوّم اعتماد می‌کند، به گونه‌ای که موجودیت اوّل فرض می‌کند که موجودیت دوّم دقیقاً به صورتی که موجودیت اوّل انتظار دارد رفتار خواهد کرد. به طور کلّی، اعتماد می‌تواند به اعتماد مستقیم و اعتماد توصیه‌شده طبقه‌بندی شود.

در مراجع علمی، توافق عمومی در مورد تعریف اعتماد و این که مدیریت اعتماد شامل چه مواردی است، وجود ندارد. در زمینه علوم کامپیوتر، مارش از اوّلین کسانی است که به مطالعه در زمینه‌ی اعتماد محاسباتی پرداخته و تعریف واضحی از مفهوم اعتماد را ارائه داده است و نهایتاً یک مدل اعتماد را در سیستم هوش مصنوعی توزیع شده معرفی کرده است تا عامل‌ها بتوانند بر اساس اعتماد تصمیم‌گیری کنند.(مارش، ۱۹۹٤)

تعریف دقیق‌تر برای اعتماد این است که: "اعتماد وضعیت روانی شامل مفهومی است برای قبول آسیب‌پذیری مبتنی بر انتظارات مثبت از نیّات یا رفتار دیگران".(پیرسون و بن امر، ۲۰۱۰)؛ از طرف دیگر اعتماد یک مفهوم نسبی است و اینکه ما چقدر به یک عامل اعتماد کنیم بستگی به زمینه‌ی فعالیت دارد. پس باید به ازای هر زمینه‌ی فعالیت، اعتماد را به طور جداگانه و مستقل از سایر زمینه‌ها محاسبه نمود.(نوری، ۱۳۹۰)

شباهت میان چندین عامل و یک شبکه‌ی اجتماعی را در نظر بگیرید. عوامل و افراد با یک شیوه‌ی مشابه، اطلاعات را جمع‌آوری می‌کنند و یکدیگر را برای توسعه‌ی اعتماد به هم، مدلسازی می‌نمایند. با این وجود، همه‌ی متخصّصان کامپیوتر یک تصوّر مبهم و پیچیده را برای اعتماد ارائه می‌دهند. که این موضوع عمدتاً به

آن دلیل است که هیچ توافق عمومی در مورد یک تعریف مشخص از اعتماد وجود ندارد و تمامی تعاریف آن در مفاهیم کلیدی زیر با هم مشترک هستند:

- ✓ اعتماد تنها زمانی نقش خواهد داشت که محیط، متغیّر و دارای ریسک باشد.
- ✓ اعتماد مبنایی است که تصمیمات قطعی بر اساس آن گرفته می‌شود.
- ✓ اعتماد بر پایه‌ی دانش و تجربه‌ی قبلی ایجاد می‌شود.
- ✓ اعتماد یک تصوّر ذهنی بر اساس نظر و ارزش‌های یک فرد می‌باشد.
- ✓ اعتماد همراه با زمان تغییر می‌کند و دانش و تجربه‌ی جدید، تأثیر مهمی بر روی دانش و تجربه‌ی قدیمی خواهد داشت.
- ✓ اعتماد وابسته به زمینه می‌باشد.
- ✓ اعتماد چند بعدی می‌باشد.(نوری، ۱۳۹۰)

2-2-5-1. ابعاد اعتماد در رایانش ابری

مفهوم اعتماد در ابعاد مختلف متفاوت است. به طور کلّی، دو گروه از محاسبات اعتماد وجود دارد: محاسبات اعتماد امنیت‌گرا و محاسبات اعتماد غیر امنیت‌گرا. (مین وو، ۲۰۱۰)

- محاسبات اعتماد امنیت‌گرا

در محاسبات اعتماد امنیت‌گرا، اعتماد مکانیزمی برای بهبود امنیت، ارائه‌ی مباحثی در حوزه‌ی احراز هویت، اختیارها، کنترل دسترسی و محرمانگی فراهم می‌کند. اعتماد درجه‌ای است که توسط یک جسم هدف(مانند نرم‌افزار، دستگاه، سرور و...) امن در نظر گرفته می‌شود.

- محاسبات اعتماد غیر امنیت‌گرا

ارزیابی اعتماد مبتنی بر اعتبار با محاسبات اعتماد غیر امنیت‌گرا مرتبط است. به طور کلّی، یک سرویس زمانی شهرت خوبی کسب می‌کند که در آن خدمات با کیفیت مناسب در طی یک دوره بلند مدت ارائه گردد. در اکثر سیستم‌ها، ارزیابی معمولاً بر رأی مشتری استوار است. با این حال، برای محاسبه‌ی صحیح ارزش نهایی، مطالعه بر روی روابط بین ارزیاب و ارزیابی‌شونده اهمیّت دارد و ممکن است به کاهش اعتبار رتبه و یا به دست آوردن اعتماد بیشتر کمک نماید.

۳-۵-۱. منطق فازی

1-3-5-1. تعریف منطق فازی

اگر از ما پرسیده شود منطق فازی چیست شاید ساده‌ترین پاسخ بر اساس شنیده‌ها این باشد که منطق فازی یک نوع منطق است که روش‌های نتیجه‌گیری در مغز بشر را جایگزین می‌کند. مفهوم منطق فازی توسط دکتر لطفی‌زاده، پروفسور دانشگاه کالیفورنیا در برکلی، ارائه گردید و نه تنها به عنوان متدولوژی کنترل ارائه شد بلکه راهی برای پردازش داده‌ها، بر مبنای مجاز کردن عضویت گروهی کوچک به جای عضویت گروهی دسته‌ای ارائه کرد. به جهت نارسا و نابسنده بودن قابلیت کامپیوترهای ابتدایی تا دهه‌ی ۷۰ این تئوری در سیستم‌های کنترلی به کار برده نشد. پروفسور لطفی‌زاده این‌طور استدلال کرد که بشر به ورودی‌های اطلاعاتی دقیق نیازی ندارد بلکه قادر است تا کنترل تطبیقی را به صورت بالایی انجام دهد. پس اگر ما کنترل‌کننده‌های فیدبک را در سیستم‌ها طوری طراحی کنیم که بتواند داده‌های مبهم را دریافت کند، این داده‌ها می‌توانند به طور ساده‌تر و مؤثرتری در اجرا به کار برده شوند.

با این تعاریف، منطق فازی دارای این قدرت است که در تنظیم سیستم‌ها از میکروکنترل‌های ساده و کوچک و جاسازی شده گرفته تا سیستم‌های چند کاناله شبکه شده بزرگ یا سیستم‌های کنترلی به کار برده شود. این منطق دارای قدرت اجرایی در سخت‌افزار، نرم‌افزار یا ترکیبی از هر دوی اینها است. در واقع منطق فازی راه ساده‌ای را برای رسیدن به یک نتیجه‌ی قطعی و معیّن بر پایه‌ی اطلاعات ورودی ناقص، خطادار، مبهم و دو پهلو فراهم می‌نماید. منطق فازی یک قانون ساده بر مبنای" IF x And y THEN z " را بیان می‌نماید. در منطق فازی، جملاتی هستند که مقداری درست و مقداری نادرست هستند. برای مثال، جمله‌ی" هوا سرد است"، یک گزاره منطقی فازی می‌باشد که درستی آن گاهی کم و گاهی زیاد است. گاهی همیشه درست و گاهی همیشه نادرست و گاهی تا حدودی درست است. منطق فازی در واقع با استفاده از مجموعه‌ای از معلومات نادقیق که با الفاظ و جملات زبانی تعریف شده‌اند به دنبال استخراج نتایج دقیق است.(رئوف نژاد، ۱۳۸٦)

2-3-5-1. اجزای ابتدایی و اصول اوّلیه تئوری مجموعه فازی

در قسمت مبدل فازی، متغیّرهای با مقادیر حقیقی به یک مجموعه فازی تبدیل شده از طریق ماشین رابط فازی و قوانین پایه، نتایج به قسمت غیرفازی‌ساز منتقل شده که یک مجموعه‌ی فازی را به یک متغیّر با مقدار حقیقی تبدیل می‌کند. به بیان دیگر، اطلاعات ورودی اغلب مقادیری پیچیده‌اند و این اعداد به مجموعه‌های فازی تبدیل می‌گردند. مدل‌ها بر اساس منطق فازی شامل قوانین اگر، آنگاه تفسیر می‌گردند.

حقیقت آن است که بعد از عبارت اگر، یک منطق مقدم بیان می‌گردد و بر اساس آن ما حقیقت دیگر را مورد بررسی قرار می‌دهیم که بعد از آنگاه می‌آید و در آن نتیجه‌ی کار توضیح داده می‌شود. در واقع منطق فازی تجربه و دانش انسانی را به صورت ترکیبی از اعداد در مقابل وی قرار می‌دهد و او را قادر می‌سازد تا تصمیمی بر اساس ریاضیات و منطق بگیرد. ریاضیات فازی یک فرامجموعه از منطق بولی است که بر مفهوم درستی نسبی دلالت می‌کند. منطق کلاسیک هر چیزی را بر اساس یک سیستم دوتایی نشان می‌دهد (درست یا غلط،۰ یا ۱، سیاه یا سفید) ولی منطق فازی درستی هر چیزی را با یک عدد که مقدار آن بین صفر و یک است نشان می‌دهد.

مثلاً اگر رنگ سیاه را عدد صفر و رنگ سفید را عدد یک نشان دهیم، آن گاه رنگ خاکستری عددی نزدیک به صفر خواهد بود. دکتر لطفی‌زاده نظریه‌ی سیستم‌های فازی را معرفی کرد. در فضایی که دانشمندان علوم مهندسی به دنبال روش‌های ریاضی برای شکست دادن مسایل دشوارتر بودند، نظریه‌ی فازی به گونه‌ای دیگر از مدلسازی اقدام کرد.(رئوف نژاد، ۱۳۸٦)

٤-٥-١. تکنیک دیمتل

تکنیک دیمتل برای اوّلین بار توسط مرکز تحقیقات مؤسسه‌ی یادبودهای جنگ در ژنو و در فاصله‌ی سال‌های 1972تا 1976 ابداع شد.(فونتلا و گابوس، ۱۹۷٦)؛ هدف از این تکنیک، مطالعه‌ی مسائل پیچیده، تحلیل آنها و ایجاد ساختاری بر اساس این تحلیل است.(هانگ و همکاران، ۲۰۱۰)

با استفاده از این تکنیک می‌توانیم ارتباط علّت و معلولی میان عوامل را درک کنیم و بر اساس آن یک مدل جامع پدید آوریم. تکنیک دیمتل یکی از ابزارهای تصمیم‌گیری برای مواردی است که چندین معیار برای تصمیم‌گیری وجود دارد. این روش می‌تواند مسائل کیفی را به معیارهای کمّی برای تصمیم‌گیری تبدیل کند. در تصمیم‌گیری چندمعیاره، هنگامی که لازم باشد مسائل پیچیده را در حین روشن کردن روابط میان عناصر مهم آنها حل کنیم، باید از روش دیمتل استفاده کنیم. در این تکنیک، روابط کمّی بین عوامل چندگانه یک مسئله و تأثیر هر یک از آنها بر دیگری محاسبه می‌شود. گفتنی است که در این روش، میزان تأثیر مستقیم و غیرمستقیم عوامل بر یکدیگر سنجیده می‌شود. با روش دیمتل می‌توانیم عوامل موجود را به دو گروه علّت و معلول تقسیم نماییم. برای این کار باید مراحل زیر را طی کنیم:

1. ایجاد ماتریس روابط مستقیم(A): برای تشکیل این ماتریس از پاسخ‌دهندگان خواسته می‌شود که روابط میان هر جفت شاخص را با عددی بین 0 تا ۱۰۰ نمایش دهند. اگر تعداد پاسخ‌دهندگان بیش از یک نفر باشد، ماتریس نهایی، از به دست آوردن میانگین هندسی اعداد پاسخ‌دهندگان حاصل می‌شود.

2. نرمالیزه کردن ماتریس روابط مستقیم: بر مبنای ماتریس روابط مستقیم، ماتریس نرمالیزه از طریق فرمول زیر به دست می‌آید.

$$X = k \cdot A \qquad (۱-۱)$$

که در آن k برابر است با:

$$K = \frac{۱}{max_{۱\leq i\leq n}\sum_{j=۱}^{\infty}(a_{ij})} \qquad i.j = ۱.۲.\ldots.n \qquad (۱-۲)$$

3. به دست آوردن ماتریس روابط کلّی: هنگامی که ماتریس روابط مستقیم نرمالیزه به دست آمد، ماتریس روابط کلّی (T) می‌تواند از فرمول زیر محاسبه شود که در آن I نشانگر ماتریس واحد است.

$$T = X(I - X)^{-۱} \qquad (۱-۳)$$

٤. ایجاد نمودار علّت و معلول: در این نمودار که از نتایج ماتریس روابط کلّی به دست می‌آید، D+R محور افقی را نشان می‌دهد که نشانگر اهمیت شاخص است و از اضافه کردن D به R به دست می‌آید که D ، جمع ستونی ماتریس روابط کلّی است و نشان می‌دهد که یک شاخص چقدر از شاخص‌های دیگر تأثیر می‌پذیرد؛ در حالی که R نشان‌دهنده‌ی جمع سطری ماتریس روابط کلّی است و نشان می‌دهد که یک شاخص چقدر بر شاخص‌های دیگر تأثیر می‌گذارد. محور عمودی R-D از تفریقD از R به دست می‌آید و می‌تواند شاخص‌ها را به دو گروه علّت و معلول تقسیم کند. اگر این مقدار مثبت باشد، شاخص به گروه علّت تعلّق دارد و در صورت منفی بودن، متعلّق به گروه معلول است.(طالبی و آرش‌پور، ۱۳۹۲)

مزیت روش دیمتل این است که می‌تواند اولویت‌بندی شاخص‌ها را چه از لحاظ تأثیرپذیری و چه از لحاظ تأثیرگذاری مشخص کند. این مهم باعث می‌شود به معیارهایی که بیشترین تأثیر را بر سایر معیارها می‌گذارند، اهمیت بیشتری داده شود و معیارهایی که بیشترین تأثیر را از سایر معیارها می‌پذیرند، از سرمایه‌ی کمتری بهره‌مند شوند.(طالبی و آرش‌پور، ۱۳۹۲)

در این پژوهش، جهت به دست آوردن داده‌های فازی، از این تکنیک بهره گرفته و برای هر پاسخ‌دهنده یک پرسشنامه ارائه می‌شود و ملاک عمل قرار می‌گیرد. با این تفاوت که از پاسخ‌دهندگان خواسته می‌شود که روابط بین هر جفت از معیارها را با عددی بین ۰ تا ۵ نمایش دهند. لذا این پرسشنامه حاوی دو جدول بوده که به کمک امتیازهای تخصیص داده شده به وضعیت‌های فازی که در جدول زیر مشاهده می‌نمایید تکمیل می‌شود:

جدول(۱-۱) امتیازات مربوط به وضعیت‌های فازی

بدون تأثیر	تأثیر همسان	تأثیر خیلی کم	تأثیر کم	تأثیر زیاد	تأثیر خیلی زیاد
۰	۱	۲	۳	٤	۵

جدول بعدی نیز مثال خوبی برای نشان دادن اوّلین جدول مربوط به پرسشنامه‌ی مذکور است که نشان‌دهنده‌ی میزان اثرگذاری معیارها بر یکدیگر است.

جدول(۲-۱) نمونه‌ی پرسشنامه‌ی مربوط به اثر معیارها بر یکدیگر

←	معیار۱	معیار۲	معیار۳
معیار ۱			
معیار۲			
معیار۳			

پس از مشخص شدن معیارهای برتر که به کمک تکنیک دیمتل به دست می‌آیند دوّمین جدول را خواهیم داشت که حاوی میزان اثر معیارها بر اعتماد می‌باشد. بنابراین، مجموع امتیازات داده شده به معیارهای انتخابی در جدول(۲) پرسشنامه‌ها را محاسبه نموده و پس از انتقال به بازه‌ی صفر تا صد به عنوان ورودی فازی استفاده می‌نماییم. نمونه‌ی جدول(۲) را در زیر می‌توانید مشاهده نمایید.

جدول(۳-۱) نمونه‌ی پرسشنامه‌ی مربوط به اثر معیارها بر اعتماد

↓	معیار۱	معیار۲	معیار۳
اعتماد			...

کلمات کلیدی فصل اوّل

Trust as a Service (TAAS)	اعتماد به عنوان یک سرویس
Fuzzy Logic or Fuzzy Theory	منطق فازی
Fuzzier	مبدل فازی
Defuzzier	غیرفازی‌ساز
Decision Making Trial And Evaluation (DEMATEL)	دیمتل

فصل دوّم:

مبانی تحقیق و مروری بر تحقیقات انجام شده

۱-۲. مقدمه

رایانش ابری یک فناوری نوظهور است که به توانمندی‌های جهان تجارت، منابع محاسباتی انعطاف‌پذیری را می‌افزاید. در کنار چندین مزیت رایانش ابری، هنوز موارد چالش‌برانگیز فراوانی مانند: امنیت و حفظ اسرار داده‌های ذخیره شده در ابر و عدم اعتماد به تأمین‌کنندگان خدمات ابری وجود دارد. اعتماد یکی از موانع اصلی رشد و به کارگیری رایانش ابری توسط صنعت فناوری اطلاعات است، به این دلیل که ساز و کار قابل اطمینان و پربازده‌ای برای ارزیابی اعتماد وجود ندارد. اگر چه مزایایی مختلفی توسط محققان برای رایانش ابری پیشنهاد شده است، اما بیشتر سازمان‌ها هنوز تردید دارند و به دلیل فقدان اعتماد به تأمین‌کنندگان ابر به سمت رایانش ابری نمی‌روند.

در این فصل ابتدا مکانیزم‌های برقراری اعتماد و انواع مدل‌های اعتماد در سطح رایانش ابری را مورد بررسی قرار داده و در ادامه‌ی آن به معرفی و شرح چند مدل اعتماد می‌پردازیم.

۲-۲. مکانیزم‌های موجود برای برقراری اعتماد

موجودیت‌ها در رایانش ابری به تأمین‌کننده‌ی خدمات ابری و کاربر ابری تقسیم می‌گردند. ارزیابی اعتماد به آثار تعاملات میان تأمین‌کننده‌ی خدمت ابری و کاربر ابری وابسته است. اثر تعامل پویا است و به هنگام بودن خوبی دارد.(حبیب و همکاران، ۲۰۱۲)؛ در واقع، ارزیابی اعتماد در محاسبات ابری به مشکل‌های امنیت و حفظ حریم خصوصی می‌پردازد. بدین منظور یک فرآیند دو مرحله‌ای به منظور بررسی مورد اعتماد بودن ابر معرفی می‌شود.(فان و همکاران، ۲۰۱۳)؛ این مراحل به صورت زیر هستند:

۱. ارائه‌ی معماری چند وجهی سیستم مدیریت اعتماد برای محاسبات ابری که هدف آن شناسایی ارائه‌دهندگان ابری قابل اعتماد از نظر صفات مختلف است.(حبیب و همکاران، ۲۰۱۱)

که این همان معرفی معماری مدیریت اعتماد است که حفظ رجیستری از ارئه‌دهندگان خدمات ابری و اعتماد مربوط به ارزش‌ها، محاسبه‌ی اعتماد CSP بر اساس بازخورد در مورد توافقنامه‌های مختلف و ویژگی‌های کیفیت سرویس را در پی دارد. (موچاهاری و سینا، ۲۰۱۲)؛ یک مدل اعتماد SLA جهت ارزیابی خدمات ابری برای کمک به کاربران جهت انتخاب منابع قابل اعتماد است که ترکیبی از چارچوب SLA برای محاسبات ابری است.(محمد و همکاران، ۲۰۱۰)؛ در این زمینه مدل اعتماد مناسب برای زیرساخت به عنوان یک سرویس نیز عنوان شده است.(گویال و همکاران، ۲۰۱۲)

۲. ارائه ی یک چارچوب برای رسیدگی به مسائل و پاسخگویی آنها در محاسبات ابری.(کو و همکاران، ۲۰۱۱)؛ توزیع این چارچوب اجازه می‌دهد که کاربر قابلیت اعتماد سرویس‌های ابری را تعیین نماید.(آباواجی، ۲۰۰۹)

فرایندهای مختلف برقراری اعتماد در محاسبات ابری به صورت زیر بیان می‌شوند:

۱. مبتنی بر اثر تعامل

در رایانش ابری، کاربر ابری درخواست‌های سرویس را به تأمین‌کننده‌ی سرویس ابری ارسال می‌کند، سپس تأمین‌کنندگان سرویس ابر سرویس‌های متناظر برای کاربران ابری را فراهم می‌کنند.(ووآ و همکاران، ۲۰۱۳) موجودیت‌های ابری یکدیگر را پس از هر تعامل موفق و ناموفقی ارزیابی می‌کنند.

۲. اعتماد مستقیم

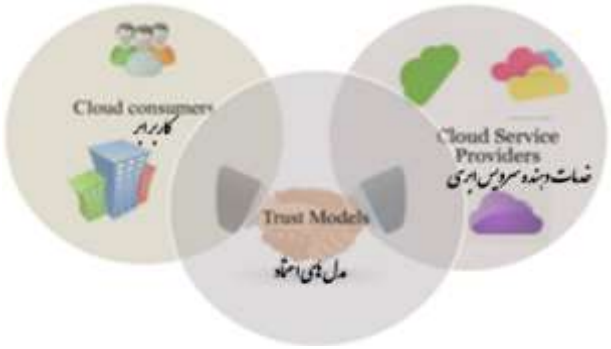
هر تعامل به عنوان یک اثر در نظر گرفته می‌شود. با پرس‌وجوی مجموعه اثرE، می‌توانیم تعداد تعاملات معتبر را در پنجره‌های زمانی محاسبه کنیم. اعتماد مستقیم میان موجودیت‌ها توسط تعاملات مستقیم محاسبه می‌شود.

۳. اعتبار

اعتماد و اعتبار همبسته هستند، اما معنی متفاوتی دارند. اعتماد میان دو موجودیت برقرار می‌شود، در حالی که اعتبار یک موجودیت یک نظر اجتماع از یک جامعه به سوی آن موجودیت است. موجودیت اطلاعات توصیه شده و مطلق را از دیگر موجودیت‌ها که با موجودیت ارزیابی شده به طور مستقیم تعامل کرده‌اند، کسب می‌کند. در مورد تعامل غیرمستقیم با موجودیت ارزیابی شده، اطلاعات توصیه شده‌اش در نظر گرفته نخواهد شد. معمولاً یک موجودیت که اعتبار بالایی دارد توسط بسیاری از موجودیت‌های موجود در آن جامعه مورد اعتماد قرار می‌گیرد. یک موجودیت که نیاز به قضاوت اعتماد بر روی یک معتمد دارد، ممکن است از اعتبار برای محاسبه یا تخمین سطح اعتماد آن معتمد استفاده کند.(هوآنگ و نیکول، ۲۰۱۳)؛ سیستم‌های اعتبار به طور گسترده‌ای در شبکه‌های تجارت الکترونیک استفاده می‌شوند. اعتبار سرویس‌های ابری یا تأمین‌کنندگان سرویس ابری مسلماً انتخاب سرویس‌های ابری کاربران ابری و در نتیجه تأمین‌کنندگان ابری را تحت تأثیر قرار خواهد داد.

٤. توافقات سطح سرویس

یک توافق‌سطح‌سرویس، یک قرارداد یا توافق قانونی میان تأمین‌کننده‌ی یک سرویس IT و مشتری آن سرویس، درباره‌ی سطح آن سرویس یا کیفیت سرویسی که باید تحویل داده شود است. به عنوان مثال ویژگی‌های کیفیت سرویس: زمان پاسخ، بازدهی، دسترس‌پذیری، امنیت، و غیره است. توافق سطح سرویس، نظر درباره‌ی تأمین‌کننده‌ی زیربنای ابری با نقطه نظر کاربر ابری را تعیین می‌کنند. اعتماد با استفاده از چندین شاخص توافق سطح سرویس محاسبه و ایجاد می‌شود. شکل(۱-۲) گویای عوامل دخیل در توافق سطح سرویس می‌باشد.



شکل(۱-۲) توافق سطح سرویس میان کاربران و تأمین‌کنندگان خدمات ابری

پس از برقراری اعتماد اوّلیه و استفاده از یک سرویس ابری، کاربر ابری نیاز به اثبات، محاسبه‌ی مجدد و ارزیابی اعتماد دارد. نظارت بر کیفیت سرویس و تصدیق توافق سطح سرویس، پایه‌ی اصلی مدیریت برای رایانش ابری است. پارامترهای توافق سطح سرویس، شامل حافظه‌ی دستیابی تصادفی ، فضای حافظه‌ی ذخیره‌سازی، پهنای باند شبکه، ظرفیت پردازش و سیستم عامل هستند. RAM برای فراهم کردن مجازی‌سازی در گره و سپس فراهم کردن سرعت بهتر برای اجرای وظیفه (تکه ابر) استفاده می‌شود. حافظه RAM بالاتر، دسترس‌پذیری را تضمین می‌کند. حافظه‌ی ذخیره‌سازی مقدار اعتماد قابل قبولی در گره فراهم می‌کند. با پهنای باند بهتر، ارتباط بهتری میان گره‌ها وجود خواهد داشت. سیستم عامل بایستی به اندازه‌ی کافی قابل اطمینان باشد تا در زمان اجرا از کار نیفتد. ظرفیت پردازش به معنای میانگین بار کاری پردازش شده توسط گره است.(شیملال و دیپک، ۲۰۱٤)

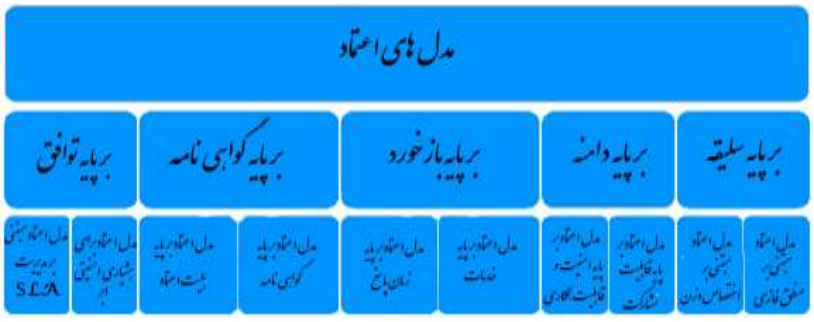
3-2. انواع مدل‌های اعتماد

برای سفارش جهت تجاری‌سازی فناوری ابری، کاربران ابر باید از منابع ارائه‌دهندگان، تکمیل شدن کار ارائه شده به عنوان سطح قابل قبول سرویس و اطلاعات پردازش شده اطمینان داشته باشند. این مهم به دلیل عدم

اعتمادی که به تأمین‌کنندگان خدمات ابری وجود دارد و اینکه ساز و کار قابل اطمینان و پربازده‌ای برای ارزیابی اعتماد وجود ندارد بسیار حائز اهمیّت است. به همین دلیل مدل‌های اعتماد متنوعی بین تأمین‌کنندگان خدمات ابری و مشتریان ابر پیشنهاد شده‌اند به صورتی که هر مدل ویژگی‌های متفاوتی را پشتیبانی می‌کند و خدمات ابری را بر اساس پارامترها و نیازمندی‌های گوناگون ارزیابی می‌نماید. لذا برای یک شرکت بزرگ (یا هر گروه علاقه‌مند دیگر) تصمیم‌گیری در مورد انتخاب و پیاده‌سازی مدل اعتماد به صورتی که خواسته‌ها را برآورده سازد، دشوار می‌گردد.

در محیط رایانش ابری، نیازمندی‌های امنیت و کیفیت خدمات از یک مصرف‌کننده به دیگری تفاوت دارد، زیرا یکی ممکن است ترجیح دهد که از جامعیت داده‌ای و حفاظت ارائه شده توسط تأمین‌کننده خدمات ابری اطمینان حاصل کند، در حالی که مصرف‌کننده‌ی دیگر خدماتی از ابر را انتخاب کند که بیشترین عرض باند در دسترس و بهترین زمان پاسخ را داشته باشد. بنابراین انتخاب مدل اعتماد مناسب به صورتی که بیشترین ویژگی‌های امنیت، کنترل و کیفیت خدمات را تضمین کند، بسیار با اهمیّت است.

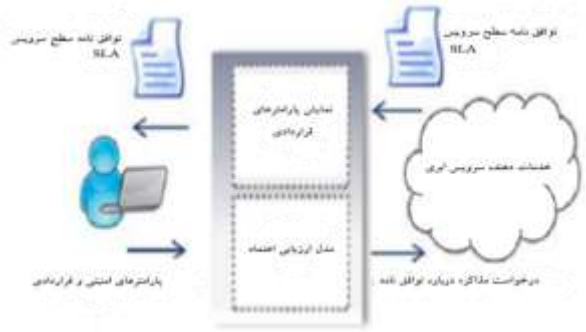
در عین حال تا آنجا که ما اطلاع داریم، هیچ معیار سنجشی برای ارزیابی این مدل‌های اعتماد در ابر معرفی نشده است. لازم است که ضوابط ارزیابی معرفی شود به صورتی که بتواند مدل‌های اعتماد مختلف را ارزیابی و تحلیل کند و روش‌هایی برای انتخاب مناسب‌ترین مدل در رایانش ابری ارائه نماید. ضوابط ارزیابی پیشنهادی به شرکت‌های بزرگ در انتخاب بهترین مدلی که قادر به برقراری اعتماد در محیط ابر است، یاری می‌رساند. (کانوال و همکاران، ۲۰۱۳) شکل(۲-۲) مدل‌های اعتماد مختلفی را نشان می‌دهد که به صورت بر پایه‌ی توافق، بر پایه‌ی گواهی‌نامه، بر پایه‌ی بازخورد، بر پایه‌ی دامنه و مدل‌های اعتماد سلیقه‌ای طبقه‌بندی شده‌اند.



شکل(۲-۲) نمونه‌هایی از مدل‌های اعتماد در رایانش ابری

۱-۳-۲. مدل‌های اعتماد بر پایه‌ی توافق

به صورتی که در شکل(۳-۲) نشان داده شده است، ایجاد اعتماد در این طبقه‌بندی بر اساس قراردادها و توافق‌های امضا شده توسط تأمین‌کنندگان خدمات رایانش ابری برای ارائه خدمات گوناگون به مشتریان است.

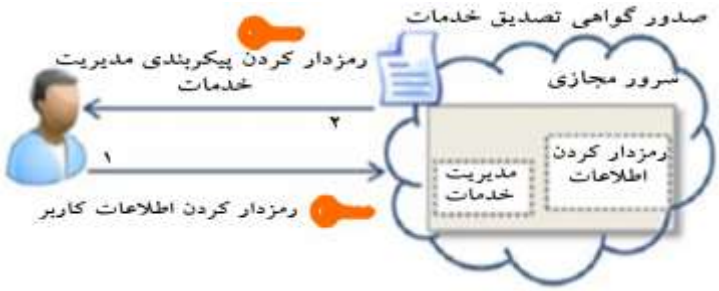


شکل(۳-۲) مدل اعتماد بر پایه‌ی توافق

در این مدل توافق‌های سطح سرویس و قراردادهای اجرای سرویس، اساس ایجاد اعتماد را تشکیل می‌دهند. برای به وجود آمدن اعتماد به تأمین‌کننده‌ی خدمات رایانش ابری، نگرانی‌های امنیتی گوناگون و صفت‌های کیفیت خدمات در قراردادها و توافق‌ها گنجانیده می‌شود.

۲-۳-۲. مدل‌های اعتماد بر پایه‌ی گواهی‌نامه

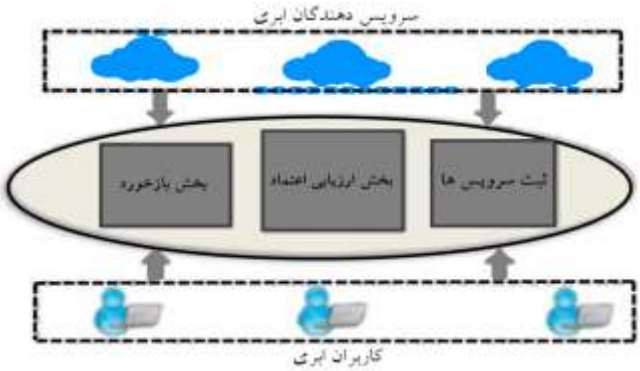
ایجاد اعتماد بین مشتریان و تأمین‌کنندگان خدمات رایانش ابری از راه گواهی‌نامه‌ها (صادر شده توسط نهادهای استاندارد شده)، بلیت‌های اعتماد، کلیدهای خصوصی و عمومی، کلیدهای تأیید شده ماژول سکوی مطمئن که توسط یک نهاد سوّم قابل اطمینان یا شرکت اعطا کننده‌ی گواهی‌نامه صادر می‌شود، ایجاد می‌گردد. همان طور که در شکل(٤-۲) نشان داده شده است، بلیت‌های اعتماد برای تضمین جامعیت، در دسترس بودن و محرمانه بودن داده‌ها در ابر صادر می‌شوند و اطمینان مشتریان را به رفتار مورد انتظار خدمات ابر افزایش می‌دهند.



شکل(٤-۲) مدل اعتماد بر پایه‌ی گواهی‌نامه

۳-۳-۲. مدل‌های اعتماد بر پایه‌ی بازخورد

همان طور که در شکل(۲-۵) نشان داده شده است، این گروه شامل مدل‌های اعتمادی است که به منظور محاسبه اعتماد در خدمت‌های ابر، بازخورد و نظرهای سایر مشتریان را جمع‌آوری می‌کند.



شکل(۵-۲) مدل اعتماد بر پایه‌ی بازخورد

این مدل اعتماد، بازخوردهای مربوط به پارامترهای گوناگون کیفیت خدمت و امنیت ارائه شده توسط تأمین‌کنندگان خدمات ابر را جمع‌آوری و مدیریت می‌کند. مورد اعتمادترین تأمین‌کننده خدمات رایانش ابری شرکتی است که همه صفت‌های مورد نیاز کیفیت خدمت و امنیت را برای مشتریان خود برآورده سازد.

همچنین این مدل، چارچوبی برای مدیریت اعتماد در محیط‌های ابری بر پایه‌ی معماری سرویس‌گرا است. در این مدل به این دلیل که رفتار سرویس‌های ابری با توجه به بازخورد اعتماد جمع‌آوری شده از طرف کاربران می‌باشد، مدل مناسبی برای تمایز بین بازخوردها به منظور ارزیابی اعتماد سرویس‌های ابری است. این مدل شامل دو پارامتر اجماع اکثریت و چگالی بازخوردها برای محاسبه‌ی ارزش اعتماد در سرویس‌های ابری می‌باشد. بعلاوه با طراحی مدل تعیین تکرار، منجر به دسترسی‌پذیری بالای سرویس مدیریت اعتماد شده که بدین صورت سرویس مدیریت اعتماد به صورت همیشگی در سطح مطلوبی از دسترسی قرار دارد. همچنین برای جلوگیری از اشکالات معماری متمرکز، سرویس مدیریت اعتماد پیشنهادی اجازه می‌دهد تا نگهداری و بازخورد اعتماد به صورت توزیع شده مدیریت شود. یکی از چالش‌های این مدل در نظر گرفتن ارزش یکسان برای تمامی سرویس‌های یک سرویس‌دهنده می‌باشد.(نور و شنگ، ۲۰۱۱)

٤-۳-۲. مدل‌های اعتماد بر پایه‌ی دامنه

همان طور که در شکل(۲-٦) نشان داده شده است، مدل‌های اعتماد بر پایه‌ی دامنه، بیشتر در رایانش گرید مورد استفاده قرار می‌گیرند، اما مدل‌های اعتماد بسیار اندکی تحت این گروه‌بندی برای محیط ابر پیشنهاد شده است. ایده‌ی اصلی این مدل، تقسیم ابر به تعدادی دامنه‌ی مستقل و ایجاد دو نوع رابطه‌ی اعتماد داخل دامنه‌ای و خارج دامنه‌ای است که به ترتیب از جدول‌های اعتماد مستقیم و توصیه‌شده استخراج می‌شوند. مقادیر اعتماد داخل دامنه‌ای به تراکنش‌های بین موجودیت‌هایی که در یک دامنه قرار دارند، بستگی دارد. اگر یک موجودیت

نیازمند محاسبه‌ی مقدار اعتماد یک موجودیت دیگر باشد، جدول اعتماد مستقیم را بررسی می‌کند اما اگر مقدار اعتماد مستقیم پیدا نشد، سپس به دنبال مقدارهای اعتماد توصیه شده از موجودیت‌های دیگر می‌گردد.

شکل(٦-٢) مدل اعتماد بر پایه‌ی دامنه

همچنین این مدل حل مسائل امنیتی را در محیط‌های ابری دنبال می‌نماید. با استفاده از این مدل، کاربر ابری قادر به انتخاب سرویس‌دهندگان مختلف می‌باشد. این مدل مبتنی بر دامنه است، به این معنا که منابع و سرویس‌های مربوط به سرویس‌دهندگان مشابه، در یک دامنه قرار گرفته و مدیریت می‌شوند. همچنین این مدل بین نقش سرویس‌دهنده و سرویس‌گیرنده تفاوت قائل شده و برای هر کدام استراتژی‌های متفاوتی را بررسی می‌نماید. علاوه بر آنچه گفته شد در این مدل توصیه‌گران اعتماد به عنوان یک سرویس در نظر گرفته می‌شوند. یکی از محدودیت‌های این مدل عدم توجه به بازخوردهای مخرب است.(لی و پینگ، ۲۰۰۹)

٥-٣-٢. مدل‌های اعتماد سلیقه‌ای

مدل‌های اعتماد سلیقه‌ای، اعتماد را به زیر کلاس‌های گوناگون مانند اعتماد مدیریتی، اعتماد کد و اعتماد اجرایی بر سکوی ابر تقسیم می‌کنند. یکی از دو روش متفاوت الگوریتم‌های احتمال یا تئوری فازی برای اختصاص وزن و محاسبه هر زیر کلاس اعتماد به کار گرفته می‌شوند. تئوری احتمال و فازی دو روش اصلی ارزیابی اطلاعات اعتماد درباره یک CSP مشخص و خدمات ارائه شده است.

مثالی واضح برای این مدل از اعتماد که در شبکه‌های گرید استفاده شده است، مدل اعتماد مبتنی بر منطق فازی است که یک مدل پویا بوده و بر اساس تعریف و توصیف اعتماد، استدلال فازی و ارزیابی روابط اعتماد به روزرسانی و تکامل می‌یابد.(سانگ و هوانگ، ۲۰۰۵)

٦-٣-٢. نمونه‌هایی از مدل‌های اعتماد

مدل اعتماد مبتنی بر نیازمندی‌های کاربران: این مدل، چارچوب و مکانیزمی برای اندازه‌گیری کیفیت و اولویت

سرویس‌های ابری بر پایه‌ی نیازمندی‌های کاربران پیشنهاد می‌دهد و تمرکز آن بر روی تجزیه و تحلیل کارایی سرویس‌دهندگان Iaas می‌باشد. سرویس‌های ابری با استفاده از مؤلفه‌های این چارچوب، امتیازدهی شده و بر پایه‌ی فرایند سلسله مراتبی تحلیلی، بر اساس کاربردهای مختلف سرویس‌ها، با توجه به نیازمندی‌های کیفیتی، مورد ارزیابی قرار می‌گیرند. یکی از چالش‌های این مدل، عدم توجه کافی به بازخوردهای مخرب از طرف بازخورددهندگان می‌باشد.(گارگا و همکاران، ۲۰۱۳)

مدل اعتماد توسعه‌پذیر: این مدل بر اساس تحقیقات و تجزیه و تحلیل‌های انجام شده بر روی مشخصات و معناشناسی اعتماد است. هسته‌ی اصلی این مدل شامل الگوریتم اعتماد مستقیم، الگوریتم توصیه شده و الگوریتم پویا می‌باشد. همچنین این مدل شامل متد ارزیابی زمان، برای نمایش اعتماد مستقیم و متد ارزیابی فاصله، برای محاسبه‌ی اعتماد توصیه شونده می‌باشد. یکی از چالش‌های این مدل، عدم دسترسی به اطلاعات در صورت عدم وجود اطلاعات مستقیم و یا توصیه شده می‌باشد.(جو و همکاران، ۲۰۱۱)

مدل اعتماد مبتنی بر مدیریت SLA: این مدل یک معماری برای انتخاب سرویس‌دهنده در جهت ارزیابی سرویس‌های‌ابری به منظور کمک به کاربران برای انتخاب بهترین منبع ارائه می‌نماید و از متد نظارت بر فعالیت‌های کسب و کار و تکنیک‌های اعتماد به منظور فراهم کردن مدلی قابل اعتماد برای انتخاب بهترین سرویس مرتبط در بین فراهم‌کنندگان خدمات ابری و تضمین کیفیت این خدمات جهت تأمین نیازمندی‌های کاربران استفاده می‌نماید. اجزای اصلی معماری پیشنهادی شامل موجودیت SLA، جستجوی سرویس ابری، سرویس‌دهنده‌ی ابری و سرویس‌گیرنده‌ی ابری است. از جمله چالش‌های این مدل، عدم تعیین اعتبار بازخوردهای اعتماد به صورت کارآمد می‌باشد.(الحَمَد و همکاران، ۲۰۱۰)

مدل اعتماد بر پایه‌ی شهرت: این مدل به عنوان اوّلین کار علمی به منظور استقرار اعتماد در محیط‌های ابر میانی مطرح است و تمرکز آن بر روی افزایش امنیت سرویس‌های وب می‌باشد. این مدل جهت شناسایی اعتبار بازخوردها، فیلتر کردن بازخوردهای نادرست و دفاع در برابر اطلاعات نادرست با استفاده از اندازه‌گیری شباهت برای محاسبه‌ی اعتبار بازخورد از طریق تجربه‌ی شخصی و متغیّر، تحمل آستانه پیشنهاد می‌دهد که به سرویس‌دهنده‌های ابری کمک می‌کند تا در برابر اطلاعات نادرست از خود دفاع نمایند و انتشار امتیازات نادرست ابری در سطوح مختلف را به حداقل برسانند. همچنین کاهش امتیازات اعتماد با گذر زمان به عنوان یکی از اهداف این مدل می‌باشد. به این صورت که زمانی که هیچ تراکنشی با سرویس‌دهنده در مدت زمان طولانی برقرار نشده باشد، رابطه‌های اعتماد قدیمی‌تر معتبر نمی‌باشد. در این مدل، اعتماد به عنوان یک رابطه‌ی

متقابل بین موجودیت‌ها و مربوط به زمینه‌ای خاص می‌باشد. از جمله چالش‌های این مدل، عدم در دسترس بودن خدمات مدیریت اعتماد و سرویس در مواقع عدم اطلاعات می‌باشد.(زیسیز و لِکّاس، ۲۰۱۲)

مدل اعتماد سلسله مراتبی: این مدل به طور عمده اهمیّت ارزیابی اعتماد رفتار کاربر و استراتژی ارزیابی اعتماد در محاسبات ابری مانند تجزیه و تحلیل اعتماد، قوانین ارزیابی اعتماد رفتار کاربر، ایده‌ی اوّلیه برای ارزیابی رفتار کاربر و استراتژی ارزیابی رفتار اعتماد کاربر برای هر نوع دسترسی را مورد بحث قرار داده است. ایده‌ی اصلی این مدل، تقسیم و ترمیم بر اساس مدل ساختار سلسله مراتبی برای تجزیه رفتار پیچیده‌ی کاربر به زیرمجموعه‌های کوچک اعتماد می‌باشد و سپس این اجزاهای کوچک را به واحدهای داده‌ای کوچکتر تقسیم می‌نماید و سپس از لایه‌های بالایی به سمت لایه‌های پایینی تقسیم‌بندی می‌نماید. این نوع تجزیه و سپس ترکیب می‌تواند عدم قطعیت، ذهنی بودن و ابهام در بررسی اعتماد کاربر در محاسبات ابری را حل نماید. همچنین این مدل، برای رفع مشکل ترکیب عدم توانایی در تخمین وزن مجموعه‌ها و شواهد رفتاری، یک روش ارزیابی و فرایند سلسله مراتبی فازی بر اساس اعداد مثلّثی فازی پیشنهاد نموده است که منجر به نتایج ارزیابی واقعی‌تر می‌شود.(کین و همکاران، ۲۰۱۰)

مدل اعتماد ترکیبی (حالت امن و غیر امن): این مدل، مدلی ساده و کارآمد برای جستجو و اشتراک‌گذاری سرویس بر پایه‌ی اعتماد در محاسبات فراگیر ارائه می‌نماید که در آن دستگاه‌های تلفن همراه قادر خواهند بود ارتباطات خودشان را بدون هیچ گونه پشتیبانی زیرساختی مدیریت کنند. این مدل یک مدل ترکیبی است که برای حالت امن و غیر امن با توجه به سطح نیازهای امنیتی دستگاه‌ها عمل می‌نماید. در این مدل برای محاسبه‌ی اعتماد از اطلاعات تراکنش‌های قدیمی و همچنین توصیه‌ی همسایگان استفاده می‌شود. همچنین در جهت رفع مشکلات عدم اطلاعات اوّلیه، با ارائه‌ی واحد مدیریت ارزیابی ریسک، ریسک مربوط به یک سرویس خاص را تجزیه و تحلیل نموده و اقدامات مناسب را در جهت اشتراک گذاشتن خدمات اتخاذ می‌نماید.(احمد و شارمین، ۲۰۰۸)

مدل اعتماد مبتنی بر مکانیزم اعتماد توصیه‌کنندگان: در این مدل، متقاضی سرویس به طور مستقل سرویس درخواستی خودش را با استفاده از رکوردهای قبلی ذخیره می‌نماید. به علاوه این رکورد در یک دوره زمانی معینی پایدار می‌باشد. بدین صورت از کاهش اعتبار در یک دوره زمانی کوتاه جلوگیری می‌نماید. همچنین در صورت حذف توصیه‌ای، اعتبار آن از طرف توصیه‌کننده کاهش می‌یابد. این مدل قادر خواهد بود از تبانی توصیه‌دهندگان و رفتارهای مخرب جلوگیری نموده و دقت انتخاب سرویس را افزایش داده و سرویس‌دهنده‌ی

مناسبی را برای متقاضی سرویس انتخاب نموده و بدین صورت کیفیت و کارایی سرویس مورد نظر را بهبود بخشد. اعتبار سرویس مورد نظر با معرفی مفاهیمی چون اعتبار توصیه‌دهندگان، اعتبار محتوای سرویس مورد نظر و اعتبار غیرمستقیم پیاده‌سازی می‌شود.(جیا و همکاران، ۲۰۱۰)

مدل اعتماد مبتنی بر شناخت رفتار انسان: این مدل یک مدل ابتکاری بر پایه‌ی شناخت رفتار انسان برای شبکه‌های نظیر به نظیر بر اساس الگوریتم‌های ترکیبی WMA-OWA می‌باشد که در آن عوامل چندگانه‌ای برای منعکس کردن پیچیدگی و عدم قطعیت ویژگی‌های اعتماد در روابط انسانی با هم ترکیب شده‌اند. این مدل برای غلبه بر محدودیت‌های مدل‌های موجود که وزن‌دهی را به طور ذهنی انجام می‌دهند ارائه شده است که وزن‌دهی این عوامل توسط الگوریتم WMA-OWA (ترکیب عملگر OWA و الگوریتم WMA) به صورت پویا انجام می‌شود. این مدل از مؤلفه‌های، شواهد، دانش، مرکز اطلاعات اعتماد، کنترل دسترسی، تابع تصمیم‌گیری اعتماد تشکیل شده است. بنابراین این مدل قادر خواهد بود جهت ارزیابی اعتماد، با جمع‌آوری، تجمیع کردن و توزیع مقدار ارزش اعتماد، بر روی رفتار کاربر نظارت داشته و همچنین در برابر محیط‌های مختلف به صورت کارا عمل نماید.(لی و همکاران، ۲۰۱۱)

مدل اعتماد مبتنی بر باور محلی و باور کل: این مدل بر اساس نظریه‌ی شفر، سیستم شهرتی را پیشنهاد داده است که بر تشخیص و حفاظت از کاربران در برابر نظرات جعلی متمرکز شده است. روش این مدل استفاده از یک الگوریتم اکثریت وزنی به منظور تشخیص باور محلی و باور کل می‌باشد و می‌توان آن را به دیگر کاربران فرستاد. باور کل، ترکیبی از باور محلی و توصیه دریافت شده از هر کاربری می‌باشد.(یو و همکاران، ۲۰۰٤)

مدل کنترل دسترسی مبتنی بر اعتماد متقابل در ابر رایانه: این مدل، ترکیبی از مدیریت اعتماد(TM) و کنترل دسترسی به منابع در محاسبات ابری است. بنابراین اعتماد بین کاربران و ارائه‌دهندگان خدمات ابر را به صورت متقابل بررسی می‌نماید. آزمایشات شبیه‌سازی شده نشان می‌دهند که این مدل می‌تواند با در نظر گرفتن اعتبار گره‌ی خدمات، تعامل بین کاربران و گره‌های سرویس ابری را تضمین نماید. از آنجا که محاسبات ابری یک حالت ارائه‌ی خدمات بر اساس اینترنت است لذا این مدل می‌تواند با ارائه‌ی خدمات مقیاس‌پذیر و ایمن، ویژگی چند مستأجری را به دور از هر گونه عدم اطمینان، ناامنی و ناسازگاری ارائه نماید. در این ویژگی کنترل دسترسی به منابع ابر بسیار حائز اهمیّت است. کنترل دسترسی اوّلیه نه تنها نیازمندی‌های دسترسی طبیعی را برای کاربران معتبر تضمین می‌نماید بلکه از حمله‌ی غیرمجاز کاربران نیز جلوگیری نموده و به این طریق می‌تواند مشکلات امنیتی ناشی از سوء استفاده از کاربران معتبر را حل نماید. این مدل با ارائه‌ی یک الگوریتم

کنترل دسترسی دقیق قابلیت اطمینان و امنیت در طول تعاملات بین کاربر و ارائه‌دهنده‌ی سرویس ابری را همواره مهم می‌شمارد. به جهت اینکه محیط ابر، محیط معمولی توزیع شده است و منابع اطلاعاتی آن ناشناس می‌باشد در نتیجه کنترل دسترسی متمرکز نمی‌تواند نیاز امنیتی محیط ابر را به خوبی برآورده نماید و همواره با یک سری چالش‌ها مواجه خواهد شد، اما ترکیب مدیریت اعتماد با کنترل دسترسی به عنوان یک راه حل مناسب در این حوزه ارائه شده است.(گویان و همکاران، ۲۰۱٤)

-مدل اعتماد مبتنی بر شواهد استدلال(ER): این مدل بر اساس منطق ذهنی است که به عدم قطعیت می‌پردازد و در آن، اعتماد رابطه‌ی بین دو نهاد برای یک بیانیه‌ی خاص بر اساس درجه‌ی باور و عدم اطمینان می‌باشد.(جوسناگ، ۲۰۰۱)؛ رویکرد این مدل مبتنی بر ادراک ارزش اعتماد و اعتبار بر اساس مقدار اعتمادی است که به ترتیب از مشتق ادغام مستقیم و غیرمستقیم شواهد اعتماد برای شناسایی خدمات قابل اعتماد در ابر به دست می‌آید. این مدل، ابعاد شواهد اعتماد به سرویس‌های ابری را از جنبه‌های مختلف در قالب تاریخچه‌ی امتیازات کاربران مورد بررسی قرار می‌دهد و با اعمال جمع رأی اعتماد چند بعدی در واحد زمان، ارزش واقعی اعتماد و قابل‌اعتمادترین سرویس را انتخاب می‌کند. همچنین در این مدل اعتماد محلی به عنوان اعتماد مستقیم از یک فرد و شهرت به عنوان جمع مقدار اعتماد از همه‌ی افراد در نظر گرفته می‌شود.(فان و همکاران، ۲۰۱۵)

-مدل اعتماد بیزی: این مدل یک مدل اعتماد مبتنی بر شبکه است که یک روش انعطاف‌پذیر برای ارائه‌ی اعتماد متفاوت و ترکیب جنبه‌های مختلف اعتماد ارائه می‌نماید.(وانگ و واسیلوا، ۲۰۰۳)؛ این مدل با زمینه‌ی خدمات و زمان، تغییر می‌یابد و ارزش اعتماد بر اساس سوابق تاریخی و عوامل دیگر به روزرسانی می‌شود.
پس از آن نیز شبکه‌ی اعتماد است که یک شبکه‌ی مفهومی است که نشان می‌دهد اعتماد، روابط بین اشخاص است و می‌تواند به صورت یک نمودار غیرمدوّر و مستقیم به تصویر کشیده شود که هر رأس آن یک نهاد و هر لبه، رابطه‌ی بین دو نهاد را نشان می‌دهد. شبکه‌های اعتماد در بسیاری از موارد استفاده شده است از جمله: شبکه‌های ادهاک، تلفن همراه، شبکه‌های حسگر و شبکه‌های اجتماعی.(جوها و همکاران، ۲۰۰٤)

-مدل اعتماد پویا بر اساس مدل زنجیره‌ی مارکوف نیز وجود دارد.(چاندراسکار و همکاران، ۲۰۱۲)؛ همچنین مدل مدیریت اعتماد تطبیقی که ترکیبی از مجموعه‌ی وزن‌هایی برای ارزیابی عملکرد خدمات ابر بر اساس ویژگی‌های متعدد است نیز وجود دارد.(لی و دو، ۲۰۱۳)

4-2. کارهای مربوطه

کارهای زیادی در زمینه‌ی مدل‌های اعتماد انجام شده‌اند، بعضی از آنها بر پایه‌ی توافق، بر پایه‌ی گواهی‌نامه، بر پایه‌ی بازخورد، بر پایه‌ی دامنه و مدل‌های اعتماد سلیقه‌ای می‌باشد، که هر کدام مزایا و معایب خود را دارند. در ادامه به توضیح چند مورد از آنها می‌پردازیم.

۱-٤-۲. مدل مدیریت اعتماد براساس کیفیت سرویس در زیرساخت ابر به عنوان یک سرویس

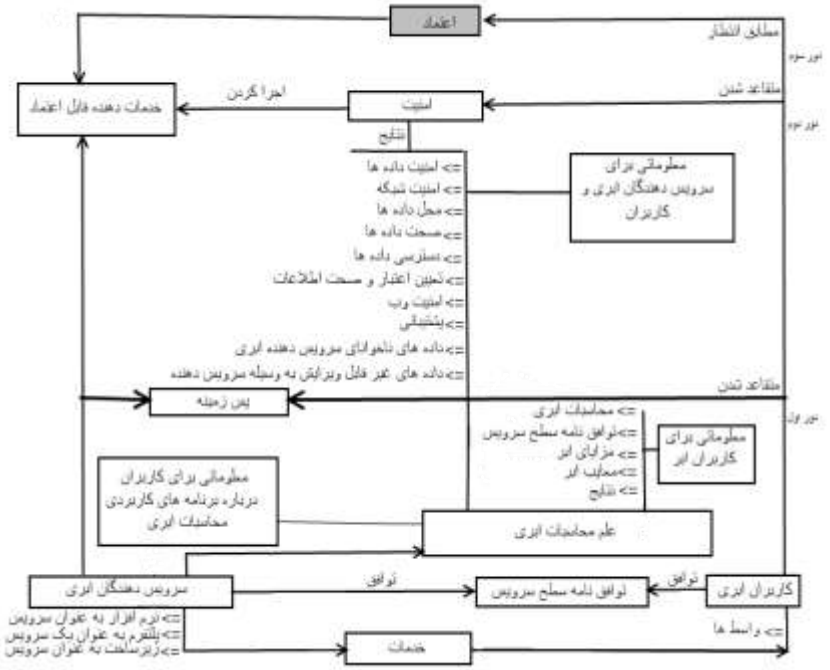
کومار گویال و همکارانش(۲۰۱۲)، یک مدل مدیریت اعتماد بر اساس الگوریتم با هزینه کارآمد، برای افزایش کیفیت سطح سرویس برای پارامترهای زیرساخت ابر به عنوان یک سرویس پیشنهاد کردند. در این مدل، اعتماد بر اساس پارامترهای مرکز داده (زمان آغاز، قیمت، سرعت پردازش، نرخ خرابی، پهنای باند) محاسبه می‌شود که براساس مقادیر اعتماد به دست آمده، مقادیر اعتماد مراکز داده، با دو لیست از مراکز داده‌ی قابل اعتماد و غیرقابل اعتماد ایجاد می‌شود. با استفاده از این لیست‌های قابل اعتماد و غیرقابل اعتماد مراکز داده، زمانبندی صورت می‌گیرد. با استفاده از این زمانبندی، منابع قابل اعتماد به یک کاربر با مقدار اعتماد بیشتر و منابع غیرقابل اعتماد به کاربر غیرقابل اعتماد تخصیص داده می‌شود.

۲-٤-۲. مدل اعتماد بین تأمین‌کنندگان خدمات و کاربران ابر

احمد و همکارانش(۲۰۱۲)، یک مدل اعتماد میان کاربران و تأمین‌کنندگان خدمات ابری پیشنهاد کرده‌اند. این مدل، اعتماد را در سه نوبت برقرار می‌کند و وقتی کاربران ابری در دو نوبت اوّل قانع شدند سپس در نوبت سوّم آنها می‌توانند روی تأمین‌کننده‌ی ابری حساب کنند. در اوّلین نوبت، کاربر باید از تجربه‌ی قبلی با تأمین‌کننده‌ی ابری راضی شده باشد و در نوبت دوّم، کاربر باید درباره‌ی مباحث امنیتی توافق‌های سطح سرویس در سطوح مختلف دانش داشته باشد. کاربر یا سازمان در سوّمین نوبت می‌تواند به تأمین‌کننده‌ی خدمات ابری قابل اطمینان اعتماد کند. در نوبت اوّل، کاربران ابر باید درباره مباحث رایانش ابری، توافق‌های سطح سرویس، مزایای ابر، معایب ابر و مسائل مربوط به رایانش ابری آشنایی داشته باشند و برای هر سازمان لازم است که مزایا و معایب رایانش ابری را درک کند. تأمین‌کنندگان خدمات ابر، سرویس‌های مختلفی را برای کاربران ابر سازمان‌ها بر اساس توافق‌نامه فراهم می‌کنند. این مهم در شکل(۷-۲) نشان داده شده است.

شکل(۷-۲) محیط رایانش ابری

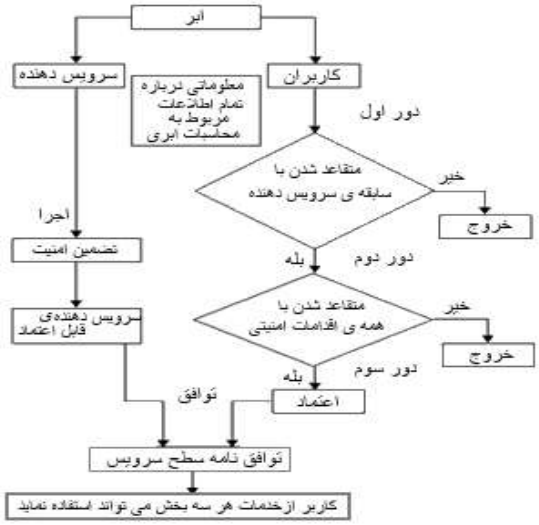
بعد از این که در این مرحله دانشی درباره این مباحث پیدا کردند و قانع شدند،مطابق شکل(۸-۲) در نوبت دوّم چیزی که برای رایانش ابری لازم است پیاده‌سازی امنیت است و موضوع امنیت باید برای کاربران و تأمین‌کنندگان ابر شفاف و روشن باشد. نکته‌ی قابل ملاحظه این است که تأمین‌کنندگان خدمات ابری مسئول اجرا کردن امنیت هستند و کاربران ابر باید دانشی در مباحث امنیت داشته باشند، مسائلی از قبیل: امنیت روی سطح داده، امنیت روی سطح شبکه، محل داده، جامعیت داده، دسترسی داده، امنیت وب، دسترسی‌پذیری و غیره. همچنین کاربران باید دانشی درباره برنامه‌های کاربردی رایانش‌ابری و تأمین‌کنندگان خدمات ابری داشته باشند، که در این زمینه، برنامه‌های کاربردی مختلف قابل دسترس در رایانش ابری شامل Google App Engine ، Google Web Toolkit و ... می‌باشد.



شکل(۸-۲) مدل اعتماد بین تأمین‌کنندگان خدمات و کاربران ابر

در این نوبت کاربران باید با زوایای مختلف امنیت بر اساس آن چه که در بالا توضیح داده شد قانع شده باشند و تمام سیاست‌های امنیت باید به وسیله تأمین‌کنندگان خدمات ابری اجرا شود.

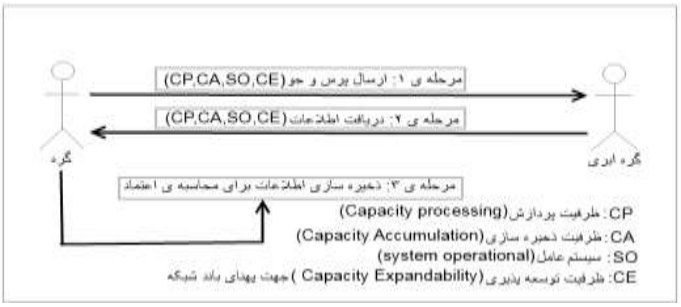
بعد از فهم همه مسائل مربوط به رایانش ابری، کاربران ابر می‌توانند در سه نوبت که در بالا توضیح داده شد به تأمین‌کنندگان خدمات ابری اعتماد کنند، که در فلوچارت شکل(۹-۲) نیز این مراحل به خوبی نشان داده شده است.



شکل(۹-۲) فلوچارت مدل اعتماد بین تأمین‌کنندگان خدمات و کاربران ابر

۳-٤-۲. تبادل فایل‌ها در ابر خصوصی توسط مدل اعتماد

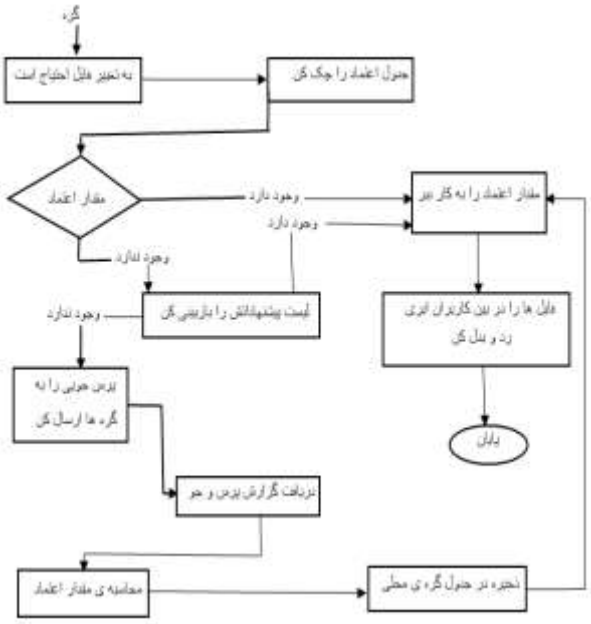
کانیدو و همکارانش(۲۰۱۲)، یک فرایند محاسبه‌ی اعتماد و مدل اعتماد برای تضمین تبادل قابل اطمینان فایل‌ها میان گره‌ها در ابر خصوصی و مطابق با معیارهای توافق شده بر اساس سابقه تعاملات/گزارشات میان گره‌ها، ارائه کرده‌اند. این مقادیر مشابه وزن‌ها در رتبه‌بندی سرویس‌های رایانش ابری به کمک اندازه‌گیری کیفیت و اولویت سرویس‌های ابری هستند و در بازه‌ی [۱-۰] قرار دارند. مطابق شکل(۲-۱۰)، ارزیابی اعتماد بر مبنای سیستم‌عامل، فضای ذخیره‌سازی گره، پهنای باند شبکه و ظرفیت پردازش است. شبیه‌سازی‌ها با استفاده از چارچوب کلودسیم انجام می‌شود تا کارایی مدل در انتخاب گره‌ی قابل اطمینان‌تر در ابر خصوصی را نشان دهد. مدل با وزن‌های پارامترهای توافق‌نامه‌ی سطح سرویس و دیگر شاخص‌های کارایی، امکان ارزیابی دقیق‌تر را فراهم کرده است.



شکل(۱۰-۲) سناریوی درخواست اطلاعات

شکل(۱۰-۲) سناریوی درخواست اطلاعات را نشان می‌دهد. سپس مقدار عددی اعتماد بر اساس مدل اعتمادی که توضیح داده شد، محاسبه می‌شود و گره درخواست شده به مقدار عددی اعتماد بزرگتر، به گره‌ای که گنجایش ذخیره‌سازی و پردازش آن بزرگتر و پهنای باند شبکه آن بهتر است اختصاص داده می‌شود و در نهایت تبادل بین گره‌ها انجام می‌شود.

در این مدل اعتماد، هر گره دو جدول اعتماد دارد که عبارتند از: جدول اعتماد مستقیم و لیست توصیه شده. فرض می‌کنیم که گره‌ای به تبادل فایل‌ها و محاسبه‌ی مقدار عددی اعتماد گره دیگر نیاز دارد، ابتدا جدول اعتماد را بررسی کرده و از مقدار عددی اعتماد استفاده می‌کند. البته در صورتی که این مقدار وجود داشته باشد و در غیر این صورت اگر مقدار آن قابل دسترس نباشد، گره درخواست‌کننده، لیست توصیه‌شده را بررسی می‌کند، برای این که گره‌ای را پیدا کند که ارتباط اعتماد مستقیم با گره خواسته شده دارد و مقدار عددی اعتماد این گره از جدول اعتماد مستقیم مورد استفاده قرار می‌گیرد و اگر مقداری وجود نداشته باشد یک پرس‌وجو را بر اساس اطلاعات درخواستی گره، فضای ذخیره‌سازی گره، سیستم عامل، پهنای باند شبکه و ظرفیت پردازش ارسال می‌کند. شکل(۱۱-۲) مراحل این مدل را به خوبی نشان می‌دهد.



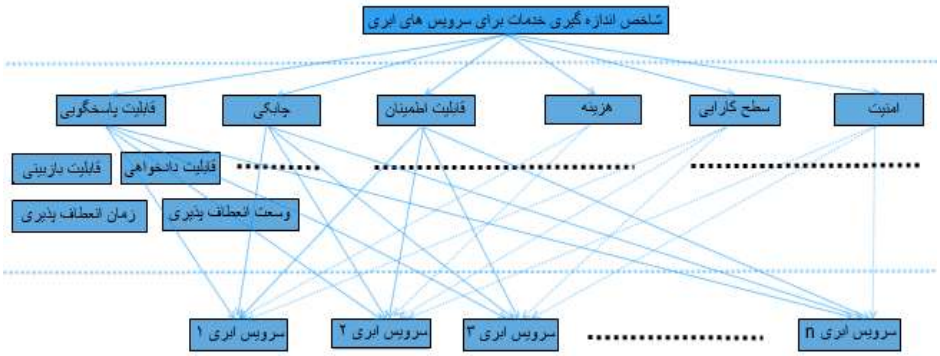
شکل(۱۱-۲) فلوچارت مدل اعتماد سطح بالا

مطابق شکل(۱۱-۲) عملکرد مدل اعتماد پیشنهاد شده به این صورت است که: گره A درخواستی را به گره‌های ابر ارسال می‌کند (مانند گره B) و به این طریق، فضای ذخیره‌سازی گره‌ها، سیستم عامل، پهنای باند شبکه و ظرفیت پردازش گره‌ها را درخواست می‌کند و گره‌ها که شامل گره B نیز هست، پاسخ اطلاعات درخواست شده را می‌فرستند. گره A، اطلاعات دریافت شده از گره B و همه گره‌ها را ارزیابی می‌کند. اگر اطلاعات فراهم شده به وسیله‌ی گره B، بر اساس آن چه که انتظار داشتیم با مقدار میانگین گره‌های دیگر که در جدول توصیه شده‌ی محلی گره A بعد از محاسبه‌ی اعتماد ذخیره شده است سازگار باشد، در جدول اعتماد محلی ذخیره می‌شود.

۴-۴-۲. چارچوبی برای رتبه‌بندی سرویس‌های رایانش ابری

کومار گارگ و همکارانش(۲۰۱۳)، چارچوبی را برای اندازه‌گیری کیفیت و اولویت سرویس‌های ابر پیشنهاد کرده‌اند. این چارچوب اثر قابل توجه و رقابت سالم در میان تأمین‌کنندگان خدمات ابر برای برآورده کردن توافق سطح سرویس و بهبود کیفیت سرویس آنها دارد. آنها فرآیند تحلیل سلسله مراتبی(ساتی، ۲۰۰۵) بر پایه‌ی مکانیزم رتبه‌بندی پیشنهاد کردند که سرویس‌های ابری را بر اساس برنامه‌های کاربردی مختلف مربوط به نیازمندی‌های کیفیت سرویس می‌تواند ارزیابی نماید. مطابق شکل(۱۲-۲)، این روش پیشنهادی فقط برای مشخصه‌های قابل اندازه‌گیری کیفیت سرویس مانند پاسخگویی، مهارت، اطمینان از سرویس، هزینه، کارایی،

امنیت، حریم خصوصی و قابلیت استفاده به کار گرفته می‌شود و فرآیند تحلیل سلسله مراتبی آن شامل سه لایه می‌باشد.



شکل(۱۲-۲) سلسله مراتب فرآیند تحلیل سلسله مراتبی برای رایانش ابری

همانطور که در شکل(۱۲-۲) دیده می‌شود، لایه‌ی اوّل که همان هدف است شاخص اندازه‌گیری سرویس را برای سرویس ابر ارائه می‌کند. ویژگی شاخص اندازه‌گیری سرویس بر پایه‌ی سازمان ملّی، برای استانداردسازی به وسیله انجمن طراحی شده است که از یک مجموعه نشانگرهای کلیدی عملکرد مربوط به تجارت، تشکیل شده است و روش استانداردی برای اندازه‌گیری و مقایسه سرویس‌های تجاری را فراهم می‌نماید. چارچوب شاخص اندازه‌گیری سرویس یک دید کلّی از کیفیت سرویس مطلوب توسط مشتری برای انتخاب تأمین‌کننده‌ی سرویس ابر بر اساس پاسخگویی، مهارت، اطمینان از سرویس، هزینه، کارایی، امنیت، حریم خصوصی و قابلیت استفاده فراهم می‌کند. لایه‌ی دوّم که همان معیارها است در فاز دوّم شامل دو بخش می‌باشد: مقایسه‌ی جفتی از مشخصه‌های کیفیت سرویس برای تعیین اولویت آنها انجام می‌شود(مقایسه‌ی زوجی معیارها بر اساس هدف) و مقایسه‌ی جفتی از سرویس‌های ابر بر اساس مشخصه‌های کیفیت سرویس آنها برای محاسبه‌ی رتبه‌ی محلّی آنها(مقایسه زوجی کاندیدها بر اساس معیارها). در فاز انتها برای هر سرویس، رتبه‌ی محلّی نسبی همه معیارها با هم جمع می‌شود تا مقادیر رتبه‌ی کلّی برای همه سرویس‌ها را تولید کند، آنگاه بر اساس مقدار اولویت به دست آمده مناسبترین سرویس ابر انتخاب می‌شود.

۵-٤-۲. مدل اعتماد برای انتخاب تأمین‌کننده‌ی سرویس ابر

دکتر ظفر و همکارانش(۲۰۱٤)، یک مدلی را پیشنهاد کردند که به کاربران سرویس ابر، در پیدا کردن تأمین‌کنندگان سرویس ابر قابل اعتماد و کارآمد، بر مبنای داده‌های گرفته شده از مسئولان قانونگذار و عملکرد تأمین‌کنندگان سرویس ابر در یک سال گذشته و بازخوردهای گرفته شده از مشتریان کمک می‌کند. انتخابی را

برای کاربر، به منظور ارزیابی ارائه‌دهنده‌ی سرویس‌های متنوع و موجود بر اساس شهرتشان در بازار، بر اساس کیفیت سرویس ارائه شده‌شان فراهم می‌کند و قابل اعتمادترین ارائه‌دهنده‌ی سرویس را انتخاب می‌کند.
همان طور که در شکل(۱۳-۲) قابل مشاهده است، اصلی‌ترین ویژگی‌هایی که در این مدل روی آن متمرکز شده‌اند، مدت زمان از کارافتادگی (غیرفعال بودن)، زمان فعال بودن، پشتیبانی از مشتری، تکرار به روزرسانی برنامه‌ها و قابلیت تحمل خطا می‌باشند، که این گزینه‌ها را در اختیار مشتری قرار داده تا بر اساس نیازهایش، تأمین‌کننده‌ی سرویس ابر را انتخاب کند.

شکل(۱۳-۲) پنجره‌ی اصلی از برنامه‌ی کاربردی توسعه یافته برای مدل گفته شده در C#

بعد از محاسبه‌ی این پارامترها، در انتها وزن‌هایی را به تمام این پنج پارامتر که یک کاربر می‌تواند بر طبق نیازش تغییر دهد، اضافه کردند. برای مثال، اگر یک مشتری، علاقه‌ی بیشتری به تجربه‌ی پشتیبانی از مشتری داشته باشد، آنگاه مشتری/ کاربر، می‌تواند وزن‌های تخصیص یافته برای آن پارامتر را تغییر دهد و هر چه وزن تخصیص یافته بالاتر باشد، نقش آن پارامتر خاص در انتخاب ارائه‌دهنده‌ی سرویس ابر، بیشتر خواهد بود. فرمول زیر گواه این موضوع است. طبق این فرمول، ارائه‌دهنده‌ی سرویس ابر، با بالاترین مقدار برای سرویس ابر انتخاب خواهد شد.

$$\text{مقدار کل} = J * DT + K * UT + L * FTC + M * CSE + N * AUF \qquad (۲-۱)$$

که مقدار J و K و L و M و Nدر محدوده ۱ تا ۱۰ قرار می‌گیرد. اما انتخاب مقدار آنها برای کاربران بر طبق اولویت‌هایشان است. در اینجا، برخی از کاربران سرویس ابر، نوعی را و برخی دیگر از آنها، نوع دیگر را ترجیح می‌دهند. از این رو، هر کدام، اهمیّت خودش را با توجه به دستورالعمل اجرایش دارد. تفسیر ویژگی‌های مورد نظر به صورت زیر است:

زمان از کارافتادگی: زمانی است که سرویس‌ها برای کاربر سرویس، در دسترس نباشد. یعنی طول زمانی است که خدمات در دسترس نمی‌باشد (کاربران ابر نمی‌توانند به ابر دسترسی یابند). این زمان باید به حداقل برسد و اگر نیازی به ارائه‌دهنده‌ی سرویس ابر برای پایین آوردن سیستم برای ارتقا، تعمیر یا نگهداری به وجود آید، آنگاه باید ترجیحاً از پیش برنامه‌ریزی شود.

زمان فعال بودن(مدت در حال کار): زمانی از سال است که سرویس‌های ارائه‌دهنده‌ی سرویس ابر، برای کاربران در دسترس باشد (زمان فعال بودن، به وضوح بیشترین زمان را هنگامی که خدمات در دسترس باشند تعریف می‌کند). اعتمادکننده، سرویس‌دهنده‌ای را ترجیح می‌دهد که بهترین زمان فعال بودن را در آن سال با توجه به دسترس‌پذیری مؤثر برای کاربران ارائه دهد.

پشتیبانی از مشتری: زمانی که مشتری به خدمات، حمایت یا کمک از ارائه‌دهنده‌ی سرویس نیاز دارد، آنگاه باید روش مناسبی برای برطرف کردن مشکل مشتری برای جلب رضایت وی ارائه گردد.

عملکرد سرویس خاص: اگر سازمان، سرویس‌های مربوط به هر گونه سرویس خاصی را فراهم می‌کند، آنگاه به طور کلّی در بازار برای آن سرویس معروف می‌شود. بنابراین، انتخاب آن ارائه‌دهنده‌ی سرویس، به طور کلّی ترجیح داده می‌شود.

به روزرسانی برنامه: وقوع خطا می‌تواند در هر خدمات شبکه‌ای که دستگاه‌های متعددی دائماً با یکدیگر کار می‌کنند اتفاق بیفتد، امّا تمام ارائه‌دهندگان سرویس باید برنامه‌های پشتیبان خود را داشته باشند یا انبارهای باتری یا ژنراتورهایی برای پشتیبانی نیرو و اتصال داده‌ها با سرورهای آنلاین دیگر برای پشتیبانی داده‌ها فراهم نمایند. بنابراین، ارائه‌دهنده‌ی سرویسی با برنامه‌های نیروی جایگزین و تسهیلات پشتیبانی را باید انتخاب نمود.

قابلیت تحمل خطا: انواع بسیاری از خطاها وجود دارد که یک سیستم می‌تواند با آن مواجه شود. گاهی اوقات، این خطاها می‌توانند مستقیماً بر سرویس‌هایی تأثیر بگذارد که ارائه‌دهنده‌ی سرویس ابر فراهم می‌کند.

زمان پاسخ: یک ارائه‌دهنده‌ی سرویس ابر که حداقل زمان را در پاسخ به شکایات، درخواست یا پرسش دارد، برای آن انتخاب، به عنوان سازمان ارائه‌دهنده‌ی سرویس ابر، ترجیح داده می‌شود.

مدل مطرح شده، شامل اولویت بالا برای ارائه‌دهنده‌ی سرویسی است که تاریخچه‌ی (سابقه) زمان از کار افتادگی حداقل را در طول یک سال گذشته دارد. بنابراین، تأمین‌کننده‌ی سرویس ابر با زمان از کار افتادگی حداقل، باید انتخاب شود. کارایی هر ارائه‌دهنده‌ی سرویس ابر را می‌توان از زمان فعال بودنش تعیین نمود. بنابراین یک تأمین‌کننده‌ی سرویس ابر با کارایی خوب را باید انتخاب کرد. مقدار تجربه‌ی حمایت از مشتری

برای وی اهمیّت زیادی دارد تا به ارائه‌دهنده‌ی سرویس ابر اعتماد کند. یک ارائه‌دهنده‌ی سرویس ابر با بالاترین رده‌بندی در حمایت از مشتری را باید انتخاب نمود.

٦-٤-٢. مدل اعتماد بر اساس معیارهای کیفیت سطح سرویس

پائول مانوئل و همکارانش(٢٠١٣)، یک مدل اعتماد بر اساس گواهینامه‌های قبلی و قابلیت‌های کنونی تأمین‌کنندگان سرویس ابری پیشنهاد داده و آن را مدل اعتماد کیفیت سطح سرویس نامگذاری کردند.

در این مدل مقدار اعتماد با استفاده از چهار پارامتر: دسترسی‌پذیری، قابلیت اطمینان، یکپارچگی داده‌ها و کارایی زمان پاسخ محاسبه شده است. پیاده‌سازی این مدل با استفاده از سیستم مدیریت اعتماد است. میزان کیفیت اعتماد سطح سرویس(QT) بر اساس فرمول زیر به دست می‌آید:

$$\mathrm{QT} = w_1 * \mathrm{AV} + \mathrm{w_2} * \mathrm{RE} + \mathrm{w_3} * \mathrm{DI} + \mathrm{w_4} * \mathrm{TE} \qquad (٢-٢)$$

که در آن w_1، w_2، w_3 و w_4 وزن‌های هر پارامتر می‌باشند و مقدار هر کدام بر اساس اولویت آن مشخص می‌شود. به طوری که: $w_1 + w_2 + w_3 + w_4 = 1$

در این فرمول، AV بیانگر دسترسی‌پذیری، RE بیانگر قابلیت اطمینان، DI یکپارچگی داده و TE کارایی زمان پاسخ می‌باشد که در ادامه، هر کدام از آنها را به صورت جداگانه محاسبه می‌نماییم.

دسترسی‌پذیری: درجه‌ای است که یک سرویس هنگامی که جهت استفاده مورد نیاز است، قابل استفاده و دست یافتنی باشد. بنابراین، منابع در یکی از وضعیت‌های زیر غیر قابل‌دسترس نامیده می‌شوند:

١- قسمتی از سرویس منبع غیر قابل‌دسترس برای کاربر باشد.
٢- منابع غیر فعال(خاموش) باشند.
٣- منبع برای پردازش تقاضا بسیار مشغول باشد.

فرض کنیم که $\{\mathrm{R_1}, \mathrm{R_2}, \dots, \mathrm{R_n}\}$ منابع ابری باشند، برای هر $\mathrm{k} = 1,2, \dots, n$، N_k به عنوان تعداد کارهای ثبت شده و A_k تعداد کار پذیرفته شده برای منبع ابری R_k در محدوده زمانی T می‌باشد. در این صورت میزان دسترس‌پذیری طبق رابطه‌ی زیر به دست می‌آید:

$$\text{Availability (AV)}\mathrm{R_k} = \frac{\mathrm{A_k}}{\mathrm{N_k}} \qquad (٢-٣)$$

قابلیت اطمینان: قابلیت اطمینان جزء مهمی از اعتماد است که نرخ موفقیت نیز نامیده می‌شود.(گوپتا و همکاران، ۲۰۱۳)؛ قابلیت اطمینان یک منبع ابری، یک مقیاس از انجام موفقیت‌آمیز کار پذیرفته شده توسط منبع ابری می‌باشد. اگر A_k تعداد کار پذیرفته شده توسط منبع R_k و C_k تعداد کار تکمیل شده موفق توسط منبع R_k در محدوده زمانی T باشد، در این صورت قابلیت اطمینان طبق رابطه‌ی زیر به دست می‌آید:

$$\text{Reliability (RE)} R_k = \frac{C_k}{A_k} \qquad (۲-٤)$$

یکپارچگی داده: یکپارچگی داده‌ها اصطلاح گسترده است و شامل امنیت، پوشیدگی و دقت داده‌ها می‌باشد که در آن، امنیت شامل داده‌های امن و پوشیدگی شامل درستی داده‌ها است.(پیرسون، ۲۰۱۳)؛ اگر C_k تعداد کار تکمیل شده موفق توسط منبع R_k و D_k تعداد کارهای یکپارچگی داده‌ای ارائه شده توسط منبع R_k در محدوده زمانی T باشد، در این صورت یکپارچگی داده طبق رابطه زیر به دست می‌آید:

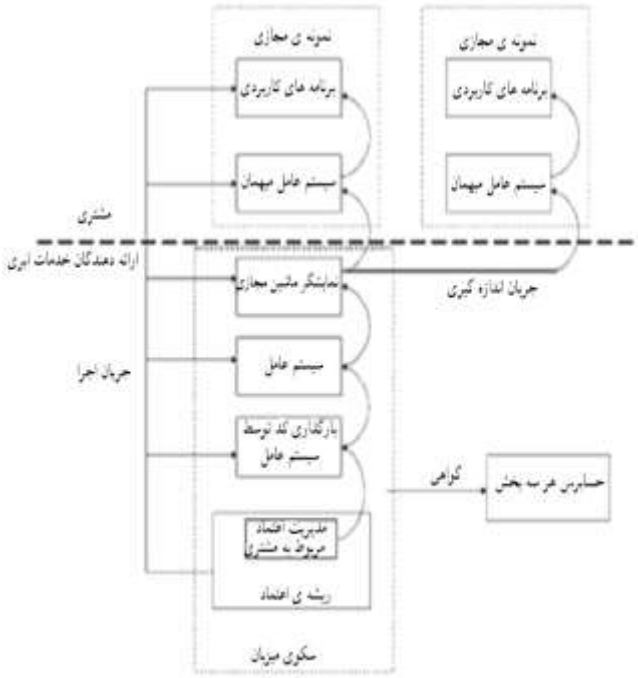
$$\text{Data Integrity (DI)} R_k = \frac{D_k}{C_k} \qquad (۲-٥)$$

کارایی زمان پاسخ: زمان پاسخ واقعی، زمان دقیق بین زمان درخواست کار (t_1) و زمان تحویل کار انجام شده به کاربر (t_2) می‌باشد. بنابراین، کارایی زمان پاسخ برابر است با:

$$\text{Turnaround Efficiency (TE)} = t_2 - t_1 \qquad (۲-٦)$$

2-4-7. معماری مدل چند کاربره قابل اعتماد محاسباتی در ابر

لی و همکارانش(۲۰۱۰)، همان طور که در شکل(2-14) قابل مشاهده می‌باشد، یک مدل چند کاربره قابل اعتماد محاسباتی معرفی کرده است. در این مدل، تأمین‌کننده‌ی سرویس ابر و کاربران با هم همکاری می‌کنند تا یک محیط محاسباتی ابری قابل اعتماد ایجاد و از آن نگهداری کنند.



شکل(2-14) مدل چند کاربره‌ی قابل اعتماد محاسباتی

این مدل با هدف تضمین یک محیط محاسباتی ابری قابل اطمینان به کاربران برای لایه IaaS طراحی شده بود و همان گونه که در شکل(۱٤-۲) مشاهده می‌شود دارای دو سطح سلسله مراتبی در مدل اعتماد متغیّر (غیرمستقیم) است که از جداسازی توجه بین کارایی و امنیت پشتیبانی می‌کند. همچنین این مدل دارای سه جریان هویتی است:

الف) مصرف‌کنندگان، که سرویس‌های محاسباتی ابر تأمین‌کننده‌ی سرویس ابر را اجاره می‌کنند.

ب) تأمین‌کننده‌ی سرویس ابر، که سرویس IaaS را تأمین می‌کند.

ج) حسابرس(اختیاری) توصیه می‌شود، که از طرف کاربر مسئول تأیید کردن این مطلب است که آیا زیرساخت تأمین شده توسط تأمین‌کننده‌ی سرویس ابر قابل اعتماد است.

۸-٤-۲. مدل اعتماد مشترک برای فایروال‌ها در رایانش ابری

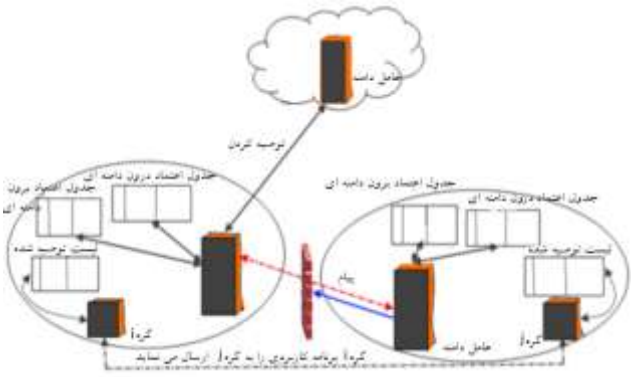
ژیمین و همکارانش(۲۰۱۰)، برای فایروال‌ها در رایانش ابری، یک مدل اعتماد اشتراکی پیشنهاد کردند. این مدل سه مزیت دارد:

۱) برای دامنه‌های مختلف از سیاست‌های امنیتی مختلفی استفاده می‌کند.

۲) این مدل ماهیت تراکنش‌ها، داده‌های قدیمی موجودیت‌ها و اثر آنها در اندازه‌گیری پویای مقدار اعتماد را در نظر می‌گیرد.

۳) این مدل اعتماد با فایروال سازگار است و سیاست‌های کنترل محلی آن را نقض نمی‌کند.

در این مدل، از یک مدل اعتماد در سطح دامنه استفاده می‌شود. اعتماد به صورت مقدار عددی برای اعتماد محاسبه می‌شود که به ماهیت موجودیت‌ها، رفتار گذشته و... بستگی دارد و مقدار آن ثابت نمی‌باشد. ابر، به تعدادی دامنه مستقل تقسیم می‌شود و روابط اعتماد بین گره‌ها، به دو دسته‌ی روابط اعتماد درون دامنه‌ای و برون دامنه‌ای تقسیم می‌شود. روابط اعتماد برون دامنه‌ای بر اساس تراکنش‌های عمل شده داخل دامنه‌ای هستند.



شکل(۱۵-۲) ساختار مدل اعتماد مشترک برای فایروال‌ها در رایانش ابری

مطابق شکل(۱۵-۲)، هر گره دو جدول دارد که عبارتند از: یک جدول اعتماد مستقیم و یک لیست توصیه شده. اگر یک گره نیاز داشته باشد که مقدار اعتماد یک گره دیگر را محاسبه کند، ابتدا جدول اعتماد مستقیم را بررسی می‌کند و اگر مقدار متناظر با گره مورد نظر موجود باشد، مقدار آن را به کار می‌گیرد، در غیر این صورت، اگر مقدار به صورت محلی موجود نباشد، گره درخواست‌کننده، لیست توصیه شده‌ها را بررسی می‌کند تا گره‌ای را مشخص کند که جدول اعتماد مستقیم آن شامل گره مورد نظر است. سپس، جدول اعتماد مستقیم گره توصیه‌شده را برای یافتن مقدار اعتماد گره مورد نظر بررسی می‌کند. این پروسه ادامه می‌یابد تا یک مقدار اعتماد برای گره مورد نظر در جدول اعتماد مستقیم یک گره یافت شود. مقادیر اعتماد درون دامنه‌ای بر اساس تراکنش‌های بین گره‌های درون دامنه‌ای محاسبه می‌شوند، مقدار اعتماد درون دامنه‌ای یک مقدار سراسری از مقادیر اعتماد مستقیم گره‌ها و مقدار اعتماد توصیه شده از سایر دامنه‌ها است. دو جدول در عامل دامنه که در هر دامنه ایجاد شده است نگهداری می‌شوند، که شامل فرم روابط اعتماد درون دامنه‌ای و جدول مقدار وزن گره‌های این دامنه است.

۹-٤-۲. مدل ارزیابی اعتماد برای رایانش ابری

ژئونیان ووآ و همکارانش(۲۰۱۳)، برای رایانش ابری یک مدل ارزیابی اعتماد مبتنی بر تئوری استناد D-S و پنجره‌های لغزان ارائه داده‌اند. در این مدل، محدودیت زمانی مستندات تعامل به عنوان یک مدرک درجه یک، با معرفی مفهوم پنجره‌های لغزان انعکاس داده شده است. اعتماد مستقیم هویت‌ها بر اساس مستندات تعامل توسط تئوری استناد D-S محاسبه می‌گردد. تضاد موجود در اعتماد توصیه شده به عنوان یک مدرک درجه دو با کمک یک دیدگاه ترکیبی ارتقاء یافته است تا جایی که ممکن است برطرف می‌شود. در پایان، ترکیب اعتماد توصیه شده اعتبار هویت‌ها را نشان می‌دهد. نتایج آزمایشی نشان می‌دهد که مدل پیشنهاد شده مؤثر و قابل گسترش است. مدل پیشنهادی آنها، دارای چندین مزیت به قرار زیر است:

اوّلاً، اجرای آن ساده است. دوّماً، زمان‌دار بودن تعامل با معرفی پنجره‌های لغزان اعمال شده است. در مکانیزم پنجره‌ی لغزان، تعاملات به دو دسته‌ی تعاملات معتبر و نامعتبر تقسیم می‌شوند. تنها تعاملات معتبر هستند که می‌توانند بر روی درجه‌ی اعتماد یک هویت تأثیر بگذارند. بنابراین، این روش قابلیت گسترش دادن سیستم را تقویت می‌کند. سوّماً، درجه‌ی اعتماد هویت‌ها به صورت پویا بر اساس رفتار هویت و بر اساس تئوری استناد D-S تغییر می‌کند. با این وجود، مقوله‌ی اعتماد، هم برای تأمین‌کننده‌ی سرویس ابر و هم برای کاربر ابر محاسبه شده و یک حفاظت امنیتی برای تأمین‌کنندگان سرویس ابر و کاربران ابر به وجود می‌آید. در نهایت، این کار می‌تواند به سیستم در یافتن هویت‌های جعلی تا حدودی کمک کند و نرخ موفقیت تعاملات را افزایش دهد. این کار مقاومت سیستم در برابر حملات را تقویت می‌کند.

۱۰-٤-۲. چهارچوب امن روی رایانش ابری

ژو کای و همکارانش(۲۰۱۰)، چارچوب "اعتماد به عنوان یک سرویس" برای اصلاح روش‌های مدیریت اعتماد در محیط ابری ارائه شده است. این مدل قابل قبول انطباقی، میان بازخوردهای اعتماد معتبر و بازخوردهای مغرضانه، به وسیله‌ی مورد توجه قرار دادن توانایی مشتریان سرویس ابری و اجتماع اکثریت بازخوردها، تفاوت می‌گذارد. به علاوه، سیستم مدیریت انتقال به ارزیابی بازخورد اعتماد و حافظه‌ی ذخیره‌سازی، اجازه‌ی مدیریت شدن در یک روش توزیع شده را می‌دهد. روش‌ها به وسیله‌ی سیستم نمونه‌ی اوّلیه و نتایج آزمایشگاهی اثبات شده‌اند.

۱۱-٤-۲. روش رایانش ابری بر اساس پلتفرم قابل اطمینان محاسباتی

ژیونگ شن و همکارانش(۲۰۱۰)، به محتوای تراکنش، داده‌ی تاریخی موجودیت‌ها و تأثیرات آنها در اندازه‌گیری پویای مقدار اعتماد توجه می‌کند.

شکل(۱۶-۲) معماری رایانش ابری بر اساس TCP

در این مدل، اعتماد توسط یک مقدار اعتماد در مفهوم موجودیت و رفتار تاریخی اندازه‌گیری می‌شود و ثابت نیست. مطابق شکل(۱۶-۲)، پلتفرم قابل اطمینان محاسباتی TCP، طرحی برای ایجاد قابلیت اعتماد ارائه کرده است که به منظور احراز هویت، محرمانه بودن و جامعیت استفاده می‌شود. این طرح نتایج مثبتی برای احراز هویت، دسترسی مبتنی بر قانون و محافظت داده را در محیط محاسبات ابری به نمایش می‌گذارد.(بل، ۲۰۱۲)

۵-۲. نتیجه‌گیری

اگر چه اعتماد، برآورد توانایی منبع ابر در کامل کردن یک کار در محیط ابری بر اساس اعتبار، هویت و دسترس‌پذیری است اما اغلب کاربران، به دلیل عدم اطلاعات ناکافی جهت تصمیم‌گیری درباره‌ی انتخاب سرویس در محیط ابری، با چالش‌های اساسی مواجه هستند. بنابراین اگر آنها به نحوی قادر به محاسبه‌ی قابل اعتماد بودن سرویس‌دهنده‌ی خود، از میان سرویس‌دهندگان مختلف با قابلیت‌های یکسان باشند، قادر خواهند بود تا خدماتی را که بهترین مطابقت با نیازهایشان دارد انتخاب نموده و استفاده نمایند. از طرفی دیگر سیاست‌های مورد استفاده در روش انتخاب سرویس، به سرویس‌دهندگان، برای ایجاد سرویسی هوشمندتر و کارآمدتر کمک می‌کند تا به بهترین وجه نیازهای کسب و کار کاربران را برطرف کنند و خدماتی را که بهترین مطابقت با نیازهای کاربران دارد ارائه دهند، که این امر مستلزم استفاده از مدل ها و چارچوب‌هایی برای جستجوی خدمات مناسب و در دسترس بر روی محاسبات ابری است. در حال حاضر مدل‌های اعتماد گسترده‌ای در رایانش ابری وجود دارند که هر

مدل امکانات مختلفی را پشتیبانی می‌کند و سرویس‌های ابری را بر اساس پارامترها و نیازمندی‌های مختلفی ارزشیابی می‌نماید. با این وجود، برای یک شرکت یا هر نهاد علاقه‌مند، مشکل است که مدلی از اعتماد را انتخاب و پیاده‌سازی نماید که به بهترین شکل، نیازمندی‌هایش را برآورده سازد، به این دلیل که این مدل‌ها نیز با خود چالش‌هایی را به همراه دارند که قابلیت اعتماد را تحت تأثیر قرار می‌دهند.

کلمات کلیدی فصل دوّم

Cloud Service Provider (CSP)	تأمین‌کننده‌ی خدمات ابری
Service Level Agreement (SLA)	توافقنامه‌ی سطح سرویس
Infrastructure as a Service (IaaS)	زیرساخت به عنوان یک سرویس
Random-Access Memory (RAM)	حافظه‌ی دستیابی تصادفی
Ordered Weighted Averaging (OWA)	عملگر OWA
Weighted Majority Algoritm (WMA)	الگوریتم WMA
Trust Management (TM)	مدیریت اعتماد
Evidential Reasoning (ER)	مبتنی بر شواهد استدلال
Trust Value	مقدار عددی اعتماد
Recommendation List	لیست توصیه‌شده
Quality Of Service (QOS)	کیفیت سطح سرویس
Service Measurement Index	شاخص اندازه‌گیری سرویس
Key Performance Indicators	نشانگرهای کلیدی عملکرد
Down Time (DT)	مدت زمان از کارافتادگی
Up Time (UT)	زمان فعال بودن
Customer Support Experience (CSE)	پشتیبانی از مشتری
Application Update Frequency (AUF)	تکرار به روزرسانی برنامه‌ها
Fault Tolerance Capability (FTC)	قابلیت تحمل خطا
Quality of service Trust model (QT)	کیفیت اعتماد سطح سرویس
Availability (AV)	دسترسی‌پذیری
Reliability (RE)	قابلیت اطمینان

Data Interity (DI)	یکپارچگی داده
Tumaround Efficiency (TE)	کارایی زمان پاسخ
Multi-tenant Trusted Computing Environment Model	مدل چند کاربره قابل اعتماد محاسباتی
Domain Agent	عامل دامنه
Transportation Management Systems (TCP)	سیستم مدیریت انتقال

فصل سوّم:

روش تحقیق

از آنجا که اعتماد، یک مفهوم مبهم و پویا است، اغلب در طول زمان و یا با تغییرات محیطی تغییر می‌یابد، ارزیابی اعتماد بر پایه‌ی به حداکثر رساندن رضایتمندی از همکاری کاربر و ارائه‌دهنده‌ی خدمات‌ابری است که این مقدار را می‌توان با یک سیستم استنتاج‌فازی و قوانین پایه به دست آورد.
بنابراین، در این پژوهش از سیستم‌های استنتاج فازی بهره می‌گیریم. اگر بخواهیم نظریه‌ی مجموعه‌های فازی را تعریف کنیم باید بگوییم که این نظریه قادر است بسیاری از مفاهیم و متغیّرها و سیستم‌هایی را که نادقیق هستند، صورت‌بندی ریاضی ببخشد و زمینه را برای استدلال، استنتاج، کنترل و تصمیم‌گیری در شرایط عدم اطمینان فراهم آورد. جهت انجام این پژوهش مراحل زیر را دنبال می‌نماییم:

۳-۱. شناسایی سیستم فازی مورد استفاده

انواع سیستم‌های فازی به صورت زیر است:

- ✓ سیستم‌های فازی خالص: مشکل این سیستم‌ها این است که ورودی‌ها و خروجی‌های آن، مجموعه‌های فازی می‌باشند. در حالی که در سیستم‌های مهندسی، ورودی‌ها و خروجی‌ها، متغیرهایی با مقادیر حقیقی می‌باشند.
- ✓ سیستم فازی تاکاگی‌سوگنو و کانگ: این سیستم دست ما را برای اعمال اصول مختلف منطق‌فازی باز نخواهد گذاشت و در نتیجه انعطاف‌پذیری سیستم‌های فازی در این ساختار وجود ندارد.
- ✓ سیستم‌های فازی با فازی‌ساز و غیرفازی‌ساز: این سیستم فازی، معایب سیستم فازی خالص و سیستم فازی تاکاگی‌سوگنو و کانگ را می‌پوشاند.(مهران،۱۳۹۰)؛ در این مبحث از این پس سیستم فازی‌ساز و غیرفازی‌ساز را سیستم فازی عنوان می‌نماییم و در این پژوهش از این سیستم جهت ارزیابی اعتماد استفاده می‌نماییم.

۳-۲. تعیین معیارها

از آنجا که در این پژوهش، ملاک افزایش اعتماد کاربران رایانش ابری در گرو امنیت است لذا ابعاد ارزیابی اعتماد در رایانش ابری را طبق آنچه در بخش‌های قبل گفته شد به دو صورت زیر در نظر می‌گیریم:

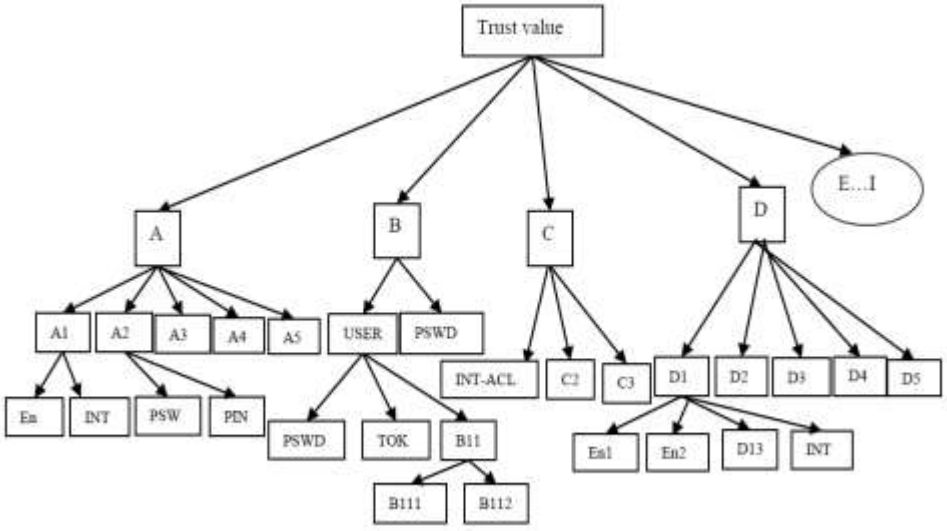
- ارزیابی اعتماد امنیت‌گرا
- ارزیابی اعتماد غیرامنیت‌گرا.

جهت استفاده از ابعاد اعتماد در تشکیل مجموعه‌ی ورودی‌های فازی، پارامترهای مختلفی را متناسب با هر بعد در نظر می‌گیریم. در اعتماد امنیت‌گرا به کمک شاخص‌هایی نظیر امنیت‌فیزیکی، احرازهویت، کنترل دسترسی و... سه پایگاه قانون متناسب با هر شاخص در نظر گرفته و به کمک داده‌های فازی آنها میزان اعتماد را برآورد می‌نماییم. در حالی که در اعتماد غیرامنیت‌گرا از شاخص‌هایی نظیر کیفیت خدمات و میزان رضایتمندی کاربران

از سرویس‌های ابری و... استفاده نموده و به کمک داده‌های فازی که از طریق پرسشنامه‌ی الکترونیکی پر شده توسط کاربران به دست می‌آید پایگاه قوانین را تشکیل و سپس میزان اعتماد را محاسبه می‌نماییم.

در این تحقیق، با تلفیق معیارهای بُعد امنیت‌گرا و روش پرسشنامه در بُعد غیرامنیت‌گرا، میزان اعتماد را ارزیابی می‌نماییم و با توجه به اینکه از افراد خبره جهت پاسخ‌دهی به پرسشنامه‌ی مد نظر استفاده می‌شود این روش تلفیقی امکانپذیر خواهد بود. ابتدا یک لیست جامع از پارامترهای امنیتی با ملاحظات امنیتی در محاسبات ابری را شناسایی می‌نماییم. این پارامترها در مدل اعتماد گنجانیده شده و نتیجه‌ی آن مقدار اعتماد است، که این مقدار اعتماد یک ارزش واحد به مفهوم قدرت امنیتی یک سرویس‌ابری است. قدرت امنیتی هر سرویس می‌تواند کاربر را به انتخاب سرویس مورد نیاز خود بر اساس خواسته‌ی خود نظیر هویت، حفاظت از داده و یا هر اقدام دیگر متناسب با مقدار اعتماد کمک نماید. در این راستا به مدل اعتماد TM می‌توان اشاره نمود که شامل پارامترهای مختلفی برای اندازه‌گیری قدرت امنیتی است.

شکل(۱-۳) ساختار مفهومی مدل اعتماد TM را با پارامترهای منحصر به فرد به خوبی شرح می‌دهد:



شکل(۱-۳) ساختار مفهومی مدل اعتماد TM

این مدل شامل پارامترهای زیر است:

مدیریت هویت(A)، احراز هویت(B)، مجوز(C)، حفاظت از اطلاعات(D)، محرمانگی ارتباطات(E)، کنترل ارتباطات(F)، جداسازی(G)، مجازی‌سازی(H)، پذیرش(I) (شیخ و دکتر کومار، ۲۰۱۵)؛ این پارامترها به صورت جداگانه اندازه‌گیری شده و برای محاسبه‌ی استحکام کلّی یک سرویس‌ابری استفاده می‌شوند.

۳-۳. سنجش معیارها (ارائه‌ی پرسشنامه)

جهت ارائه‌ی پرسشنامه از روش دیمتل استفاده می‌نماییم که پایایی این پرسشنامه با توجه به اینکه توسط خبرگان پاسخ داده می‌شود تأیید شده است. این روش، برای ساختاردهی یک دنباله از اطلاعات مفروض کاربرد دارد، به طوری که شدّت ارتباطات را به صورت امتیازدهی مورد بررسی قرار داده و بازخوردهای توأم با اهمیّت آنها را تجسّس می‌نماید، در نتیجه، با تبدیل مسائل کیفی به معیارهای کمّی و همچنین تقسیم‌بندی مجموعه‌ی وسیعی از عوامل پیچیده در قالب گروه‌های علّت-معلولی، تصمیم‌گیرنده را در شرایط مناسب‌تری از درک روابط قرار می‌دهد. مزیت این روش نسبت به سایر تکنیک‌ها (نظیر تکنیک تحلیل شبکه‌ای و...) روشنی و شفافیت آن در انعکاس ارتباطات متقابل میان مجموعه‌ی وسیعی از اجزاء می‌باشد، به طوری که متخصّصان قادر خواهند بود با تسلّط بیشتری به بیان نظرات خود در رابطه با اثرات (جهت و شدّت اثرات) میان عوامل بپردازند. با این تفاسیر، تکنیک دیمتل یکی از ابزارهای تصمیم‌گیری برای مواردی است که چندین معیار برای تصمیم‌گیری وجود دارد. بنابراین، در تصمیم‌گیری‌های چندمعیاره، هنگامی که لازم باشد مسائل پیچیده را در حین روشن‌کردن روابط میان عناصر مهم آنها حل کنیم، می‌توانیم از آن استفاده نماییم. در این تکنیک، روابط کمّی بین عوامل چندگانه یک مسئله و تأثیر هر یک از آنها بر دیگری محاسبه می‌شود. همچنین در این روش، میزان تأثیر مستقیم و غیرمستقیم عوامل بر یکدیگر سنجیده می‌شود، در نتیجه، با آن می‌توانیم عوامل موجود را به دو گروه علّت و معلول تقسیم نماییم و بر اساس آن یک مدل جامع پدید آوریم که این مهم جهت توافقنامه‌ی بین کاربر و سرویس‌دهنده‌ی ابری بسیار حائز اهمیّت است.(طالبی و آرش‌پور، ۱۳۹۲)

از آنجا که تکنیک دیمتل از انواع روش‌های تصمیم‌گیری بر اساس مقایسه‌های زوجی استفاده می‌نماید، لذا کافی است یک ماتریس مقایسه زوجی تشکیل داده و سپس از یک طیف مشخص برای نمره‌دهی استفاده نمود. ما نیز این ماتریس را در قالب پرسشنامه‌ای شامل دو جدول پاسخ مطرح نموده‌ایم و جهت سنجش رویکرد خبرگان از عبارات کلامی مطابق با طیف پنج درجه‌ای موجود در جدول راهنمای این پرسشنامه استفاده نموده منتها بعد از گردآوری عبارات کلامی، این دیدگاه‌ها مطابق درجات مشخص شده در این جدول کمّی می‌شوند. جدول(۱) میزان اثرگذاری هر کدام از معیارها بر یکدیگر را نشان می‌دهد. اهمیّت این جدول در این است که معیارهای امنیتی ارجح در استفاده از سرویس‌های ابری را برای هر دوره از محاسبه‌ی اعتماد به خوبی شناسایی می‌نماید. این مهم جهت تضمین ارزیابی صحیح از اعتماد در محیط پویای ابر است که همواره امکان رویارویی با چالش‌های امنیتی جدید را خواهد داشت. جدول(۲) نیز حاوی پاسخ‌هایی از خبرگان خواهد بود که مجموعه مقادیر $\{2,3,4,5\}$ از جدول راهنمای پاسخگویی را به خود پذیرفته و میزان تأثیر هر کدام از معیارهای امنیتی

برگزیده را در یک دوره‌ی معیّن بر روی اعتماد افراد خبره‌ی پاسخگو نسبت به استفاده از سرویس‌های ابری مورد استفاده می‌سنجد. این پرسشنامه به صورت زیر است:

پرسشنامه‌ی دیمتل

کارشناس محترم:

با سلام و احترام

پرسشنامه‌ی زیر در راستای پژوهشی جهت برآورد میزان اعتماد در استفاده از سرویس‌های ابری است که مقوله‌ی امنیت را تحت‌الشعاع خود قرار می‌دهد. لذا با تخصیص زمان ارزشمندتان به طور دقیق آن را تکمیل نمایید. پیشاپیش از همکاری شما صمیمانه سپاسگزاریم.

جدول راهنمای روش پاسخ‌دهی به پرسش‌ها و الگوی امتیازدهی(منظور از تأثیر همسان، تأثیر یک معیار بر خودش است)

بدون تأثیر	تأثیر همسان	تأثیر خیلی کم	تأثیر کم	تأثیر زیاد	تأثیر خیلی زیاد
۰	۱	۲	۳	٤	٥

دقت کنید تأثیر هر سطر را بر عنصر یا عناصر مندرج در ستون مشخص نمایید. برای نمونه اگر تأثیر یک شاخص از یک سطر بر یک شاخص از یک ستون زیاد باشد لزوماً عکس این ممکن است صحیح نباشد. یعنی دو آیتم ممکن است بر هم تأثیر داشته باشند یا اصلاً تأثیر نداشته باشند.

میزان تأثیر هر یک از معیارهای جدول زیر را نسبت به یکدیگر تعیین نمایید:

۱)

←	A	B	C	D	E	F	G	H	I
A	۱								
B		۱							
C			۱						
D				۱					
E					۱				
F						۱			
G							۱		
H								۱	
I									۱

میزان تأثیر هر یک از معیارهای جدول زیر بر روی اعتماد خود در استفاده از سرویس‌های ابری را تعیین نمایید:

۲)

↓	A	B	C	D	E	F	G	H	I

TRUST									

تعاریف پارامترهای این پرسشنامه به صورت زیر می‌باشد اما می‌توان از سایر پارامترها نیز در آن استفاده نمود:

A. مدیریت هویت: یک عنصر کلیدی برای امنیت ابر یا برنامه‌های کاربردی اینترنت است. هر سرویس ابری فرآیند تولید هویت برای کاربران را دنبال می‌نماید و از این فرآیند می‌توان جهت تعیین قدرت امنیتی بهره گرفت. پارامترهای مربوط به این فرآیند شامل ایجاد هویت، ذخیره‌سازی و چرخه‌ی مدیریت هویت است.

B. احراز هویت: برای افزایش امنیت روانی و اعتماد کاربران در زمان فرآیند ورود به ابر و تأیید هویت، چک احراز هویت مورد نیاز است. این یک فرآیند دو طرفه است. برای کاربران، دسترسی به خدمات ارائه‌دهندگان سرویس ابری معتبر و برای ارائه‌دهندگان خدمات ابری، ارائه‌ی خدمات به کاربران مشروع را ایجاب می‌نماید.

C. مجوز: کاربر مجاز به استفاده از هر گونه خدماتی نیست. به این صورت که هر گونه عملی از جمله دسترسی به خدمات و هر گونه عملیات ورودی/ خروجی نیاز به مجوز دارد که یک سرویس ابری آن را فراهم می‌نماید. پارامترهای این فرآیند شامل کنترل دسترسی، مدیریت اطلاعات و اعتبارسنجی از کاربران می‌باشد.

D. حفاظت از اطلاعات: داده‌ها، دارایی یک کاربر یا یک سازمان در ابر هستند. حفظ حریم خصوصی عمده نگرانی موجود در استفاده از سرویس‌های ابری است. پارامترهایی نظیر محرمانگی اطلاعات و یکپارچه‌سازی آنها و کنترل دسترسی در زیر گروه این فرآیند قرار می‌گیرند.

E. محرمانگی ارتباطات: یک سرویس ابری باید محرمانه بودن ارتباط بین کاربران ابر و ارائه‌دهندگان سرویس‌های ابری را تضمین نماید. پارامترهای این فرآیند شامل اندازه‌گیری محرمانگی، تکنیک دستیابی به حریم خصوصی داده‌ها، کنترل هویت بین ارائه‌دهنده‌ی سرویس‌های ابری و کاربر می‌باشد.

F. کنترل ارتباطات: داده‌ها و پیام‌های مصوب در محیط محاسبات ابری مستعد ابتلا به استراق سمع هستند. پس به کمک استانداردهای انتقال پیام و ارتباطات در محیط‌های ابری می‌توان این پارامتر را اندازه‌گیری نمود.

G. جداسازی: منظور، جداسازی منابع در میان کاربران مختلف است. پس اندازه‌گیری قدرت جداسازی توسط مدل اعتماد، سطح حفاظت را تعیین می‌نماید.

H. مجازی‌سازی: مفهوم محاسبات ابری ناقص و بدون ویژگی مجازی‌سازی است. زیرساخت‌های مجازی مستعد حملات فیزیکی هستند. به طور کلّی مهمترین اقدام امنیتی کاربردی برای حفاظت از محیط مجازی، مجازی‌سازی است. پارامترهای این فرآیند شامل قدرت VMM،VM، قدرت حفاظت و سایر ابزار نظارتی است.

I.پذیرش: نشان می‌دهد که روش و فرآیند یک سرویس، خاص بوده و کمتر توسط سازمان یا کاربران مجاز شناخته شده است و با صدور گواهینامه‌ی تصدیق و استانداردهای مختلف تعیین می‌شود. یا به طور کلّی، پذیرش کارآمدی امکانات یک سرویس با توجه به پشتیبانی استانداردهای مختلف از آن سرویس می‌باشد.

جدول(3-1) روش کار مدل پیشنهادی، یعنی ارزیابی اعتماد در استفاده از سرویس‌های ابری به کمک منطق فازی را به خوبی نشان می‌دهد.

جدول(۱-۳) فلوچارت روش ارزیابی اعتماد در استفاده از سرویس‌های ابری به کمک منطق فازی

ردیف	اهداف	نحوه‌ی تجزیه و تحلیل داده‌ها	روش کار
۱	تکمیل پرسشنامه توسط افراد خبره	محاسبه‌ی آلفای کرونباخ جداول شماره (۱) پرسشنامه	اگر مقدار آلفای کرونباخ کمتر از 0/5 باشد پرسشنامه رد می‌شود، در غیر این صورت پذیرفته می‌شود.
۲	محاسبه‌ی میانگین هندسی مؤلفه‌های جداول(۱) در پرسشنامه‌ها	میانگین هندسی مؤلفه‌های مشابه در هر کدام از جداول شماره(۱) پرسشنامه‌ها را محاسبه می‌نماییم.	مقادیر نهایی را در جدول نهایی به عنوان ماتریس روابط مستقیم ذخیره می‌نماییم.
۳	به دست آوردن ماتریس روابط کلّی	با استفاده از فرمول‌های موجود در تکنیک دیمتل، ماتریس روابط کلّی را به دست می‌آوریم.	از داده های موجود در ماتریس روابط کلّی جهت تعیین سه معیار برتر مورد نیاز استفاده می‌نماییم.
٤	تعیین شروط انتخاب معیارهای برتر	مجموع مقادیر هر کدام از سطرها را R و مجموع مقادیر هر کدام از ستون‌ها را D در نظر می‌گیریم، سپس مقادیر R-D و R+D را محاسبه می‌نماییم.	شرط اوّل: معیارهایی که در حیطه‌ی علّت باشند انتخاب می‌شوند. اگر R-D از یک معیار، مثبت باشد، آن معیار در حیطه‌ی علت قرار می‌گیرد، در غیر این صورت آن معیار در حیطه‌ی معلول قرار خواهد گرفت. شرط دوّم: معیارهایی که میزان اثرگذاری(R) بیشتری دارند انتخاب می‌شوند. شرط سوّم: در صورت نتیجه ندادن شرط دوّم، معیارهایی انتخاب می‌شوند که میزان اثرپذیری(D) کمتری دارند. شرط چهارم: در صورت نتیجه ندادن شرط سوّم، معیارهای دارای اهمیّت (R+D) بیشتر انتخاب می‌شوند.
۵	تعیین مقادیر معیارهای برتر	مجموع مولفه‌های مشابه هر معیار در جداول شماره(۲) پرسشنامه‌ها را محاسبه می‌نماییم.	مجموع اثرات هر معیار بر روی اعتماد افراد خبره‌ی پاسخگو را محاسبه نموده و مقدار به دست آمده را به بازه‌ی [0-100] انتقال می‌دهیم و نتیجه را به عنوان مقادیر ورودی فازی برای هر کدام از معیارها در منطق فازی استفاده می‌نماییم.

٦	ارزیابی میزان اعتماد به کمک منطق فازی	ورودی‌ها و خروجی و قوانین استنتاج فازی را مشخص می‌نماییم.	سه معیار برتر را به عنوان ورودی در نظر می‌گیریم و خروجی حاصل را اعتماد می‌نامیم. قوانین را طبق انتظاراتی که از سیستم تصمیم‌گیری داریم طرح می‌نماییم. مقادیر ورودی‌ها را وارد کرده و میزان اعتماد را ارزیابی می‌نماییم.

بنابراین، با توجه به اهداف تعیین شده در جدول(3-1)، در ادامه‌ی این پژوهش، روش کار خود را بیشتر توضیح می‌دهیم.

٤-٣. مراحل انجام کار

١-٤-٣. تکمیل پرسشنامه

جهت تکمیل این پرسشنامه و استفاده از آن در منطق‌فازی، نیاز به نمونه‌ی جامعه‌ی آماری داریم، لذا از آنجا که تعداد جامعه‌ی کل نامعلوم است، حجم نمونه را طبق "فرمول کوکران برای جامعه‌ی نامعلوم" محاسبه می‌نماییم. این فرمول به صورت زیر است:

$$n = \frac{z^2\, p(1-p)}{d^2} \qquad (٣-١)$$

که در آن z سطح اطمینان، p انحراف استاندارد و d حاشیه‌ی خطای در نظر گرفته شده می‌باشد.(مختاری و مجدی، ١٣٨١)؛ سطوح اطمینان رایج نیز عبارتند از:

- $90\% \rightarrow z = 1/645$
- $95\% \rightarrow z = 1/96$
- $99\% \rightarrow z = 2/326$

در نتیجه با در نظر گرفتن ٩٠٪ جهت سطح اطمینان مقدار z را ١/٦٤٥ خواهیم داشت. مقدار p را نیز ٠/٥ در نظر می‌گیریم زیرا این مقدار تضمین می‌کند که نمونه‌ی آماری ما به اندازه‌ی کافی بزرگ باشد. بازه‌ی اطمینان یا حاشیه‌ی خطا را نیز $\pm 11/6\%$ در نظر می‌گیریم. طبق این مقادیر جامعه‌ی آماری ما برابر می‌شود با:

$$n = \frac{(1/645)^2 \times 0/5(1-0/5)}{(0/116)^2} = \frac{(1/45)^2 \times (0/5)^2}{0/116^2} = \frac{2/71 \times 0/25}{0/0135} = \frac{0/6775}{0/0135} = 50$$

نکته‌ی قابل تأمل در فرمول بالا این است که چون از قبل اطلاعاتی درباره‌ی توزیع پاسخ‌ها در دست نیست، به جای مقدار p از $0/5$ که محافظه‌کارترین مقدار است استفاده نموده‌ایم. همچنین در صورت زیاد شدن حجم نمونه‌ی محاسبه شده می‌توان به آرامی سطح اطمینان را کاهش یا حاشیه‌ی خطا را افزایش داد. البته با این کار

شانس بروز خطا در نمونه‌گیری افزایش می‌یابد ولی به هر حال، حجم نمونه‌ی مورد نیاز به طور چشمگیری کاهش می‌یابد. به این ترتیب، در این پژوهش با در نظر گرفتن حاشیه‌ی خطای 11/6% حجم نمونه‌ای برابر با ۵۰ نفر از جامعه‌ی کل خواهیم داشت که شامل افراد خبره‌ی مرتبط با حوزه‌ی رایانش ابری بوده و از آنها خواسته می‌شود که روابط میان هر جفت شاخص را با عددی بین 0 تا 5 نمایش دهند.

البته اهمیّت جدول(۲) پرسشنامه‌ی مذکور این است که پاسخگویی به این جدول توسط تمامی کاربران نیز می‌تواند انجام بپذیرد اما از آنجا که اصطلاحات تخصصی در آن استفاده می‌شود بهتر است از خبرگان جهت تکمیل آن استفاده شود. در صورتی که نیاز به استفاده از کاربران در تکمیل آن باشد باید یک سری سؤالات شبیه‌سازی شده در راستای برآورد نتیجه‌ی مورد نیاز طراحی نمود که انتظارات ما از مقادیر ورودی ارزیابی اعتماد را برآورده سازد. به طور مثال جهت تعیین اثر کنترل ارتباطات بر اعتماد کاربر می‌توانیم در چارچوب این پرسشنامه از وی بپرسیم: "چقدر احساس می‌کنید که پیام‌های شما در این سرویس به صورت امن رد و بدل می‌شوند؟"

۲-٤-۳. محاسبه‌ی میانگین هندسی مؤلفه‌های جداول(۱) در پرسشنامه‌ها

از آنجا که تعداد پرسشنامه‌ها بیشتر از یک است لذا در این مرحله از طریق محاسبه‌ی میانگین هندسی امتیازات داده شده به هر معیار، تمام امتیازات داده شده به هر پرسشنامه را در قالب یک پرسشنامه خواهیم داشت. جهت این امر از تابع Geometric mean() استفاده می‌نماییم. از آنجا که این پرسشنامه به صورت ماتریس عنوان شده است لذا از اصطلاحات مربوط به بحث ماتریس‌ها بهره گرفته و محاسبات را به کمک ترفندهای محاسباتی ماتریس‌ها پیگیری می‌نماییم. بنابراین، امتیازات داده شده به هر مؤلفه را به عنوان مقادیر متعلّق به یک متغیّر در نظر گرفته و سپس به کمک نرم‌افزار spss، میانگین هندسی هر یک از این مجموعه‌ها را محاسبه نموده و به عنوان مقدار مؤلفه‌ی مربوط به پرسشنامه‌ی نهایی در نظر می‌گیریم. به طور مثال فرض کنید:

$$a_{ij} = \{2,3,4,4,5,3,5\}$$

از آنجا که این مجموعه دارای هفت عضو است بنابراین، میانگین هندسی مربوط به مقادیر موجود در این مجموعه برابر است با:

$$\sqrt[7]{2 \times 3 \times 4 \times 4 \times 5 \times 3 \times 5} = \sqrt[7]{7200} = 3/56$$

در نتیجه این مقدار در جدول نهایی به جای مؤلفه‌ی مورد نظر قرار می‌گیرد. بنابراین، طبق روش دیمتل، جدول به دست آمده را به عنوان ماتریس روابط مستقیم خواهیم داشت.

۳-٤-۳. به دست آوردن ماتریس روابط کلّی

جهت به دست آوردن ماتریس روابط کلّی، مراحل زیر را دنبال می‌نماییم:

۱. ایجاد ماتریس روابط مستقیم(A): همانطور که در مرحله‌ی قبل گفتیم، برای تشکیل این ماتریس از پاسخ‌دهندگان خواسته می‌شود که روابط میان هر جفت شاخص را با عددی بین 0 تا 5 نمایش دهند. اگر تعداد پاسخ‌دهندگان بیش از یک نفر باشد، ماتریس نهایی، از به دست آوردن میانگین هندسی امتیازات مربوط به رابطه‌ی هر جفت شاخص حاصل می‌شود.

2. نرمالیزه کردن ماتریس روابط مستقیم: بر مبنای ماتریس روابط مستقیم، ماتریس نرمالیزه از طریق فرمول زیر به دست می‌آید.

$$X = k \cdot A \qquad (۱-۱)$$

که در آن k برابر است با معکوسِ بزرگترین عدد مربوط به مجموع اعداد سطری ماتریس روابط مستقیم که به صورت زیر عنوان می‌شود:

$$K = \frac{۱}{max_{۱\le i\le n}\sum_{j=۱}^{\infty}(a_{ij})} \qquad i.j = ۱.۲.\ldots.n \qquad (۱-۲)$$

3. به دست آوردن ماتریس روابط کلّی: هنگامی که ماتریس روابط مستقیم نرمالیزه به دست آمد، ماتریس روابط کلّی (T) می‌تواند از فرمول زیر محاسبه شود که در آن I نشانگر ماتریس واحد است.

$$T = X(I - X)^{-۱} \qquad (۱-۳)$$

۳-٤-۳. تعیین شروط انتخاب معیارهای برتر

پس از تکمیل پرسشنامه مذکور توسط افراد خبره‌ای که در زمینه‌ی محاسبات ابری و امنیت آن از دانش و اطلاعات بسیار مطلوبی برخوردار هستند، به کمک تکنیک دیمتل معیارهای برتر را به ترتیب طبق شرایط زیر تعیین خواهیم نمود:

۱. تعیین معیارهایی که در ارزیابی علّت و معلول در حیطه‌ی علّت قرار دارند.
۲. تعیین معیارهایی که میزان اثرگذاری بیشتری نسبت به سایر معیارها دارند.
۳. در صورت تساوی میزان اثرگذاری دو یا چند معیار، تعیین معیار یا معیارهایی که میزان اثرپذیری کمتری نسبت به سایر معیارها دارند.

٤. در صورت نتیجه ندادن شروط ۲ و ۳، تعیین معیار یا معیارهایی که دارای اهمیّت بیشتری نسبت به سایر معیارها هستند.

با بررسی سلسله مراتبی این شروط، سه معیار برتر را به راحتی به دست می‌آوریم. جهت این امر ابتدا جمع سطری (R) و ستونی (D) را در ماتریس روابط کلّی خواهیم داشت. مقادیر R میزان تأثیرگذاری هر کدام از معیارها را بر روی خود و سایر معیارها نشان می‌دهد، در حالی که مقادیر D بیانگر میزان اثرپذیری هر معیار از خود و سایر معیارها است. در این پژوهش ما سه معیار برتر را نیاز خواهیم داشت که با بررسی شروط طبق همان ترتیبی که آورده‌ایم آنها را انتخاب می‌نماییم. جهت بررسی شرط اوّل، مقادیر R-D را برای هر کدام از معیارها خواهیم داشت که اگر این مقدار برای هر کدام از معیارها مثبت بود آن معیار در حیطه‌ی علّت قرار گرفته و در ادامه نیز از آن استفاده می‌نماییم، در غیر این صورت آن معیار در حیطه‌ی معلول قرار گرفته و در ادامه‌ی پژوهش از آن صرف نظر می‌شود. جهت بررسی شرط دوّم نیز مقادیر R را برای معیارهای خروجی از شرط اوّل خواهیم داشت و معیارهایی انتخاب می‌شوند که مقدار R بزرگتری نسبت به سایر معیارها دارند. اما اگر در این مرحله، بیش از سه معیار با مقادیر یکسان R داشته باشیم، شرط سوّم را بررسی نموده و معیارهایی را انتخاب می‌کنیم که مقادیر D کوچکتری نسبت به سایر معیارها داشته باشند. در نهایت، در صورتی که هیچکدام از شروط قبل جهت انتخاب معیارهای مورد نظر پاسخگو نبودند شرط چهارم را بررسی نموده و معیارهایی را انتخاب می‌نماییم که دارای اهمیّت بالاتری نسبت به سایر معیارها هستند یعنی مقادیر R+D آنها بزرگتر است. البته اگر پس از بررسی تمام شروط، چندین معیار، ارزش یکسانی داشتند به طور تصادفی سه معیار از آنها را انتخاب می‌نماییم یا اگر تعداد آنها کم بود می‌توانیم از تمامی آنها جهت ورودی منطق فازی بهره بگیریم.

۵-٤-۳. تعیین مقادیر معیارهای برتر

پس از مشخص شدن سه معیار برتر، با استفاده از جدول(۲) پرسشنامه، مجموع امتیازات داده شده به هر معیار را محاسبه نموده و هر کدام از آنها را به درصد تبدیل نموده و سپس در منطق فازی از آنها بهره می‌گیریم. به طور کلّی اگر حجم نمونه‌ی ما متشکل از m نفر از افراد خبره باشد و بیشترین امتیاز را n در نظر بگیریم، حال آنکه بازه‌ی ورودی در منطق فازی نیز [0.100] اختصاص داده باشیم، لذا نیاز به مبدل درصد (x) داریم تا مجموع امتیازات داده شده به هر معیار را در آن ضرب نماییم به این دلیل که ماکزیمم اعداد ورودی از صد تجاوز ننماید. جهت این امر، فرمول(۳-۲) را ارائه می‌دهیم:

$$mnx = 100 \qquad (۲-۳)$$

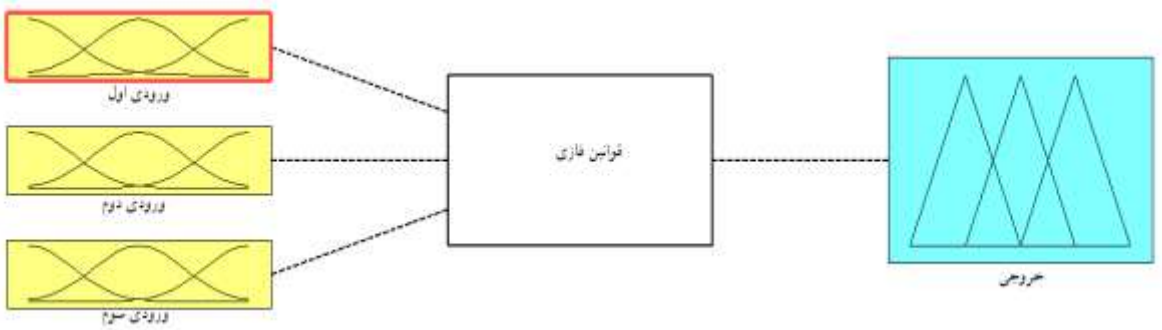
در این پژوهش، تعداد افراد خبره را ۵۰ نفر داریم و بیشترین امتیاز نیز ۵ می‌باشد، لذا طبق فرمول فوق مقدار x برابر می‌شود با:

$$50 \times 5 \times x = 100 \rightarrow x = \frac{100}{250} = 0/4$$

بنابراین جهت محاسبه‌ی مقادیر ورودی، ابتدا مجموع امتیازات داده شده به جداول(۲) پرسشنامه‌ها را به دست آورده و سپس هر کدام از آنها را در مبدل درصد یعنی $0/4$ ضرب می‌نماییم و اعداد حاصل را به عنوان ورودی‌های فازی استفاده می‌نماییم.

۶-٤-۳. ارزیابی میزان اعتماد به کمک منطق فازی

پس از معین شدن مقادیر سه معیار برتر، که درصد اثرگذاری هر یک از این معیارهای تعیین شده بر اعتماد را نشان می‌دهد، از این مقادیر به عنوان مقادیر ورودی فازی برای آن معیارها استفاده می‌نماییم. لذا با استفاده از این مقادیر و همچنین قوانین فازی موجود در منطق فازی، خروجی حاصل که میزان اعتماد است را به دست می‌آوریم. شکل(3-2) ساختار مفهومی منطق فازی را به خوبی نشان می‌دهد.



شکل(3-2) ساختار مفهومی منطق فازی

5-3. نتیجه‌گیری

در عصر حاضر که استفاده از محاسبات ابری رو به گسترش است ناگزیر باید روشی مطمئن برای ارزیابی اعتماد به آن لحاظ نمود زیرا چالش‌هایی از قبیل امنیت، کیفیت خدمات و ...، میزان رضایتمندی کاربران این حوزه و در نتیجه اعتماد آنها به استفاده از سرویس‌های ابری را تحت تأثیر قرار خواهند داد. در این پژوهش با بهره‌گیری از معیارهای امنیتی در حوزه‌ی محاسبات ابری، روشی را ارائه نموده‌ایم که به کمک سیستم‌های

استنتاج فازی، میزان اعتماد به سرویس‌های ابری را محاسبه می‌نماید. در این روش، چارچوب کلّی زیر را دنبال خواهیم نمود:

۱. تعیین معیارهای امنیتی مورد نیاز که به نوعی با مسئله‌ی اعتماد به سرویس‌های ابری در ارتباط هستند.
۲. تعیین معیارهای برتر به عنوان ورودی‌های منطق فازی به کمک جدول(۱) پرسشنامه‌ی دیمتل.
۳. تعیین مقادیر ورودی فازی به کمک جدول(۲) پرسشنامه‌ی دیمتل.
٤. تعیین وضعیت نهایی اعتماد با استفاده از منطق فازی ممدانی.

البته، جنبه‌ی نوآور بودن این روش، در استفاده از منطق‌فازی جهت ارزیابی قدرت امنیتی سرویس‌های ابری و در نتیجه‌ی آن میزان اعتماد در استفاده از آنها است. در حالی که در گذشته این امر مهم به کمک توابع و الگوریتم‌های مختلفی صورت می‌پذیرفت که خروجی حاصل از آنها از آنجا که باید تنها پارامترهای مقداری را در خود حل می‌نمود تا حدودی ناکارآمد بود، زیرا بسیاری از معیارهای پیش روی ارزیابی اعتماد را نمی‌توان به عنوان یک مقدار خاص در نظر گرفت. به عنوان مثال، معیار امنیت را می‌توان نام برد که از لحاظ منطقی چنین نتیجه‌ای بی معنی است که"میزان امنیت یک است"، بلکه نتیجه‌ی صحیح این است که: "میزان امنیت ضعیف است". پس جایگزین نمودن پارامترهای فازی به جای پارامترهای عددی عوامل مهمتری را در ارزیابی میزان اعتماد دخیل می‌نماید(مرحله‌ی فازی‌سازی) و این در حالی است که در انتهای کار که میزان اعتماد را برآورد می‌نمائیم یک عدد به دست می‌آید و نشان می‌دهد که منطق‌فازی، کار الگوریتم‌ها را با درصد کاملتری به سرانجام می‌رساند که این عدد در بازه‌ی ضعیف تا قوی بیان می‌شود و برای کاربران نیز خیلی راحت‌تر قابل درک خواهد بود(مرحله‌ی غیرفازی‌سازی).

کلمات کلیدی فصل سوّم

Trust Management	مدیریت اعتماد
Decision Making Trial And Evaluation (DEMATEL)	روش دیمتل
Virtual Machine (VM)	ماشین مجازی
VM Monitor (VMM)	نمایشگر ماشین مجازی

فصل چهارم:

رویکرد پیشنهادی و نتایج ارزیابی

۱-٤. پایایی و روایی پرسشنامه

پایایی پرسشنامه‌ی دیمتل، با توجه به اینکه توسط خبرگان پاسخ داده شده است، تأیید شده است.(طالبی و آرش‌پور، ۱۳۹۲)؛ با این حال جهت بررسی پایایی و روایی پرسشنامه‌های تکمیل شده باید گفت: "پایایی، درجه‌ای از ثبات نتایج طی زمان و قابلیت تکرار آنها می‌باشد که سنجش پایایی علاوه بر روش معمول آلفای کرونباخ با روش‌های دیگر نیز قابل اندازه‌گیری است، در حالی که روایی درجه‌ای از صحت نتایج می‌باشد".(محمد بیگی و همکاران، ۱۳۹۳)؛ از طرف دیگر، شرط لازم برای روایی یک آزمون، پایایی آن است ولی شرط کافی نیست و برای اینکه یک آزمون معتبر روا باشد باید پایا باشد. به بیان دیگر، روایی نشان‌دهنده‌ی صحّت اندازه‌گیری است.(لانگ و ویلکرسون، ۲۰۰۸)

جهت تعیین روایی می‌توان از دو روش کیفی و کمّی استفاده کرد. در روش کیفی، می‌توان با متخصّصین درباره‌ی پیامد مورد اندازه‌گیری مصاحبه و مشاوره داشت. در ارزیابی کیفی، رعایت دستور زبان، استفاده از کلمات مناسب، اهمیّت آیتم‌ها، قرارگیری آیتم‌ها در جای مناسب خود، زمان تکمیل ابزار طراحی شده مورد توجه قرار می‌گیرد.(پولیت و بِک، ۲۰۰٦)؛ از آنجا که این پرسشنامه توسط افراد خبره و متخصّص در حوزه‌ی رایانش ابری تکمیل شده است لذا هرگونه اشکالی از بابت سنجش روایی آن مورد بررسی قرار داده و نسبت به رفع آن کوشیده‌ایم.

در این پژوهش جهت تعیین پایایی پرسشنامه‌ها از روش آلفای کرونباخ بهره گرفته‌ایم. روش آلفای کرونباخ نه تنها برای گزینه‌های دو ارزشی صفر و یک، بلکه برای گزینه‌های چند ارزشی (مانند طیف ۵ گزینه‌ای لیکرت) نیز قابل استفاده است. اگر بخش‌های آزمون یا خرده آزمون‌هایی که از مجموع آنها آزمون کلّی تشکیل شده است به طور جداگانه نمره‌گذاری شوند، در آن صورت ضریب آلفا مستلزم این نیست که تک تک سؤالات به صورت صحیح و غلط باشند.

اگر ضریب آلفای کرونباخ ۰/۷ یا بیشتر باشد، پرسشنامه از پایایی مطلوبی برخوردار است و می‌توانیم از بابت همبستگی درونی سؤالات مطمئن باشیم. ولی اگر مقدار آلفا بین ۰/۵ تا ۰/۷ باشد اعتبار پرسشنامه در حد متوسط ارزیابی می‌شود و در صورتی که مقدار آلفا کمتر از ۰/۵ باشد پرسشنامه فاقد پایایی لازم است.

فرمول محاسبه‌ی آلفای کرونباخ به صورت زیر است:

$$\alpha = \frac{K}{K-1}\left(1 - \frac{\sum S_i^2}{S_t^2}\right) \qquad (٤-١)$$

که در آن K تعداد معیارها، S_i^2 واریانس معیار i و S_t^2 واریانس کل پرسشنامه می‌باشد.

بنابراین، ابتدا پرسشنامه‌های تکمیل شده از نظر پایایی، یکی یکی مورد بررسی قرار می‌گیرند. این مهم را به کمک نرم‌افزار SPSS انجام می‌دهیم. از آنجا که یک پرسشنامه با تعدادی سؤال (مانند طیف ۵ گزینه‌ای لیکرت) مانند یک آزمون است، می‌توان مقدار پایایی را به کمک آلفای کرونباخ به دست آورد.

لذا در شرایطی که مقدار آلفای کرونباخ در پرسشنامه‌های تکمیل شده ۰/۵ یا بیشتر از ۰/۵ باشد پایایی پرسشنامه مورد تأیید قرار می‌گیرد، در غیر این صورت باید پاسخگویی به پرسشنامه‌ها تکرار شود. این به این معنی است که ممکن است فرد خبره، پاسخنامه‌ی خود را بدون توجه به عملکرد معیارها تکمیل نموده باشد.

۲-٤. پیاده‌سازی داده‌ها در spss

نمونه‌ی پرسشنامه‌ی تکمیل شده‌ی زیر را در نظر بگیرید:

جدول(۱-٤) نمونه‌ی پرسشنامه‌ی تکمیل شده‌ی بدون کارایی

	A	B	C	D	E	F	G	H	I
A	۱,۰۰	۵,۰۰	۳,۰۰	٤,۰۰	۵,۰۰	۳,۰۰	۲,۰۰	۲,۰۰	۵,۰۰
B	۵,۰۰	۱,۰۰	٤,۰۰	٤,۰۰	٤,۰۰	۳,۰۰	۲,۰۰	۲,۰۰	٤,۰۰
C	٤,۰۰	٤,۰۰	۱,۰۰	۳,۰۰	٤,۰۰	۳,۰۰	٤,۰۰	۳,۰۰	۵,۰۰
D	٤,۰۰	۵,۰۰	۵,۰۰	۱,۰۰	٤,۰۰	٤,۰۰	۵,۰۰	۳,۰۰	٤,۰۰
E	۵,۰۰	۳,۰۰	٤,۰۰	٤,۰۰	۱,۰۰	٤,۰۰	۵,۰۰	۳,۰۰	٤,۰۰
F	٤,۰۰	۳,۰۰	۳,۰۰	۳,۰۰	۳,۰۰	۱,۰۰	٤,۰۰	۲,۰۰	٤,۰۰
G	۲,۰۰	۲,۰۰	۳,۰۰	٤,۰۰	٤,۰۰	۳,۰۰	۱,۰۰	۲,۰۰	٤,۰۰
H	٤,۰۰	۲,۰۰	٤,۰۰	٤,۰۰	٤,۰۰	۳,۰۰	۲,۰۰	۱,۰۰	٤,۰۰
I	٤,۰۰	٤,۰۰	٤,۰۰	۳,۰۰	٤,۰۰	۳,۰۰	٤,۰۰	۳,۰۰	۱,۰۰

پس از ورود این داده‌ها به SPSS مقدار خروجی آلفای کرونباخ به صورت جدول زیر به دست می‌آید:

جدول(۲-٤) آلفای کرونباخ نامطلوب

تعداد معیارها	آلفای کرونباخ
۹	-۰/۳٤۷

بنابراین، برای جدول(۱-٤)، مقدار آلفا منفی و کمتر از ۰/۵ می‌باشد، لذا از این پرسشنامه‌ی تکمیل شده صرف نظر کرده و مابقی پرسشنامه‌ها را به همین صورت مورد بررسی قرار داده و در صورت احراز پایایی لازم از

داده‌های آن در پیشبرد این پژوهش بهره می‌گیریم، این در حالی است که نمونه‌ی پرسشنامه‌ی تکمیل شده‌ی زیر شرایط بسیار متفاوتی را دارا است.

جدول(۳-٤) نمونه‌ی پرسشنامه‌ی تکمیل شده با کارایی لازم

	A	B	C	D	E	F	G	H	I
A	۱,۰۰	۵,۰۰	۵,۰۰	۵,۰۰	٤,۰۰	٤,۰۰	۵,۰۰	۳,۰۰	۵,۰۰
B	۵,۰۰	۱,۰۰	٤,۰۰	٤,۰۰	٤,۰۰	٤,۰۰	۵,۰۰	۳,۰۰	٤,۰۰
C	٤,۰۰	۳,۰۰	۱,۰۰	۳,۰۰	۳,۰۰	۲,۰۰	٤,۰۰	۲,۰۰	٤,۰۰
D	٤,۰۰	۳,۰۰	٤,۰۰	۱,۰۰	۳,۰۰	۳,۰۰	٤,۰۰	۵,۰۰	٤,۰۰
E	۳,۰۰	٤,۰۰	٤,۰۰	٤,۰۰	۱,۰۰	۵,۰۰	۵,۰۰	۳,۰۰	٤,۰۰
F	۳,۰۰	٤,۰۰	۳,۰۰	٤,۰۰	٤,۰۰	۱,۰۰	۳,۰۰	۳,۰۰	٤,۰۰
G	۲,۰۰	۰۰.	۳,۰۰	۲,۰۰	۰۰.	۰۰.	۱,۰۰	٤,۰۰	۳,۰۰
H	۲,۰۰	۰۰.	۲,۰۰	۰۰.	۰۰.	۰۰.	۲,۰۰	۱,۰۰	۳,۰۰
I	۵,۰۰	۵,۰۰	۵,۰۰	۵,۰۰	۵,۰۰	۵,۰۰	۲,۰۰	۵,۰۰	۱,۰۰

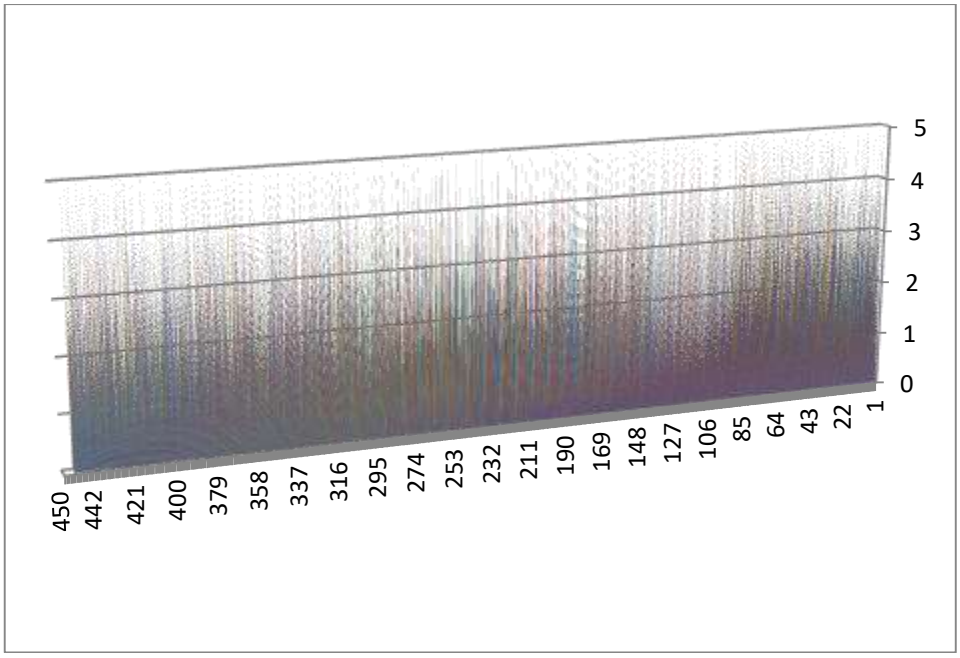
پس از محاسبه‌ی آلفای کرونباخ این پرسشنامه‌ی پاسخ داده شده در SPSS، جدول زیر را در خروجی به دست آوردیم:

جدول(٤-٤) آلفای کرونباخ مطلوب

تعداد معیارها	آلفای کرونباخ
۹	۰/۸٤۲

همانگونه که مشاهده می‌شود مقدار آلفای حاصل از بررسی پایایی این پرسشنامه برابر ۰/۸٤۲ بوده و بیشتر از ۰/۷ است. لذا این پرسشنامه از پایایی خوبی برخوردار بوده و در ادامه‌ی پژوهش نیز از آن بهره می‌گیریم.

نمودار(۱-٤) نیز نشانگر تراکم پاسخ‌ها به معیارهای مورد نظر در جدول(۱) حاصل از مجموع امتیازات پنجاه پرسشنامه‌ی تکمیل شده می‌باشد. از آنجا که جدول(۱) در پرسشنامه شامل ۹ معیار اثرگذار بوده و تعداد پرسشنامه‌ها نیز ۵۰ عدد می‌باشد لذا در این نمودار بازه‌ی بین ۰ تا ٤۵۰ را خواهیم داشت. این به این معنی است که تعداد کل سؤالات پاسخ داده شده ٤۵۰ سؤال می‌باشد.



نمودار(۱-٤)تراکم پاسخ‌ها به معیارها در حد بالای امتیازات(۳ تا ۵)

طبق نمودار فوق، تراکم خوب خطوط در بازه‌ی ۳ تا ۵، نشانگر وجود معیارهای ارجح در پرسشنامه می‌باشد.

۳-٤. انتخاب معیارهای برتر

جهت انتخاب معیارهای برتر ابتدا میزان اثرگذاری و اثرپذیری معیارها را با استفاده از تکنیک دیمتل به دست می‌آوریم. بنابراین در ادامه، مراحل این تکنیک را گام به گام دنبال می‌نماییم.

۱-۳-٤. ایجاد ماتریس روابط مستقیم

در این روش جهت ایجاد ماتریس روابط مستقیم (A) از امتیازات داده شده به جداول(۱) پرسشنامه‌های تکمیل شده بهره می‌گیریم. از آنجا که تعداد پرسشنامه‌ها بیشتر از یک است لذا در مرحله‌ی اوّل از طریق محاسبه‌ی میانگین هندسی امتیازات داده شده به هر معیار، ماتریس روابط مستقیم را که یک ماتریس ۹×۹ می‌باشد به دست خواهیم آورد. جهت این امر از تابع Geometric mean() استفاده می‌نماییم. این تابع در محیط spss قابل دسترسی است به این صورت که مقادیر مربوط به روابط بین دو معیار را در مجموعه‌ی متعلّق به یک متغیّر قرار داده و آن متغیّر را در محیط spss تعریف می‌نماییم. سپس به کمک تابع مذکور، میانگین هندسی مقادیر اختصاصی را جهت تشکیل ماتریس نهایی محاسبه می‌نماییم. این فعالیت جهت تعیین مقادیر نهایی تمام مؤلفه‌ها

به صورت جداگانه صورت می‌پذیرد. جدول(٥-٤) ماتریس روابط مستقیم (A) حاصل از این فعالیت را به خوبی نشان می‌دهد.

جدول(5-4) عناصر ماتریس روابط مستقیم (A)

	A	B	C	D	E	F	G	H	I
A	١	٣/١٢	٣/٤٠	٣/٧٠	٣/٠٣	٢/٨٣	٢/٨٦	٢/٨١	٣/٠٨
B	٣/٠٤	١	٣/٥١	٣/٠٦	٣/٠٥	٣/١٣	٢/٨٤	٢/٤٨	٢/٨٠
C	٣/١٧	٣/٤٢	١	٣/٠٢	٣/١٠	٢/٩٥	٢/٦٢	٢/٦٨	٣/١٦
D	٣/١٨	٢/٩٥	٢/٩٨	١	٣/٤٦	٢/٤٨	٣/٠٣	٣/٥٧	٣/١٦
E	٢/٩٨	٣/٢٩	٣/٠٧	٢/٩٤	١	٣/٥١	٢/٩٣	٠	٢/٩
F	٢/٩٣	٣	٣/٢٨	٣/٢٤	٣/٢١	١	٠	٢/٧٩	٣/١٦
G	٠	٠	٣/٠١	٣/٠٩	٠	٠	١	٣/٣٧	٣/٠٩
H	٠	٠	٢/٨٨	٠	٠	٠	٣/٠٤	١	٢/٨٦
I	٢/٨٨	٣/١٤	٣	٣/٠٦	٢/٦٥	٢/٧٣	٢/٦١	٣/٣٥	١

٢-٣-٤. نرمالیزه کردن ماتریس روابط مستقیم

جهت نرمالیزه کردن ماتریس A از فرمول زیر استفاده می‌نماییم:

$$X = k \cdot A \qquad (٤-٢)$$

$$K = \frac{١}{max_{١\le i\le n}\sum_{j=١}^{\infty}(a_{ij})} \qquad i.j = ١.٢.\ldots.n \qquad (٤-٣)$$

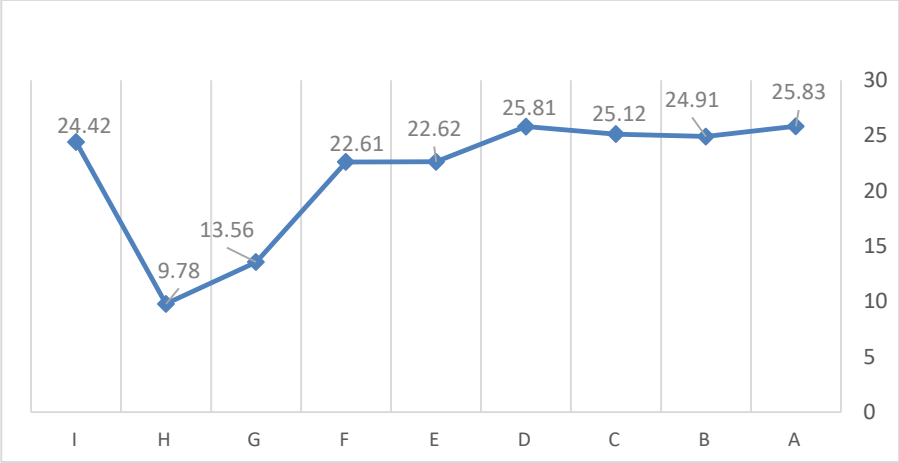
که در آن X همان ماتریس نرمالیزه شده است و جهت محاسبه‌ی مقدار K، ابتدا مجموع عناصر تک تک سطرها در ماتریس روابط مستقیم A را به دست می‌آوریم و از بین آنها مقدار ماکزیمم را انتخاب و معکوس می‌نماییم. جدول(٦-٤) حاوی مجموع مقادیر هر سطر از ماتریس روابط مستقیم طبق معیارهای روبروی آن می‌باشد.

جدول(٦-٤) مجموع مقادیر هر یک از سطرهای ماتریسA

25.83	A
24.91	B
25.12	C
25.81	D
22.62	E
22.61	F
13.56	G

9.78	H
24.42	I

نمودار(۲-٤) مقایسه‌ی مقادیر موجود در جدول(٦-٤) را جهت انتخاب مقدار ماکزیمم انجام می‌دهد.



نمودار(۲-٤) مجموع عناصر هر سطر در ماتریس A

با توجه به نمودار(۲-٤)، مقدار ماکزیمم مجموع عناصر سطرهای A برابر است با ۲۵/۸۳، در نتیجه K برابر است با:

$$K = \frac{۱}{۲۵/۸۳} = ۰/۰۳۹$$

بنابراین

$$X = ۰/۰۳۹ \times A$$

خروجی حاصل از این عبارت به صورت جدول زیر به دست می‌آید:

جدول(۷-٤) عناصر ماتریس نرمالیزه شده ی ماتریس A

I	H	G	F	E	D	C	B	A	
۰/۱۲	۰/۱۱	۰/۱۱	۰/۱۱	۰/۱۲	۰/۱٤	۰/۱۳	۰/۱۲	۰/۰٤	A
۰/۱۱	۰/۱۰	۰/۱۱	۰/۱۲	۰/۱۲	۰/۱۲	۰/۱٤	۰/۰٤	۰/۱۲	B
۰/۱۲	۰/۱۰	۰/۱۰	۰/۱۲	۰/۱۲	۰/۱۲	۰/۰٤	۰/۱۳	۰/۱۲	C
۰/۱۲	۰/۱٤	۰/۱۲	۰/۱۰	۰/۱۳	۰/۰٤	۰/۱۲	۰/۱۲	۰/۱۲	D
۰/۱۱	۰/۰۰	۰/۱۱	۰/۱٤	۰/۰٤	۰/۱۱	۰/۱۲	۰/۱۳	۰/۱۲	E
۰/۱۲	۰/۱۳	۰/۰۰	۰/۰٤	۰/۱۳	۰/۱۳	۰/۱۳	۰/۱۱	۰/۱۱	F

G	۰/۰۰	۰/۰۰	۰/۱۲	۰/۱۲	۰/۰۰	۰/۰۰	۰/۰٤	۰/۱۳	۰/۱۲
H	۰/۰۰	۰/۰۰	۰/۰۰	۰/۱۱	۰/۰۰	۰/۰۰	۰/۱۲	۰/۰٤	۰/۱۱
I	۰/۱۱	۰/۱۲	۰/۱۲	۰/۱۱	۰/۱۰	۰/۱۱	۰/۱۰	۰/۱۳	۰/۰٤

٤-۳-۳. به دست آوردن ماتریس روابط کلّی

جهت به دست آوردن ماتریس روابط کلّی از فرمول زیر استفاده می‌نماییم که در آن I نشانگر ماتریس واحد است.

$$T = X(I - X)^{-1} \qquad (٤-۳)$$

با جایگذاری ماتریس‌های خواسته شده در این عبارت، جدول نهایی زیر حاصل می‌شود که روابط کلّی معیارهای مورد نظر را به خوبی نمایش می‌دهد.

جدول(۸-٤) روابط کلّی معیارها

	A	B	C	D	E	F	G	H	I
A	۰/۵۹	۰/٦۸	۰/۸۵	۰/۷۸	۰/٦٦	۰/٦٤	۰/۷۱	۰/۷٤	۰/۸۲
B	۰/٦٤	۰/۵۹	۰/۸۳	۰/۷٤	۰/٦۵	۰/٦۳	۰/٦۹	۰/۷۰	۰/۷۹
C	۰/٦۵	۰/٦۸	۰/۷۵	۰/۷٤	۰/٦٦	۰/٦۳	۰/٦۸	۰/۷۲	۰/۸۱
D	۰/٦۵	۰/٦٦	۰/۸۲	۰/٦۷	۰/٦۷	۰/٦۱	۰/۷۰	۰/۷۵	۰/۸۱
E	۰/٦۳	۰/٦٦	۰/۷۹	۰/۷۲	۰/۵٦	۰/٦۳	۰/٦٦	۰/۵۹	۰/۷٦
F	۰/٦۲	۰/٦٤	۰/۷۹	۰/۷۱	۰/٦٤	۰/۵۳	۰/۵٦	۰/٦۸	۰/۷٦
G	۰/۲٦	۰/۲۷	۰/٤٦	۰/٤۲	۰/۲۷	۰/۲۵	۰/۳٤	۰/٤٤	۰/٤٦
H	۰/۱۸	۰/۱۹	۰/۳۵	۰/۲۲	۰/۱۸	۰/۱۷	۰/۳۲	۰/۲٦	۰/۳۵
I	۰/۲٦	۰/٦٤	۰/۷۹	۰/۷۱	۰/٦۲	۰/۵۹	۰/٦٦	۰/۷۱	۰/۷۰

٤-۳-٤. ایجاد نمودار علّت و معلول

جهت ایجاد نمودار علّت و معلول از جدول(۸-٤) استفاده نموده و موارد زیر را از آن استخراج می‌نماییم:

D: به عنوان جمع ستونی ماتریس روابط کلّی در نظر گرفته می‌شود و نشان می‌دهد که یک معیار چقدر از معیارهای دیگر تأثیر می‌پذیرد.

R: به عنوان جمع سطری ماتریس روابط کلّی در نظر گرفته می‌شود و نشان می‌دهد که یک معیار چقدر بر معیارهای دیگر تأثیر می‌گذارد.

R-D: از تفریق D از R به دست می‌آید و می‌تواند شاخص‌ها را به دو گروه علّت و معلول تقسیم نماید. اگر این مقدار مثبت باشد، شاخص به گروه علّت تعلّق دارد و در صورت منفی بودن، متعلّق به گروه معلول است.

R+D: از اضافه کردن D به R به دست می‌آید و نشان دهنده‌ی اهمیّت هر معیار است.

تمام این موارد را در جدول صفحه‌ی بعد یعنی جدول(۹-٤) می‌توانید مشاهده نمایید.

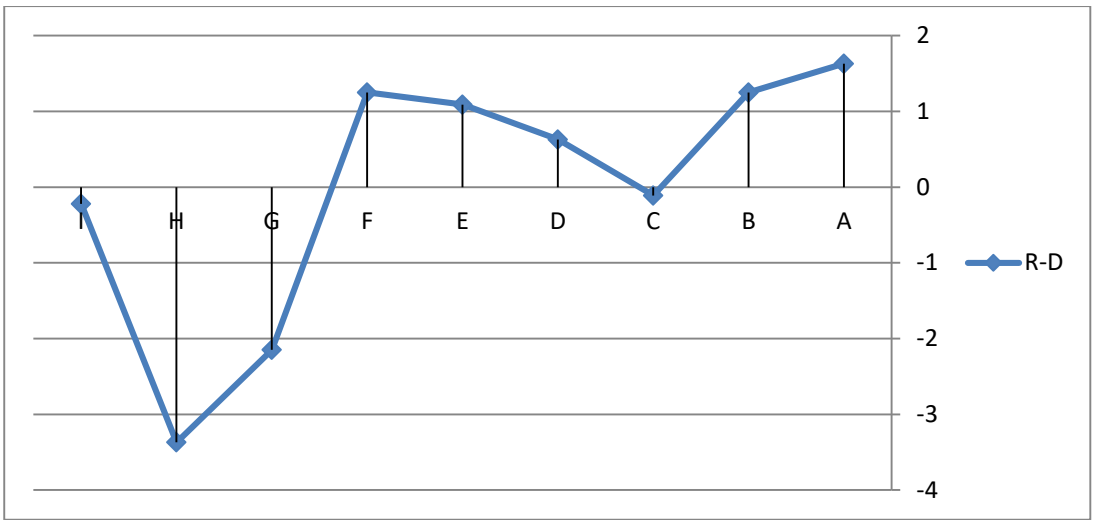
جدول(۹-٤) جمع سطری و جمع ستونی ماتریس روابط کلّی

	A	B	C	D	E	F	G	H	I
D	٤/٨٤	٥/٠١	٦/٤٣	٥/٧١	٤/٩١	٤/٦٨	٥/٣٢	٥/٥٩	٦/٢٦
R	٦/٤٧	٦/٢٦	٦/٣٢	٦/٣٤	٦	٥/٩٣	٣/١٧	٢/٢٢	٦/٠٤
R-D	١/٦٣	١/٢٥	-٠/١١	٠/٦٣	١/٠٩	١/٢٥	-٢/١٥	-٣/٣٧	-٠/٢٢
R+D	١١/٣١	١١/٢٧	١٢/٧٥	١٢/٠٥	١٠/٩١	١٠/٦١	٨/٤٩	٧/٨١	١٢/٣

بنابراین، با استفاده از نتایج جدول(۹-٤) شروط تعیین معیارهای برتر را بررسی می‌نماییم.

شرط اوّل: معیارهایی برتر هستند که در ارزیابی علّت و معلول در حیطه‌ی علّت قرار داشته باشند.

جهت این امر مقادیر R-D را بررسی می‌نماییم. اگر مقدار اختصاصی R-D از یک معیار مثبت باشد آن معیار متعلّق به گروه علّت است و آن را به عنوان یکی از معیارهای مورد نظر مورد بررسی قرار می‌دهیم اما در صورت منفی بودن این مقدار، آن معیار متعلّق به گروه معلول است و از آن صرف نظر می‌کنیم. نمودار زیر حیطه‌ی هر کدام از معیارها را به خوبی نشان می‌دهد:



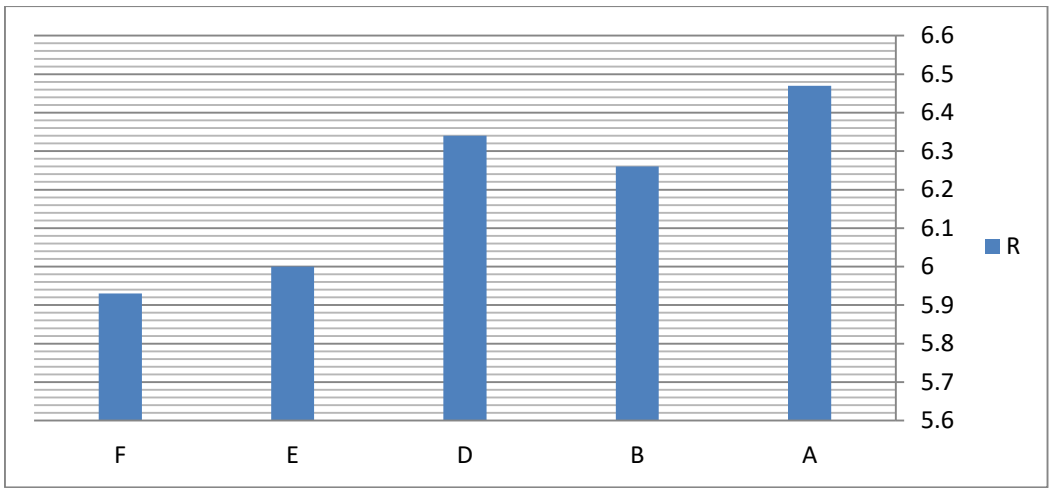
نمودار(۳-٤) بررسی علّت یا معلول بودن معیارها

همانطور که در نمودار(۳-٤) مشاهده می‌شود معیارهای A و B و D و E و F در قسمت مثبت نمودار فوق قرار گرفته‌اند، در نتیجه آنها را به عنوان معیارهای مفید مورد بررسی قرار می‌دهیم اما از آنجا که معیارهای C و G و H و I در قسمت منفی نمودار قرار گرفته‌اند از آنها صرف نظر می‌کنیم. بنابراین پس از بررسی شرط اوّل، معیارهای A و B و D و E و F انتخاب شده و در ادامه پژوهش از آنها بهره می‌گیریم.

شرط دوّم: معیارهایی برتر هستند که میزان اثرگذاری بیشتری نسبت به سایر معیارها داشته باشند.

جهت تعیین این معیارها مقادیر مختص R را مورد بررسی قرار می‌دهیم و با رسم نمودار آن، سه معیار با بیشترین اثرگذاری را از بین سایر معیارها انتخاب می‌نماییم. اما در صورت مساوی بودن مقادیر چند معیار انتخابی با یکدیگر، شرط بعد (یعنی معیاری که اثر پذیری کمتری نسبت به سایر معیارها دارد) را بررسی می‌نماییم.

نمودار(٤-٤) با استفاده از معیارهای علّت و حذف معیارهای معلول جهت بررسی شرط دوّم ارائه شده است:



نمودار(٤-٤) تعیین سه معیار با بیشترین اثرگذاری بر سایر معیارها

طبق نمودار(٤-٤)، از آنجا که معیارهای A و B و D دارای بیشترین مقدار R یعنی بیشترین میزان اثرگذاری نسبت به سایر معیارها می‌باشند به عنوان سه معیار برتر انتخاب می‌شوند و دیگر نیازی به بررسی شرط سوّم و چهارم نیست. لازم به ذکر است که شرط سوّم در صورت تساوی میزان اثرگذاری چند معیار با یکدیگر معیاری را برمی‌گزینند که میزان اثرپذیری کمتری نسبت به سایر معیارها داشته باشد، لذا مقادیر D را مورد بررسی قرار داده و معیاری با کمترین مقدار D انتخاب می‌نماید و شرط چهارم نیز در صورتی که شروط قبلی منجر به نتیجه‌ی درست نشوند معیاری را برمی‌گزینند که دارای اهمیّت بیشتری نسبت به سایر معیارها باشد، در نتیجه مقادیر R+D را مورد بررسی قرار می‌دهد و معیاری با ماکزیمم مقدار R+D را برمی‌گزینند.

٤-٤. تعیین داده‌های ورودی فازی

نقطه‌ی شروع ساخت یک سیستم فازی به دست آوردن مجموعه‌ای از قواعد "اگر-آنگاه فازی" از دانش افراد خبره یا دانش حوزه‌ی مورد بررسی می‌باشد، مرحله‌ی بعدی، ترکیب این قواعد در یک سیستم واحد است.

همانطور که گفته شد پرسشنامه‌ی مذکور، تأثیرات هر کدام از معیارها بر اعتماد را در پی دارد و با توجه به جدول راهنما که در زیر نشان داده‌ایم این تأثیرات قابل امتیازدهی است:

جدول(١٠-٤) راهنمای امتیازدهی به معیارها

بدون تأثیر	تأثیر همسان	تأثیر خیلی کم	تأثیر کم	تأثیر زیاد	تأثیر خیلی زیاد
٠	١	٢	٣	٤	٥

جهت تعیین مقادیر ورودی فازی برای سه معیار برتر نیز ابتدا مجموع امتیازات داده شده به هر معیار در جداول(۲) پرسشنامه‌ها را به کمک spss محاسبه نموده و سپس با کمک مبدل درصد که طبق فرمول زیر محاسبه می‌شود، مقادیر مجموع را به بازه‌ی [100-0] انتقال می‌دهیم.

$$mnx = 100 \qquad (٤-٤)$$

در این پژوهش، تعداد افراد خبره (m) را ۵۰ نفر داریم و بیشترین امتیاز (n) نیز ۵ می‌باشد، لذا طبق فرمول فوق مقدارx برابر می‌شود با:

$$50 \times 5 \times x = 100 \rightarrow x = \frac{100}{250} = 0/4$$

بنابراین جهت محاسبه‌ی مقادیر ورودی، پس از محاسبه‌ی مجموع امتیازات داده شده به هر معیار، هر کدام از آنها را در مبدل درصد (x) یعنی 0/4 ضرب می‌نماییم و اعداد حاصل را گرد کرده و به عنوان ورودی‌های فازی استفاده می‌نماییم. جدول‌های (۱۱-٤) و (۱۲-٤) اطلاعات به دست آمده از جداول(۲) پرسشنامه‌ها را نشان می‌دهند که حاصل از پاسخگویی تعداد پنجاه نفر از افراد خبره می‌باشد و آنها را با یکدیگر ترکیب نموده‌ایم.

جدول(*4-11*) اطلاعات به دست آمده از جداول(۲) پرسشنامه‌های تکمیل شده

➡	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T
A	2	2	3	5	2	3	5	2	4	2	3	2	5	2	4	2	3	2	0	2	4	4	3	3	**3**
B	4	4	2	4	4	2	4	4	2	4	5	2	5	4	3	5	5	3	4	4	3	5	4	3	**5**
C	4	5	3	4	5	4	3	5	4	3	4	4	3	4	3	5	4	4	4	3	4	3	4	4	**5**
D	5	4	2	4	2	4	2	5	4	3	3	3	5	3	4	3	4	5	2	5	5	4	3	3	**4**
E	5	4	3	4	3	4	3	3	4	3	3	4	3	4	3	3	4	3	3	4	3	3	3	5	**4**
F	3	4	3	3	3	5	4	3	4	3	4	3	3	4	2	3	3	2	3	2	3	2	2	5	**5**
G	4	3	3	4	3	3	3	5	4	3	4	3	4	3	3	4	3	3	2	2	3	3	4	4	**3**
H	5	5	4	3	4	5	3	4	5	4	4	3	4	5	4	4	5	4	3	4	4	4	4	3	**4**
I	5	4	4	3	5	5	5	4	4	3	3	2	4	3	5	4	3	4	4	3	5	4	4	4	**4**

جدول(۱۲-٤) ادامه‌ی اطلاعات به دست آمده از جداول(۲) پرسشنامه‌های تکمیل شده

➡	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T
A	4	3	2	3	5	4	3	2	2	4	2	3	2	5	2	2	4	3	5	2	2	4	4	3	3
B	3	3	3	4	5	3	5	3	3	3	4	3	2	3	2	4	5	5	2	3	2	3	5	4	2
C	5	4	4	3	5	4	5	4	5	3	4	3	5	4	4	5	3	5	4	3	4	5	4	5	3
D	3	3	2	4	2	2	2	5	3	2	2	3	3	3	4	3	5	3	4	3	2	2	2	3	2
E	4	4	3	3	4	3	4	3	3	4	3	4	3	4	3	4	3	3	4	3	3	4	3	3	3
F	2	3	3	4	3	4	3	4	4	3	5	4	3	3	4	3	4	3	4	3	4	3	3	4	3
G	3	3	4	3	3	4	3	3	3	5	4	3	4	3	4	3	3	4	3	3	4	3	4	3	3
H	5	5	5	5	5	3	3	4	4	3	3	4	4	5	3	4	4	5	4	4	5	3	4	4	4
I	5	5	4	4	3	3	2	4	3	5	4	3	4	4	3	5	4	3	5	5	4	4	3	5	5

جدول زیر مجموع امتیازات داده شده به هر معیار و مقادیر ورودی فازی حاصل از ضرب مجموع امتیازات در مبدل درصد را به خوبی نشان می‌دهد:

جدول(4-13) تعیین مقادیر ورودی‌های فازی

I	H	G	F	E	D	C	B	A	
50	50	50	50	50	50	50	50	50	**تعداد پرسشنامه**
197	203	168	167	173	163	201	178	150	**مجموع**
79	81	67	67	69	٦٥	80	٧١	٦٠	**مقادیر ورودی فازی**

بنابراین، با توجه به جدول(4-13) مقادیر زیر را برای سه معیار برتر خواهیم داشت:

$$A = 60; B = 71; D = 65$$

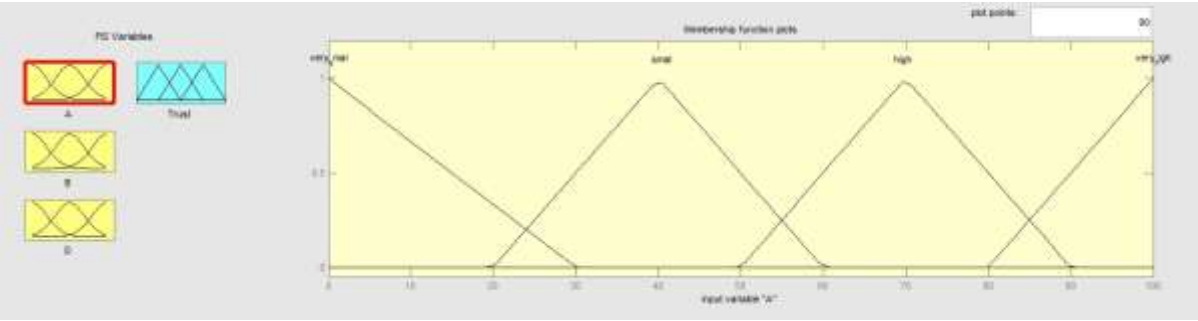
٥-٤. استفاده از منطق فازی

از آنجا که معیارهای برتر هر حوزه به کمک SPSS مشخص شده و میزان اثرگذاری هر کدام از این معیارها بر اعتماد نیز در دسترس می‌باشد لذا به راحتی می‌توان از این مقادیر جهت مقداردهی متغیّرهای ورودی منطق فازی استفاده نمود. جهت این امر مهم، از منطق‌فازی_ممدانی که شامل مراحل فازی‌سازی، پردازش و غیرفازی‌سازی است بهره می‌گیریم.

١-٥-٤. مرحله‌ی فازی‌سازی

مرحله‌ی فازی‌سازی را با جایگذاری معیارهای انتخاب شده به عنوان پارامترهای ورودی آغاز می‌نماییم. نکته‌ی قابل توجه این است که این پارامترها را به عنوان ویژگی‌های امنیتی تعیین شده جهت استفاده در ورودی منطق‌فازی

در نظر گرفته‌ایم. شکل(١-٤) گویای نحوه‌ی چینش ورودی‌ها و خروجی در منطق فازی است.



شکل(۱-٤) پیاده‌سازی ورودی‌ها در منطق فازی و تعیین وضعیت‌های فازی

همانطور که مشاهده می‌شود بازه‌های ورودی بین صفر تا ۱۰۰ هستند. وضعیت‌های فازی برای هر کدام از ویژگی‌های استخراج شده به ترتیب شامل very small، smal، high و very high می‌باشد. کد زیر وضعیت رنج‌بندی هر سه ورودی و خروجی را در منطق فازی به خوبی نشان می‌دهد:

```
[Input1]
Name='A'
Range=[0 100]
NumMFs=4
MF1='very_small':'trimf',[0 0 30]
MF2='small':'trimf',[20 40 60]
MF3='high':'trimf',[50 70 90]
MF4='very_high':'trimf',[80 100 100]

 [Input2]
Name='B'
Range=[0 100]
NumMFs=4
MF1='very_small':'trimf',[0 0 30]
MF2='small':'trimf',[20 40 60]
MF3='high':'trimf',[50 70 90]
MF4='very_high':'trimf',[80 100 100]

 [Input3]
Name='D'
Range=[0 100]
NumMFs=4
MF1='very_small':'trimf',[0 0 30]
MF2='small':'trimf',[20 40 60]
MF3='high':'trimf',[50 70 90]
MF4='very_high':'trimf',[80 100 100]

 [Output1]
Name='Trust'
Range=[0 100]
NumMFs=4
MF1='very_small':'trimf',[0 0 30]
MF2='small':'trimf',[20 40 60]
MF3='high':'trimf',[50 70 90]
MF4='very_high':'trimf',[80 100 100]
```

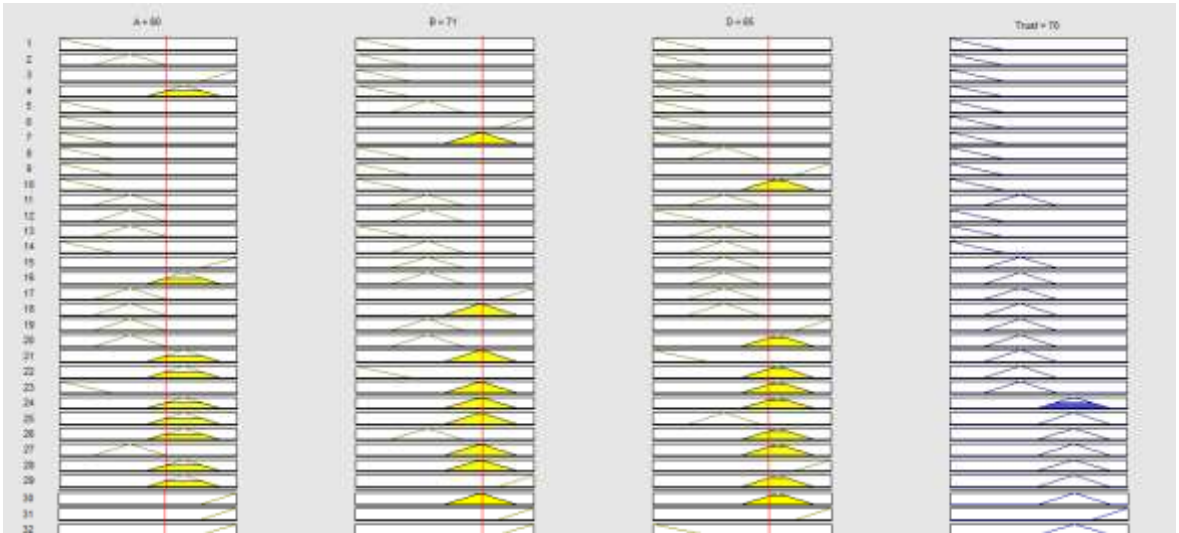
۲-۵-٤. مرحله‌ی پردازش

جهت انجام مرحله‌ی پردازش در منطق فازی، یک سری قوانین با توجه به انتظاراتی که از پاسخ‌دهی سیستم به میزان اعتماد داریم تعیین می‌شود. این قوانین برای سه پارامتر ورودی A,B,D عبارتند از:

(1) If (A is very-small) and (B is very-small) and (D is very-small) then (Trust is very-small)
(2) If (A is small) and (B is very-small) and (D is very-small) then (Trust is very-small)
(3) If (A is very-high) and (B is very-small) and (D is very-small) then (Trust is very-small)
(4) If (A is high) and (B is very-small) and (D is very-small) then (Trust is very-small)
(5) If (A is very-small) and (B is small) and (D is very-small) then (Trust is very-small)

(6) If (A is very-small) and (B is very-high) and (D is very-small) then (Trust is very-small)
(7) If (A is very-small) and (B is high) and (D is very-small) then (Trust is very-small)
(8) If (A is very-small) and (B is very-small) and (D is small) then (Trust is very-small)
(9) If (A is very-small) and (B is very-small) and (D is very-high) then (Trust is very-small)
(10) If (A is very-small) and (B is very-small) and D is high) then (Trust is very-small)
(11) If (A is small) and (B is small) and (D is small) then (Trust is small)
(12) If (A is small) and (B is small) and (D is very-small) then (Trust is very-small)
(13) If (A is small) and (B is very-small) and (D is small) then (Trust is very-small)
(14) If (A is very-small) and (B is small) and (D is small) then (Trust is very-small)
(15) If (A is very-high) and (B is small) and (D is small) then (Trust is small)
(16) If (A is high) and (B is small) and (D is small) then (Trust is small)
(17) If (A is small) and (B is very-high) and (D is small) then (Trust is small)
(18) If (A is small) and (B is high) and (D is small) then (Trust is small)
(19) If (A is small) and (B is small) and (D is very-high) then (Trust is small)
(20) If (A is small) and (B is small) and (D is high) then (Trust is small)
(21) If (A is high) and (B is high) and (D is very-small) then (Trust is small)
(22) If (A is high) and (B is very-small) and (D is high) then (Trust is small)
(23) If (A is very-small) and (B is high) and (D is high) then (Trust is small)
(24) If (A is high) and (B is high) and (D is high) then (Trust is high)
(25) If (A is high) and (B is high) and (D is small) then (Trust is high)
(26) If (A is high) and (B is small) and (D is high) then (Trust is high)
(27) If (A is small) and (B is high) and (D is high) then (Trust is high)
(28) If (A is high) and (B is high) and (D is very-high) then (Trust is high)
(29) If (A is high) and (B is very-high) and (D is high) then (Trust is high)
(30) If (A is very-high) and (B is high) and (D is high) then (Trust is high)
(31) If (A is very-high) and (B is very-high) and (D is very-high) then (Trust is very-high)
(32) If (A is very-high) and (B is very-high) and (D is very-small) then (Trust is high)
(33) If (A is very-high) and (B is very-small) and (D is very-high) then (Trust is high)
(34) If (A is very-small) and (B is very-high) and (D is very-high) then (Trust is high)
(35) If (A is small) and (B is very-high) and (D is very-high) then (Trust is very-high)
(36) If (A is very-high) and (B is small) and (D is very-high) then (Trust is very-high)
(37) If (A is very-high) and (B is very-high) and (D is small) then (Trust is very-high)
(38) If (A is very-high) and (B is very-high) and (D is high) then (Trust is very-high)
(39) If (A is very-high) and (B is high) and (D is very-high) then (Trust is very-high)
(40) If (A is high) and (B is very-high) and (D is very-high) then (Trust is very-high)

شکل (4-2) خروجی حاصل از اجرای قوانین داده شده در منطق فازی را به خوبی نشان می‌دهد.



شکل(۲-٤) خروجی حاصل از اجرای قوانین داده شده در منطق فازی

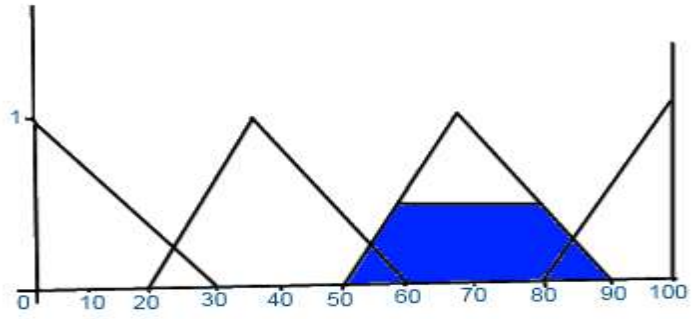
همانطور که مشاهده می‌شود مقادیر ورودی $A = 60$ و $B = 71$ و $D = 65$ بوده و مقدار خروجی آن برابر با 70 می‌باشد که وضعیت فازی اعتماد را در وضعیت زیاد قرار داده است.

۳-۵-٤. مرحله‌ی غیرفازی‌سازی

نکته‌ی قابل توجه این است که مقدار خروجی 70 در شکل(۲-٤) در مرحله‌ی غیرفازی‌سازی به دست آمده است. از آنجا که ما از شکل مثلّثی برای تعیین وضعیت ورودی‌ها و خروجی استفاده نموده‌ایم لذا جهت انجام مرحله‌ی غیرفازی‌سازی، از یکی از قضایای زیر بهره می‌گیریم و تابع عضویت را به راحتی به دست می‌آوریم.

$$\begin{cases} 0 & x < a \\ (x-a)/(b-a) & a \le x \le b \\ (c-x)/(c-b) & b \le x \le c \\ 0 & x > c \end{cases} \qquad (٤-٥)$$

خروجی ما مطابق شکل(۳-٤) است. بنابراین، به این نتیجه خواهیم رسید که تابع عضویت را تنها برای مثلّث رنگی که در این شکل مشخص شده است باید به دست بیاوریم.

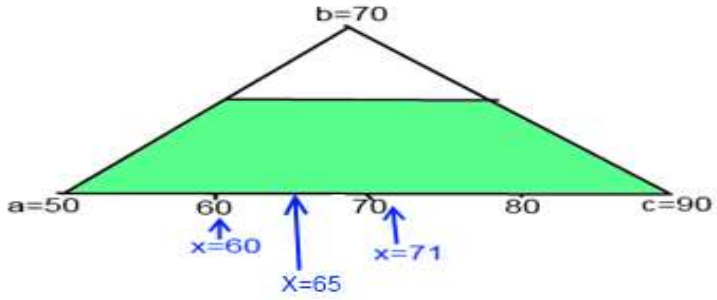


شکل(۳-٤) خروجی منطق فازی

ورودی‌های ما نیز به ترتیب زیر است:

$x = ٦٠.٧١.٦٥$

از آنجا که این سه ورودی متعلّق به مثلّث رنگی خروجی است و تنها به این مثلّث جهت انجام مرحله‌ی غیرفازی‌سازی نیاز داریم لذا این مثلّث را به صورت زیر فرض می‌نماییم که در آن محل قرارگیری ورودی‌ها نیز مشخص شده است:



شکل(٤-٤) محل قرارگیری ورودی‌های فازی در مثلّث خروجی

به کمک شکل(٤-٤)، تابع عضویت هر کدام از xهای مشخص شده را به دست آورده و تابع عضویتی با مقدار مینیمم را بر می‌گزینیم. از آنجا که $x = ٦٠$ در نیمه‌ی اوّل مثلّث مورد نظر قرار گرفته است لذا از قضیه‌ی مربوط به این ناحیه استفاده نموده و تابع عضویت آن را به دست خواهیم آورد:

$(x - a)/(b - a) \qquad a \le x \le b$

$x = ٦٠; \quad a = ٥٠ ; \quad b = ٧٠$

$$\rightarrow \frac{٦٠ - ٥٠}{٧٠ - ٥٠} = \frac{١٠}{٢٠} = ٠/٥$$

$x = ٦٥$ نیز در نیمه‌ی اوّل مثلّث مورد نظر واقع شده است در نتیجه تابع عضویت آن مشابه $x = ٦٠$، به صورت زیر به دست خواهد آمد:

$$(x - a)/(b - a) \qquad a \le x \le b$$
$$x = ٦٥; \quad a = ٥٠; \quad b = ٧٠$$

$$\rightarrow \frac{٦٥ - ٥٠}{٧٠ - ٥٠} = \frac{١٥}{٢٠} = ٠/٧٥$$

اما $x = ٧١$ در نیمه‌ی دوّم مثلّث مورد نظر قرار گرفته است لذا از قضیه‌ی مربوط به این ناحیه استفاده نموده و تابع عضویت آن را به دست خواهیم آورد.

$$(c - x)/(c - b) \qquad b \le x \le c$$
$$x = ٧١; \quad b = ٧٠; \quad c = ٩٠$$

$$\rightarrow \frac{٩٠ - ٧١}{٩٠ - ٧٠} = \frac{١٩}{٢٠} = ٠/٩٥$$

از آنجا که در قوانین منطق فازی از عملگر and استفاده نموده‌ایم، بنابراین تابع عضویتی را انتخاب خواهیم کرد که مقدار مینیمم را دارا باشد. یعنی از بین مقادیر ٠/٥ و ٠/٧٥ و ٠/٩٥ که متعلّق به تابع عضویت است مقدار ٠/٥ را انتخاب می‌نماییم. سپس با استفاده از اعداد متعلّق به بازه‌ی پوشیده شده توسط مثلّث مورد نظر یعنی مجموعه‌ی {٥٠,٦٠,٧٠,٨٠,٩٠ } و همچنین مقدار تابع عضویت تعیین شده، مرحله‌ی غیرفازی‌سازی را به صورت زیر ادامه داده و جواب نهایی را به دست خواهیم آورد.

$$\frac{\left(٥٠ + ٦٠ + ٧٠ + ٨٠ + ٩٠\right) \times ٠/٥}{٠/٥ + ٠/٥ + ٠/٥ + ٠/٥ + ٠/٥} = \frac{١٧٥}{٢/٥} = ٧٠$$

این مقدار همان مقدار خروجی حاصل از منطق فازی است و میزان اعتماد را در وضعیت زیاد قرار می‌دهد.

6-4. نتیجه‌گیری

با توجه به مطالب عنوان شده در این فصل از پژوهش، روش ارزیابی اعتماد پیشنهادی ما مبتنی بر منطق‌فازی است و بر اساس تعریف و توصیف اعتماد، استدلال فازی و ارزیابی روابط اعتماد به روزرسانی و تکامل می‌یابد و مزیت آن نسبت به سایر روش‌های ارزیابی اعتماد این است که به راحتی می‌توان نظرات کاربران را در رابطه

با معیار اعتماد در آن گنجاند و اینکه بازخورد همراه با برداشت انتظارات کاربران واقعی را به کمک افراد خبره ممکن می‌سازد و با تمرکز بر تأثیر دو طرفه‌ی معیارها بر یکدیگر، معیارهای اساسی را شناسایی می‌نماید و اینگونه در برآورد میزان اعتماد، دقت بالایی را به خرج می‌دهد، در حالی که در سایر مدل‌ها این امور، گاهاً به صورت نسبی دنبال شده و یا اصلاً در نظر گرفته نشده است.

کلمات کلیدی فصل چهارم

منطق‌فازی _ممدانی	Fuzzy Logic-mamdani
خیلی کم	very small
کم	smal
زیاد	high
خیلی زیاد	very high
اعتماد	Trust

فصل پنجم:

بحث و نتیجه‌گیری

۵-۱. بحث

مسائل و چالش‌های مربوط به مدل‌های اعتماد ذکر شده در محیط‌های محاسبات ابری را می‌توان به چهار دسته‌ی کلّی تقسیم نمود که عبارتند از:

- ✓ چگونه با توجه با خصوصیات منحصر به فرد محاسبات ابری، اعتماد را تعریف و ارزیابی نماییم.
- ✓ چگونه اطلاعات مخرب توصیه شده را رسیدگی کنیم به این علّت که رابطه‌ی اعتماد در ابرها موقت و پویا است.
- ✓ چگونه سطوح متفاوت امنیتی را با توجه به درجه‌ی اعتماد فراهم کنیم.
- ✓ چگونه تغییرات ارزش اعتماد را با زمان و زمینه‌های مختلف مدیریت نماییم تا منعکس‌کننده‌ی رابطه‌ی اعتماد پویا با زمان و مکان باشد.(سان و همکاران، ۲۰۱۱)

با این تفاسیر، بررسی برخی از مدل‌های اعتماد بر پایه رویکردهای مختلف امری ضروری است، که این بررسی در قالب مقایسه‌ی نوع مدل، نحوه‌ی عملکرد، مزایا و معایب هر کدام از مدل‌های مورد بررسی است. جداول زیر حاوی موارد ذکر شده است.

جدول(۱-۵) مقایسه‌ی مدل‌های اعتماد بر پایه‌ی رویکردهای مختلف نظیر بر پایه‌ی توافق

رویکرد مربوطه	تقسیم بندی	نحوه عملکرد	مزایا	معایب
رویکرد احمد و همکارانش: مدل اعتماد بین تأمین‌کنندگان خدمات و کاربران ابر	بر پایه‌ی توافق	برقرار شدن اعتماد در سه نوبت بین کاربران و تأمین کنندگان ابر	شفاف بودن بین کاربران و تأمین‌کنندگان خدمات ابر	وابسته بودن کاربر به تأمین‌کنندگان خدمات ابر
رویکرد کومار گارگ و همکارانش: مدل مدیریت اعتماد بر اساس کیفیت سرویس در زیرساخت ابر به عنوان یک سرویس	بر پایه‌ی توافق	استفاده از مکانیزم رتبه‌بندی برای ارزیابی سرویس های ابری با استفاده از فرآیند تحلیل سلسله مراتبی	برای مشخصه‌های قابل اندازه‌گیری کیفیت سرویس‌استفاده می‌شود مانند: اطمینان از سرویس،هزینه، کارایی، امنیت و ...	مناسب نبودن برای خصیصه‌های غیرقابل اندازه‌گیری مانند: دسترس‌پذیری، زمان، قابلیت اطمینان و سازگاری عملکرد

جدول(۱-۵) حاوی دو مورد از مدل‌های اعتماد بوده که بر پایه‌ی توافق بنا نهاده شده‌اند و در آنها تأمین‌کنندگان خدمات ابر، سرویس‌های مختلفی را برای کاربران ابر بر اساس توافق‌نامه فراهم می‌کنند. یکی از مشکلات جدی این مدل‌ها، وابستگی کاربران به ارائه‌دهندگان سرویس‌های ابری است.

جدول(۲-۵) مقایسه‌ی مدل‌های اعتماد بر پایه‌ی رویکردهای مختلف نظیر بر پایه‌ی بازخورد و گواهی‌نامه

رویکرد مربوطه	تقسیم بندی	نحوه عملکرد	مزایا	معایب
رویکرد ظفر و همکارانش: مدل اعتماد برای انتخاب تأمین‌کننده‌ی سرویس ابر	برپایه‌ی بازخورد	پیدا کردن تأمین‌کنندگان سرویس ابر قابل اعتماد و کارآمد، بر مبنای عملکرد تأمین‌کنندگان سرویس ابر در یک سال گذشته و بازخوردهای گرفته شده از مشتریان (زمان از کارافتادگی، زمان فعال بودن، پشتیبانی از مشتری، قابلیت تحمل خطا) و مبنای داده‌های گرفته شده از مسئولان قانونگذار	انتخاب راندمان بالا در انتخاب تأمین‌کنندگان سرویس ابر از نظر هزینه، کیفیت سرویس خوب	پر هزینه بودن برای مشتری
رویکرد مانوئل و همکارانش: مدل اعتماد بر اساس معیارهای کیفیت سطح سرویس	بر پایه‌ی گواهی‌نامه	محاسبه‌ی مقدار اعتماد منبع با استفاده از چهار پارامتر: دسترسی‌پذیری و بیانگر قابلیت اطمینان و یکپارچگی داده و کارایی زمان پاسخ	انتخاب بهترین منبع	نادیده گرفتن زمان‌بندی درخواست‌های کاربر
رویکرد لی و همکارانش: مدل چند کاربره قابل اعتماد محاسباتی	بر پایه‌ی توافق	ایجاد یک محیط محاسباتی ابری قابل اعتماد با استفاده از مدل چند کاربره قابل اعتماد محاسباتی	میزبان یا مهمان خاص در داخل ابر IaaS یا PaaS می‌تواند به طور همزمان به چندین دامنه‌ی امنیتی مختلف، چندین موضوع امنیتی مختلف از طریق سیاست‌های امنیتی مختلف تعلّق داشته باشد.	مدیریت همزمان مشتری و تأمین‌کنندگان سرویس ابر

جدول(۲-۵) نیز در ادامه‌ی جدول قبل آورده شده است که در آن یکی از مدل‌ها بر اساس بازخورد عمل می‌نماید. این بازخورد بر مبنای داده‌های گرفته شده از مسئولان قانونگذار و عملکرد تأمین‌کنندگان سرویس ابر در یک سال گذشته و بازخوردهای گرفته شده از مشتریان می‌باشد و یک مدل دیگر نیز بر پایه‌ی گواهی‌نامه بوده و بر اساس گواهی‌نامه‌های قبلی و قابلیت‌های کنونی تأمین‌کنندگان سرویس ابری عمل می‌نماید.

جدول(۳-۵) مقایسه‌ی مدل‌های اعتماد بر پایه‌ی رویکردهای مختلف نظیر بر پایه‌ی دامنه

رویکرد مربوطه	تقسیم بندی	نحوه عملکرد	مزایا	معایب
رویکرد ژیمین و همکارانش: مدل اعتماد مشترک برای فایروال‌ها در رایانش ابری	بر پایه‌ی دامنه	محاسبه‌ی مقدار اعتماد بین گره‌ها بر اساس تبادلات میان گره‌ها، جدول اعتماد، جدول اعتماد درون دامنه‌ای و جدول اعتماد برون دامنه‌ای	۱) برای دامنه‌های مختلف از سیاست‌های امنیتی مختلفی استفاده می‌کند ۲) این مدل ماهیت تراکنش‌ها، داده‌های قدیمی موجودیت‌ها و اثر آنها در اندازه‌گیری پویای مقدار اعتماد را در نظر می‌گیرد ۳) این مدل اعتماد با فایروال سازگار است و سیاست‌های کنترل محلی آن را نقض نمی‌کند.	در نظر نگرفتن این که گره ممکن به چندین دامنه تعلّق داشته باشد و عدم توانایی در نظر گرفتن موضوع تراکنش که یک عامل ضروری در تشخیص مقدار اعتماد است.
رویکرد شن و همکارانش: مدل اعتماد بر اساس پلتفرم قابل اطمینان محاسباتی	بر پایه‌ی توافق	ارزیابی اعتماد توسط یک مقدار اعتماد در مفهوم موجودیت و رفتار تاریخی	برای احراز هویت، دسترسی مبتنی بر قانون و محافظت داده نتایج مثبتی را به همراه دارد.	به علّت پیشرفته شدن پلتفرم‌های محاسباتی، این مدل اعتماد، حمایت کافی برای مقابله با تغییرات سریع پارادایم‌های محاسباتی جدید را فراهم نمی‌کند.

جدول(۳-۵) نیز مانند جداول قبل، حاوی عملکرد چند مدل اعتماد دیگر است، با این تفاوت که یکی از مدل‌ها بر پایه‌ی دامنه عمل می‌نماید. در این مدل، ابر، به تعدادی دامنه‌ی مستقل تقسیم شده و روابط اعتماد بین گره‌ها، به صورت دو دسته‌ی روابط اعتماد درون دامنه‌ای و برون دامنه‌ای در نظر گرفته می‌شود. البته، روابط اعتماد برون دامنه‌ای بر اساس تراکنش‌های عمل شده‌ی درون دامنه‌ای هستند.

طبق نظر بسیاری از پژوهشگران، چالش‌های پیش روی مدل‌های اعتماد موجود شامل موارد زیر است:

۱. عدم تعیین اعتبار بازخوردهای اعتماد به صورت کارآمد: با توجه به پذیرش محاسبات ابری در صنعت، یکی دیگر از چالش‌برانگیزترین مسائل در حال ظهور در محیط‌های محاسبات ابری، تعیین اعتبار بازخوردهای اعتماد و چگونگی اعتماد به این بازخوردها، با توجه به تداول تراکنش‌ها بین سرویس‌گیرنده‌ها و سرویس‌دهنده‌ها می‌باشد که به عنوان یک چالش مهم در مدیریت اعتماد در بین سرویس‌دهندگان و سرویس‌گیرندگان موجود پذیرفته شده است. از یک طرف سیستم‌های مدیریت اعتماد غالباً رفتارهای مخرب را از یکدیگر تجزیه می‌کنند و از طرف دیگر، کیفیت بازخورد اعتماد افراد با یکدیگر متفاوت می‌باشد و بستگی به تجربه‌ی افراد مختلف دارد.(نور و شنگ، ۲۰۱۱)

۲. عدم توجه به بازخوردهای مخرب از طرف بازخورددهندگان: مدیریت بازخورد اعتماد در محیط‌های ابر با توجه به تعداد غیرقابل پیش‌بینی از کاربران ابری و طبیعت بسیار پویای محیط‌های ابری بسیار چالش‌برانگیز می‌باشد. اگر چه به تازگی راه حل‌های مختلفی در جهت مدیریت بازخورد اعتماد مطرح شده است اما چگونگی تعیین اعتبار بازخوردهای ارائه شده، اغلب مورد غفلت قرارگرفته است. به دلیل تراکنش‌های پویای بین سرویس‌های ابری این احتمال وجود دارد که سرویس‌گیرنده‌ی ابری، تراکنش‌های بسیاری با سرویس‌دهندگان یکسانی داشته باشد که منجر به بازخوردهای چندگانه شود. به علاوه، دانستن این موضوع که چه تعداد کاربر ابری با تجربه وجود دارد و این بازخوردهای مخرب از طرف چه کسانی می‌باشد، بسیار مشکل است.(نور و شنگ، ۲۰۱۱)

۳. در نظر گرفتن ارزش یکسان برای تمامی سرویس‌های یک سرویس‌دهنده: در این زمینه در حالی که یک سرویس‌دهنده چندین سرویس مجزا ارائه می‌دهد، به دلیل اثرات منفی اعتماد در یکی از سرویس‌های آن، سایر سرویس‌های آن نیز تحت تأثیر قرار می‌گیرند.

٤. عدم در دسترس بودن خدمات مدیریت اعتماد و سرویس در مواقع عدم اطلاعات: چالش جدی دیگر این مدل‌ها تضمین در دسترس‌بودن خدمات مدیریت اعتماد با توجه به تعداد غیرقابل پیش‌بینی کاربران ابری و طبیعت بسیار پویای محیط‌های ابری می‌باشد.

۵. عدم حمایت مدل‌های اعتماد از تغییرات سریع پارادایم‌های محاسبات ابری: به علّت پیشرفته شدن پلتفرم‌های محاسباتی، ویژگی‌ها و خصوصیات ساختار محاسباتی، پویاتر و غیرقابل پیش‌بینی‌تر شده‌اند. مدل‌های اعتماد موجود حمایت کافی برای مقابله با تغییرات سریع پارادایم‌های محاسباتی جدید را فراهم نمی‌کنند.

٦. فراهم آوردن اطلاعات و توصیه‌های نادرست: فراهم آورندگان اطلاعات می‌توانند، با فراهم آوردن اطلاعات اشتباه و منحرف‌کننده، کاملاً فریب‌دهنده عمل کنند. همچنین موجودیت‌ها در برابر حملاتی

چون توصیه‌های نادرست از طرف عناصر بدخواه و رفتارهای متفاوت این عناصر، در برابر گروه‌های کاربری مختلف آسیب‌پذیر می‌باشند. از طرفی مکانیزم‌های امنیتی سنتی نیز در مقابل این نوع تهدیدها کاملاً ناتوان هستند و از طرف دیگر سیستم‌های شهرت و اعتماد می‌توانند در برابر این نوع تهدیدها، حفاظت ایجاد نمایند.

۷. عدم ایجاد اعتماد پویا: به طور خاص، ایجاد روابط اعتماد بین سرویس‌دهنده و سرویس‌گیرنده در سیستم‌های محاسبات ابری یک موضوع اساسی و چالش برانگیز است. این موضوع به دلیل پویا بودن محیط‌های ابری می‌باشد که چالش‌های بسیاری را برای مدیریت امن و همکاری قابل اعتماد به ارمغان می‌آورد؛ بنابراین، مشکل ایجاد اعتمادهای پویا بین مدیران، بدون داشتن رابطه‌ی اعتماد از قبل، به عنوان تنگنای موجود برای تراکنش می‌باشد.(آباواجی، ۲۰۱۱)

۸. عدم به روزرسانی مقدار اعتماد: چالش بعدی مربوط به این موضوع می‌باشد که در این مدل‌ها هیچ روشی برای به روزرسانی مقدار اعتماد به توصیه‌کنندگان ارائه نشده است. همچنین فرایند تصمیم‌گیری وابسته به کاربر صورت می‌گیرد.

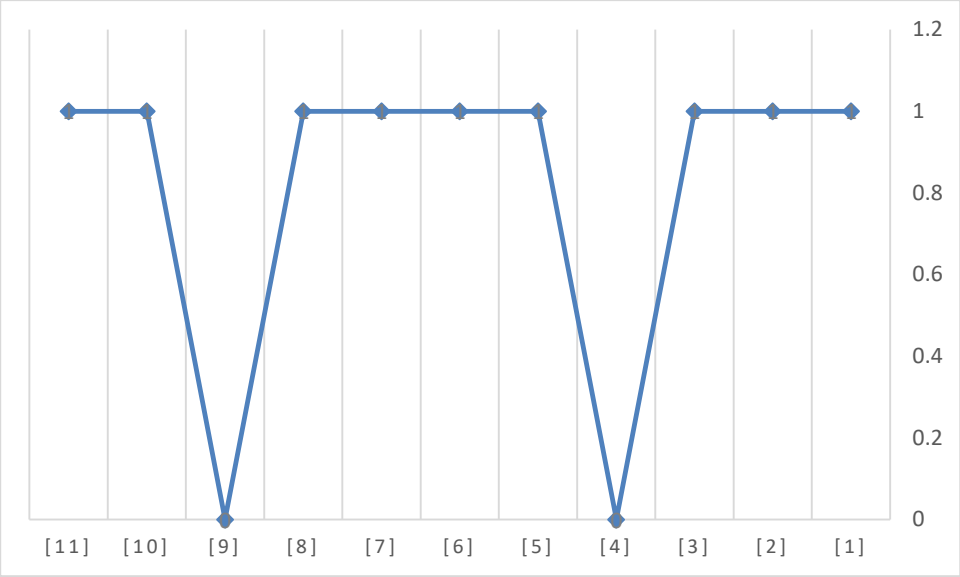
۹. عدم تعریف واحد از اعتماد: از دیگر مشکلات موجود، سردرگمی در تعریف واحدی از اعتماد با وجود ادبیات غنی در زمینه‌های مختلف اعتماد می‌باشد. ازآنجا که اعتماد یک مفهوم ذهنی است، در حال حاضر در بین ادبیات موجود هیچ توافقی در رابطه با تعریف اعتماد و اجزای مدیریت اعتماد موجود نمی‌باشد.(کانیدو و همکاران،۲۰۱۱)

۱۰. نحوه‌ی مدل کردن اعتماد: مدل کردن اعتماد نیازمند حل دو چالش اساسی است. چالش اوّل، نحوه‌ی نمایش و توصیف مقادیر اعتماد و ارائه‌ی تعریفی محاسباتی از آنها است و چالش دوّم، مدیریت اعتماد است که در آن نحوه‌ی جمع‌آوری شواهد و چگونگی ارزیابی ریسک مطرح است.(ریس و همکاران۲۰۰۶)

۱۱. ارزیابی عملکرد مدل‌های اعتماد و عدم تحقق و کاربرد این مدل‌ها: از دیگر مشکلات موجود در مدل‌های ذکر شده بر اساس پیچیدگی ذاتی اعتماد، ذهنی بودن برخی عوامل، دشوار بودن نمایش متنی و اندازه‌گیری اعتماد می‌باشد که به عنوان یکی از چالش‌های مطرح، عنوان می‌شود.(پیرسون، ۲۰۱۳)

از آنجا که مدل پیشنهادی ما یعنی "ارزیابی اعتماد در استفاده از سرویس‌های ابری به کمک منطق‌فازی" در مجموعه‌ی مدل‌های اعتماد سلیقه‌ای قرار گرفته و مدل کردن اعتماد در آن با کمک منطق فازی قابل نمایش و مقادیر آن قابل توصیف و تعریف محاسباتی است و مهمتر از همه اینکه از خبرگان حوزه‌ی رایانش ابری در

جهت برآورد میزان اعتماد بهره می‌جوید، لذا در این مدل پیشنهادی، چالش‌های پیش روی سایر مدل‌ها به طرز چشم‌گیری کاهش می‌یابد. نمودار(۱-۵) گویای تقابل این مدل با یازده چالش ذکر شده‌ی فوق است.



نمودار(۱-۵) مقایسه‌ی مدل پیشنهادی با سایر مدل‌های اعتماد

محور افقی این نمودار، به ترتیب، یازده چالشی که در زمینه‌ی مدل‌های اعتماد در بخش همین فصل ذکر شده است را نشان می‌دهد و محور عمودی آن جهت رفع چالش‌های پیش رو، دارای دو مقدار صفر و یک می‌باشد، که عدد صفر به معنی ضعف در بررسی چالش‌ها بوده و عدد یک قابلیت رفع آنها را نشان می‌دهد. طبق این نمودار، عملکرد مدل پیشنهادی ما در بسیاری از موارد به سمت مقدار یک سوق پیدا می‌کند یعنی قابلیت رفع چالش‌ها را دارا است در حالی که تنها در دو مورد ضعف سایر مدل‌ها را با خود به همراه دارد. با این وجود، یکی از مزایای "ارزیابی اعتماد در استفاده از سرویس‌های ابری به کمک منطق‌فازی" این است که این مدل قابلیت مقیاس‌پذیری را دارا بوده و از آنجا که از افراد خبره‌ی شناخته شده در این حوزه بهره می‌گیریم لذا چالش‌هایی از قبیل وجود بازخوردهای مخرب را نخواهیم داشت. اگر چه در صورت بروز اینگونه رفتار از طرف هر کدام از آنها، به علّت کوچک و قابل شناسایی بودن جامعه‌ی آماری می‌توان در کمترین زمان ممکن این مشکل را برطرف نمود. همچنین به علّت قابلیت به روزرسانی میزان اعتماد در این مدل و قابلیت شناسایی معیارهای اثرگذار برتر با توجه به عملکرد آنها در محیط محاسبات ابری، چالش عدم حمایت مدل‌های اعتماد از تغییرات سریع پارادایم‌های محاسبات ابری را به طرز چشم‌گیری کاهش خواهیم داد. حتی می‌توانیم با تقسیم‌بندی معیارها بر اساس عملکرد یک سرویس از یک سرویس‌دهنده که چندین سرویس‌همزمان ارائه می‌دهد، ارزیابی اعتماد را تنها برای آن سرویس انجام دهیم و سایر سرویس‌ها هیچگونه تأثیری از این ارزیابی

نخواهند پذیرفت. بنابراین در این مدل، عملکرد سرویس‌های ابری و انتظارات کاربران از هر کدام از این سرویس‌ها را در درجه‌ی اول اهمیت قرار داده که این معیارهای مهم را به عنوان بازخورد مفید می‌توانیم در نظر بگیریم. این بازخورد مفید علاوه بر این که باعث افزایش کیفیت سرویس‌دهی می‌شود، تعداد کاربران بیشتری را به خود جذب می‌نماید.

۵-۲. نتیجه‌گیری

امروزه استفاده از سیستم‌های توزیع شده مانند محاسبات ابری در بین کاربران محبوب شده است. در این بین به علّت افزایش چالش‌های موجود در محاسبات ابری، همچنین به علّت ویژگی‌های خاص این محیط‌ها از جمله، پویا بودن، افزایش تعداد ارائه‌دهندگان با قابلیت‌های مشابه، ناهمگن بودن، گسترده بودن این نوع از سرویس‌ها و فراهم نمودن سرویس‌های نادرست و ناکامل از طرف سرویس‌دهندگان، انتخاب سرویس‌دهنده‌ی مناسب از میان سرویس‌های موجود، به یک موضوع پژوهشی بسیار مهم در این حوزه تبدیل شده است.

از این رو قبل از هر چیزی، درک این مشکل در محاسبات ابری که ما نیازمند روش‌هایی مقیاس‌پذیر و پویا در جهت انتخاب سرویس‌دهنده‌ای هستیم که برطرف‌کننده‌ی نیازمندی‌های کیفیتی مورد انتظار کاربر است، امری ضروری می‌باشد. بنابراین این امر مستلزم استفاده از ابزارها و تکنیک‌های صحیح برای جستجوی خدمات مناسب و در دسترس بر روی ابر می‌باشد. در این پژوهش سعی نمودیم که چارچوبی را ارائه دهیم که به کاربران اجازه‌ی ارزیابی و رتبه‌بندی سرویس‌های ابری بر اساس توانایی و عملکردشان در جهت تضمین نیازمندی‌های امنیتی مختلف را دهد. این روش، مقیاس‌پذیر بوده و تنها با تکمیل یک پرسشنامه توسط افراد خبره‌ی هر کدام از حوزه‌های ابری نتیجه‌ی آن قابل برآورد و به روزرسانی است. اگر چه استفاده از افراد خبره در این امر مهم کیفیت عملکرد ارزیابی را بالا برده و باعث کاهش بسیاری از چالش‌ها که سایر مدل‌های اعتماد را تحت تأثیر قرار داده است خواهد شد.

۵-۳. پیشنهادات:

کارهایی که در راستای این تحقیق می‌توان انجام داد عبارتند از:

۱. استفاده از بعد اعتماد غیر امنیت‌گرا در تعیین معیارهای اثرگذار بر اعتماد در سطح محاسبات ابری

۲. استفاده از تلفیق ابعاد اعتماد (امنیت‌گرا، غیر امنیت‌گرا) در تعیین معیارهای اثرگذار بر اعتماد که به نسبت آن معیارهای بیشتری را در برآورد اعتماد در محاسبات ابری می‌توان دخالت داد.

۳. استفاده از تقسیم‌بندی معیارها بر اساس حوزه‌ی فعالیت یک سرویس جهت برآورد میزان اعتماد در آن حوزه‌ی ابری.

منابع و مآخذ

منابع فارسی:

۱. رئوف‌نژاد، زهرا. منطق فازی. مجله‌ی ارتباط‌گستر همراهان. ۱۳۸٦.

۲. رشیدی، احمد. مدلی برای ارزیابی سطح اعتماد کاربران در محاسبات ابری. پایان‌نامه جهت اخذ درجه کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی. دانشکده‌ی فنی مهندسی کامپیوتر، دانشگاه اصفهان. ۱۳۹۱.

۳. طالبی، داوود؛ آرش‌پور، آسیه. ارزیابی عملکرد آموزشی با رویکرد مقایسه‌ای تحلیل شبکه‌ای و دیمتل. دانشگاه شهید بهشتی، ارائه شده در مجله‌ی چشم‌انداز مدیریت صنعتی. شماره ۱۰. ص‌ص ۱۰۰-۸۵. تابستان ۱۳۹۲.

٤. محمدبیگی، ابوالفضل؛ محمدصالحی، نرگس؛ گل، محمدعلی. روایی و پایایی ابزارها و روش‌های مختلف اندازه‌گیری آنها در پژوهش‌های کاربردی در سلامت. مجله دانشگاه علوم پزشکی رفسنجان. دوره ۱۳. اسفند ۱۳۹۳.

۵. مختار، مهران. "مباحث کاربردی و مهم در تحقق یک سیستم هوش مصنوعی". پایان نامه تخصصی هوش مصنوعی، دانشکده ی فنی مهندسی، دانشگاه آزاد اسلامی واحد زاهدشهر، ۱۳۹۰.

٦. مختاری، امیر؛ مجدی، گیتی. نمونه‌گیری: روش‌ها و کاربردها. لِوی، پل؛ لمیشو، استنلی. ترجمه از انگلیسی به فارسی. تهران: پژوهشکده‌ی آمار. ۱۳۸۱.

۷. نوری، مهدی. افزایش اعتماد استفاده از سرویس ها در بستر رایانش ابری. پایان‌نامه جهت دریافت درجه کارشناسی ارشد. دانشکده‌ی فنی و مهندسی کامپیوتر. دانشگاه پیام نور مرکز تهران- واحد ری. بهمن ماه ۱۳۹۰.

منابع لاتین:

1. Abawajy J. "Determining service trustworthiness in intercloud computing environments". in: Proceedings of 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN). 2019; pp. 784–788.
2. Abawajy J. "Establishing Trust in Hybrid Cloud Computing Environments". IEEE 10th International Conference onTrust, Security and Privacy in Computing and Communications. 2018; pp. 118-125.
3. Ahmad Sh, Ahmad B, Saqib S. M and Khattak R. M. "Trust Model: Cloud's Provider and Cloud's User". International Journal of Advanced Science and Technology Vol.44. July 2019.
4. Ahamed S, Sharminb M. "A trust-based secure service discovery (TSSD) model for pervasive computing". journal of Computer Communications, 31(18). 2008; pp. 4281–4293.
5. Alhamad M, et. al. "SLA-Based Trust Model for Cloud Computing". 13th International Conference onNetwork-Based Information Systems (NBiS). 2010; pp. 321- 324.
6. Azzedin F, Maheswaran M. "Toward trust-aware resource management in grid computing systems". Tn cluste computing and the grid. may 2002; pp. 452.
7. Canedo E. D, de Sousa Junior R. F, de Oliveira Albuquerque R And de Mendonca F. L. L. "File Exchange in a Private Cloud supported by a Trust Model". International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover,978-0-7695-4810-4/12,IEEE Computer Society 2012.
8. Canedo E. D, et. al. "Trust Model for File Sharing in Cloud Computing". The Second International Conference on Cloud Computing. 2011; pp. 66-73.
9. Chandrasekar A, Chandrasekar K, Mahadevan M, Varalakshmi P. QoS monitoring and dynamic trust establishment in the cloud". in: Advances in Grid and Pervasive Computing, Springer, Berlin Heidelberg, 2012; pp. 289-301.
10. Dr. Zafar I, Naseer M. K, Jabbar S. "A Novel Trust Model for Selection of Cloud Service Provider". (IEEE 2014).
11. Fan W. J, Yang Sh, Pei J. "A novel two-stage model for cloud service trustworthiness evaluation, Expert Syst". 2013.
12. Fan W. J, Yang Sh. L, Pei J, Perros H. "A Multi-dimensional Trust-aware Cloud Service Selection Mechanism Based on Evidential Reasoning Approach". April 2015; pp. 208–219.
13. Fontela E, Gabus A. "The dematel observer". Battelle Geneva Research Centre. 1976.
14. Garg S. K, Versteeg S and Buyya R. G. "SIM Cloud: A Framework for Comparing and Ranking Cloud Services". in 4th IEEE International Conference in Utility and Cloud Computing. 2013; pp. 210- 218.
15. Grandison T, Sloman M. "Trust management formal techniques and system". ln proceeding of second IFIP conference.2002.
16. Goyal N. K, Aggarwal A, Gupta P, Kumar P. "QoS based trust management model for cloud IaaS". in: Proceedings of Second IEEE International Conference on Parallel Distributed and Grid Computing (PDGC). 2012; pp. 843–847.

17. Guha R, Kumar R, Raghavan P, Tomkins A. "Propagation of trust and distrust". in: Proceedings of the 13th International Conference on World Wide Web, ACM. 2004; pp.403_412.
18. Guo Q, et al. "Modeling and evaluation of trust in cloud computing environments ". (ICACC) 3rd International Conference on Computer Control. 2011; pp. 112-116.
19. Guoyuan L, Danrul W, Yuyul B, Min L. "MTBAC: A Mutual Trust Based Access Control Model in Cloud Computing". Nanjing University. China. April 2014.
20. Gupta P, Goyal M. K, Kumar P and Aggarwal A. "Trust and Reliability Based Scheduling Algorithm for Cloud IaaS". Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing, Lecture Notes in Electrical Engineering Volume 150. 2013; pp 603-607.
21. Habib S. M, Ries Se, Muhlhauser M, Hauke S. "Trust as a facilitator in cloud computing: a survey". Journal of Cloud Computing: Advances, Systems and Applications. Springer 2012.
22. Habib S. M, Ries Se, Muhlhauser M. "Towards a trust management system for cloud computing". in: Proceedings of 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2011; pp. 933–939.
23. Huang J, Nicol D. M. "Trust mechanisms for cloud computing". Journal of Cloud Computing, Advances, Systems and Applications. Springer Open Journal 2013.
24. Hung W. H, et el. "A Combination of AHP and DEMATEL in Evaluating the criteria of Employment Service Dutreach Program Personnel". International Thchnology Journal, 9(13). 2010; PP.569-575.
25. Jia Z, et. al. "A service model based on recommendation trust in pervasive computing environment". International Conference on Pervasive Computing and Applications (ICPCA). 2010; pp. 393- 397.
26. Jøsang A. "A logic for uncertain probabilities". Int. J. Uncertainty, Fuzz. Knowl. 2001; pp. 279-311.
27. Kai X, Zhao L, Shuguo Y. "Research on Secure Frame of Cloud Computing". Computer & Telecommunication .2010.
28. Kanwal A, Masood R, Um E Ghazia U. E, Shibli M. A, Abbasi A. G. "Assessment Criteria for Trust Models in Cloud Computing". IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing. 2013.
29. Ko R. K, Jagadpramana P, Mowbray M, Pearson S, Kirchberg M, Liang Q, Lee B. S. "TrustCloud: a framework for accountability and trust in cloud computing". in: Proceedings of 2011 IEEE World Congress on Services (SERVICES), 2011;pp.584-588.
30. Lang W, Wilkerson J. "Accuracy vs. Validity, Consistency vs. Reliability, and Fairness vs. Absence of Bias: A Call for Quality". Annual Meeting of the American Association of Colleges of Teacher Education (AACTE); New Orleans, LA. 2008**.**
31. Li W, Ping L. "Trust Model to Enhance Security and Interoperability of Cloud environment". the 1st International Conference on Cloud Computing,Vol 5931. 2009; pp: 69-79.
32. Li X, Du J. "Adaptive and attribute-based trust model for service-level agreement guarantee in cloud computing". IET Inform. Secur. 7 (2). 2013; 144-154.

33. Li X, et. al. "A multi-dimensional trust evaluation model for large-scale P2P computing". Journal of Parallel and Distributed Computing,71(6). 2011; pp. 837–847.
34. Li X-Y, Zhou L-T, Shi Y, and Guo Y. "A Trusted Computing Environment Model in Cloud Architecture". Proceedings of the Ninth International Conference on Machine Learning and Cybernetics, 978-1-4244-6526-2. Qingdao, China. July 2010; pp. 11-14.
35. Manuel P. "A trust model of cloud computing based on Quality of Service". DOI 10.1007/s10479-013-1380-x. Springer 2013.
36. Marsh S. P. "Formalising Trust as a Computational Concept". Ph.D.Thesis, University of Stirling.1994.
37. Min Wu. "Cloud Trust Model in E-Commerce". Proceedings of the Second International Symposium on Networking and Network Security (ISNNS ’10). 2010.
38. Mohammed A, Dillon T, Chang E. "SLA-based trust model for cloud computing". in: Proceedings of 2010 13th International Conference on Network-Based Information Systems (NBiS). 2010; pp. 321–324.
39. Muchahari M. K, Sinha S. K. "A new trust management architecture for cloud computing environment". in: Proceedings of 2012 International Symposium on Cloud and Services Computing (ISCOS). 2012; pp. 136–140.
40. Noor T, Sheng Q. "Credibility-Based Trust Management for Services in Cloud Environments". 9th international conference on Service-Oriented Computing,Vol 7084. 2011; pp. 328-343.
41. Noor T, Sheng Q. "Trust as a Service: A Framework for Trust Management in Cloud Environments". Web Information System Engineering, Vol 6997. 2011; pp 314-321.
42. Pearson S, Benameur A. " Privacy, Security and Trust Issues Arising from Cloud Computing". 2nd IEEE International Conference on Cloud Computing Technology and Science. 2010.
43. Pearson S. "Privacy, Security and Trust in Cloud Computing". Conference on Computer Communications and Networks. 2013; pp. 3-42.
44. Polit D. F, Beck C. T. "The content validity index: are you sure you know what's being reported? Critique and recommendations". Research in Nursing & Health 29(5). 2006; pp.489-497.
45. Qin L, et. al. "Evaluation of user behavior trust in cloud computing". International Conference on Computer Application and System Modeling (ICCASM). 2010; pp. 567- 572.
46. Ries s, et. al. "A classification of trust system". OTM workshap(1) , Vol 4277. 2006; pp. 894-903.
47. Robinson Ne, Valeri L, Cave Jo, Starkey T, Graux H, Creese Sa, Hopkins p. "The Cloud: Understanding the Security, Privacy and Trust Challenges". Final Report, Directorate-General Information Society and Media, European Commission 2010.
48. Saaty T. "Theory and Applications of Analytic Network Process". RWS Publications Pittsburgh, vol. 4922. 2005.
49. Shaikh Ri, Dr. Sasikumar M. "Trust Model for Measuring Security Strength of Cloud Computing Service". Elsevier Procedia Comput. 2015; 45:380-389.
50. Shen Zh, Li L, Yan F and Xiaoping Wu Xi. "Cloud Computing System Based on Trusted Computing Platform". Intelligent Computation Technology and Automation (ICICTA), IEEE International Conference on Volume:1. China.2010; pp.942-945.

51. Shyamlal K, Deepak T. "SLA-Aware Trust Model Cloud Service Deployment". International Journal of Computer Applications (0975 – 8887), Volume 90 – No 10. March 2014.
52. Song S, Hwang K. "Fuzzy trust integration for security enforcement in grid computing". in: Proceedings of the Int'l Symposium on Network and Parallel Computing, LNCS 3222, Springer-Verlag, Berlin, 2005; pp.9-21.
53. Sun D, et. al. "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments". Jornal of Procedia Engineering, Vol. 15. 2011; pp. 2852–2856.
54. Wang Y, Vassileva J. "Bayesian network-based trust model". in: Proceedings of IEEE/WIC International Conference on Web Intelligence, 2003; pp. 372–378.
55. Wua Xi, Zhang R, Zeng Bi, yuan Sh. "A trust evaluation model for cloud computing". Procedia Computer Science 17, Information Technology and Quantitative Management (ITQM), Elsivier 2013; pp. 1170-1177.
56. Yan Zh, Zhang p, Vasilakos A. V. "A survey on trust management for Internet of Things". Elsevier Ltd Network and Comput. 2014; 42: 120–134.
57. Yu B, et. al. "Developing trust in large-scale peer-to-peer systems". IEEE First Symposium on Multi-Agent Security and Survivability. 2004; pp. 1-10.
58. Zissis D, Lekkas D. "Addressing cloud computing security issues". jornal of Future Generation Computer Systems, 28(3). 2012; pp 583–592.
59. Zhimin Y, Lixiang Q, Chang L, Chi Y and Guangming W. "A collaborative trust model of firewall-through based on Cloud Computing". Proceedings of the International Conference on Computer Supported Cooperative Work in Design. Shanghai, China. 2010; pp. 329-334.

Abstract:

Trust has attracted a lot of researchers as a solution to enhance security In cloud computing. This category is one of the most important ways to improve the reliability of computing resources provided in the cloud environment and plays an important role in cloud computing environments. Also, trust is one of the main obstacles to the development of cloud computing by the information technology industry, because there is no reliable and cost-effective mechanism for evaluating it. Trust is the estimation of the cloud's ability to complete a work in distributed environments based on credibility, identity, and accessibility, which helps the user to select the appropriate service on the heterogeneous cloud infrastructure.
In this research, we have presented a trust model based on the security criteria measured by cloud computing experts. Simulation results show that our proposed approach, taking into account service quality criteria, selects the most reliable service in the cloud environment, also benefits from similar models.

Keywords: Cloud Computing, Security, Trust, Fuzzy logic.