Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: www.jscit.nit.ac.ir
Volume 7, Number 1, Spring & Summer 2018, pp. 29-41
Received: 2017/09/14; Revised: 2018/09/07; Accepted: 2018/09/29

Cloud Service Selection based on the Credibility persistency of Users' Feedbacks

Mohammad Javad Salehi[1], Mehrdad Ashtiani[2*] and Behrouz Minaei Bidgoli[3]
1- Computer Engineering Department, University of Applied Science & Technology, Tehran, Iran
2*- Computer Engineering Department, Iran University of Science and Technology, Tehran, Iran.
3- Computer Engineering Department, Iran University of Science and Technology, Tehran, Iran.
[1] mj.salehi@uast.ac.ir, [2*] m_ashtiani@iust.ac.ir, and [3] b_minaei@iust.ac.ir

Corresponding author address: Mehrdad Ashtiani, Computer Engineering Department, Iran University of Science and Technology, Tehran, Iran, Post Code: 16846 – 13114.

Abstract- Nowadays, trust is a major topic under discussion in the cloud computing environments. The existence of a mechanism for building and preserving trust among service consumers and providers is a critical component in the success of providing cloud services. Therefore, computational trust in cloud computing environments has turned into a considerable concern. The lack of trust among service providers and consumers may result in the reduction of the general appeal for the acceptance of cloud services among users. In other words, even though the services provided by each vendor maybe similar in terms of functionality, they may vastly differ in terms of quality of service. For this reason, a false choice in selecting a service may have devastating impacts on the requirements and goals of the end-user. To this aim, in this paper, a computational trust model based on the credibility of users' feedbacks for the calculation of services' trustworthiness is introduced. The proposed model, not only takes into account the existing experiences that other users have with a service provider, but also considers the credibility of such feedbacks as well as the persistency of correct and constructive feedbacks through time. In the end, the efficiency of the proposed model is investigated through a series of evaluation scenarios and it is shown that the proposed model is capable of accurately calculating the trustworthiness of the system. Such accuracy is maintained even in the presence of malicious users.

Keywords- Computational trust, Cloud computing, Credibility, Persistency, Feedback.

مجله علمی پژوهشی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: www.jscit.nit.ac.ir
جلد ۷، شماره ۱، فصل بهار و تابستان ۱۳۹۷، صفحه ۲۹-۴۱
دریافت: ۱۳۹۶/۰۶/۲۳، بازنگری: ۱۳۹۷/۰۶/۱۶، پذیرش: ۱۳۹۷/۰۷/۰۷

انتخاب سرویس ابری مبتنی بر پایداری در اعتبار بازخورد کاربران

محمد جواد صالحی[۱]، مهرداد آشتیانی[۲*]، بهروز مینایی بیدگلی[۳]
۱- دانشکده مهندسی کامپیوتر، دانشگاه جامع علمی-کاربردی، تهران، ایران.
*۲- دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران، ایران.
۳- دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران، ایران.
[1] mj.salehi@uast.ac.ir, [2*] m_ashtiani@iust.ac.ir, [3] b_minaei@iust.ac.ir

* نشانی نویسنده مسئول: مهرداد آشتیانی، تهران، خیابان هنگام، دانشگاه علم و صنعت ایران، دانشکده مهندسی کامپیوتر، کد پستی: ۱۳۱۱۴-۱۶۸۴۶

چکیده- امروزه، اعتماد یکی از مهم‌ترین موضوعات مورد بحث در سیستم‌های ابری است. وجود مکانیزمی برای ساخت و حفظ اعتماد بین مصرف‌کننده و فراهم‌کننده خدمات ابری و همچنین میان خود فراهم‌کنندگان ابر، به منظور موفقیت در ارائه سرویس‌های ابری ضروری است. به همین علت، موضوع اعتماد در سیستم‌های ابری به یک نگرانی تبدیل شده است. به طوری که کمبود اعتماد بین مصرف‌کنندگان و فراهم‌کنندگان ابری از مقبولیت همگانی برای پذیرش سرویس‌های ابری خارجی جلوگیری می‌نماید. بنابراین ممکن است سرویس‌های فراهم‌کنندگان از نظر عملکردی مشابه، اما از نظر کیفیت سرویس با یکدیگر تفاوت داشته باشند. از این رو، انتخاب اشتباه ممکن است خسارات جبران ناپذیری را برای کاربر در پی داشته باشد. در این مقاله، یک مدل محاسباتی مبتنی بر اعتبار بازخورد کاربران، به منظور محاسبه اعتماد سرویس‌ها ارائه می‌شود. این مدل علاوه بر تجربیات کاربران از اعتبار کاربران به همراه میزان پایداری بازخوردهای درست آنها استفاده می‌نماید. در انتها، میزان کارایی مدل بررسی شده و ارزیابی‌ها نشان می‌دهد که مدل ارائه شده با وجود کاربران بدخواه، توانسته است اعتماد سیستم را به درستی محاسبه نماید.

واژه‌های کلیدی: اعتماد محاسباتی، محاسبات ابری، اعتبار، سرویس، پایداری بازخورد

۱- مقدمه

سیستم‌های توزیعی مجموعه‌ای از کامپیوترهای مستقل هستند که از دیدگاه کاربران مانند یک سیستم منسجم[۱] و منفرد[۲] عمل می‌کنند. هدف اصلی سیستم‌های توزیعی دسترسی به منابع، شفافیت[۳]، بازبودن[۴] و مقیاس‌پذیری[۵] است[۱]. سیستم‌های ابری دسته‌ای از سیستم‌های توزیعی هستند که دسترسی راحت، فراگیر[۶] و بر حسب تقاضا را از طریق شبکه به یک مخزن مشترک از منابع محاسباتی قابل پیکربندی فراهم می‌کند که این منابع با حداقل تلاش مدیریتی یا تعامل با فراهم‌کننده ابری به سرعت در اختیار گرفته و آزاد می‌شوند[۲, ۳]. بنابراین، سیستم‌های ابری علی‌رغم اینکه مزیت‌های زیادی برای کاربران فراهم کرده است، به همان ترتیب مشکلاتی را برای امنیت اطلاعات و ایجاد اعتماد بین موجودیت‌ها در ابر ایجاد کرده است. بنابراین، حفظ ویژگی‌های سیستم‌های ابری در تمام مکانیزم‌های حریم خصوصی، امنیت و اعتماد سخت و گاهی غیر ممکن است [۴, ۵]. در این بین، اعتماد نقش تعیین‌کننده‌ای را در سیستم‌های توزیعی ایفا کرده و به یکی از چالش‌های مورد توجه سیستم‌های ابری تبدیل شده است[۶-۸]. اعتماد در محیط ابری، معانی، دیدگاه‌ها و ویژگی‌های مختلفی بسته به اهداف مصرف‌کنندگان خواهد داشت. اعتماد را می‌توان به عنوان پیش‌بینی مصرف‌کننده در مورد فعالیت‌هایی که از سایرین انتظار دارد، بیان کرد. پذیرش همگانی استفاده از سیستم‌های ابری مستلزم وجود اعتماد بین مصرف‌کنندگان و فراهم‌کنندگان سرویس ابری

است [۹].

مصرف‌کننده برای دریافت سرویس مورد نظر خود، نیاز به ارزیابی قابلیت اعتماد سرویس ارائه شده توسط فراهم‌کننده دارد. سیستم مدیریت اعتماد یک روش کارآمد برای اطمینان از امنیت، قابلیت اطمینان، هماهنگی برنامه‌های کاربردی و ارزیابی اعتماد است. سیستم‌های مدیریت اعتماد با جمع‌آوری اطلاعات مورد نیاز، یک رابطه اعتماد ایجاد می‌کنند [۱۰]. هدف اصلی سیستم‌های مدیریت اعتماد، کمک به کاربران در تصمیم‌گیری با استفاده از رفتارهای گذشته به عنوان پیش‌بینی‌کننده رفتار احتمالی آینده است[۱۱, ۱۲]. اما آنچه در این مقاله به آن پرداخته خواهد شد، افزایش اعتماد در انتخاب سرویس‌های ابری است. بنابراین، در این زمینه بازخوردهای توزیع شده، ارزش‌گذاری بازخوردها، یکپارچه‌سازی بازخوردها، برآورده‌کردن معیارهای اعتماد مدنظر کاربران و مقابله با بازخوردهای مخرب، چالش‌هایی هستند که سرویس مدیریت اعتماد جهت انتخاب سرویس معتمد باید در نظر بگیرد. به همین دلیل، سرویس‌های مدیریت اعتماد یک رابطه مبتنی بر اعتماد را به گونه‌ای میان فراهم‌کننده و مصرف‌کننده ایجاد می‌نمایند که مصرف‌کننده بدون نیاز به روش‌های پیچیده مقابله با سرویس‌های بدخواه، بتواند سرویس مورد نظر خود را از میان سرویس‌های موجود با اعتماد بیشتری انتخاب نماید. در ادامه این فصل در بخش دوم جایگاه اعتماد در ابر را بررسی می‌نماییم. در بخش سوم، چارچوب مدل پیشنهادی را معرفی خواهیم کرد و در بخش چهارم و پنجم به ترتیب مدل پیشنهادی را ارائه و ارزیابی خواهیم نمود. در انتها و در بخش ششم، جمع‌بندی نتایج به دست آمده از این پژوهش بیان خواهد گردید.

۲- جایگاه اعتماد در محیط‌های محاسبات ابری

با وجود موفقیت اولیه، محبوبیت و در دسترس‌پذیر بودن گستره‌ای از فراهم‌کننده‌های سرویس‌های ابری، خطرات و چالش‌های قابل توجهی این مدل محاسباتی را تهدید می‌کند. فراهم‌کنندگان و توسعه‌دهندگان باید این چالش‌ها و مخاطرات را با استفاده مناسب در نظر بگیرند. این چالش‌ها، همانگونه که در [۱۳, ۱۴] به آن اشاره شده است عبارتند از:

۱. امنیت، حریم خصوصی و اعتماد.

۲. قفل داده‌ها[۷] و استانداردسازی.

۳. در دسترس‌پذیری، تحمل‌پذیری خطا و ترمیم فاجعه[۸].

۴. مدیریت منابع و کارایی مصرف انرژی[۹].

فناوری اینترنت، معماری سرویس‌گرا و الگوی سیستم‌های ابری مزایای بسیار زیادی، برای کاربران برخط به منظور اتصال راحت‌تر به منابع را فراهم کرده است. این در حالی است که ویژگی‌های جدیدی از این فناوری همانند پویا بودن و چنداجاره‌ای[۱۰]، چالش‌هایی را نیز به منظور ایجاد امنیت اطلاعات و اعتماد بین موجودیت‌ها در فضای ابر برای کاربران ایجاد کرده است[۱۵, ۱۶]. امنیت، حریم خصوصی و اعتماد میان فراهم‌کننده و مصرف‌کننده سرویس‌های ابر یکی از مهمترین موضوعات برای رشد این سیستم‌ها محسوب می‌گردد. تجاوز به حریم خصوصی افراد و اختلال در امنیت ابر می‌تواند پیامدهای سنگینی را برای سازمان‌ها و یا سایر موجودیت‌های موجود در ابر ایجاد نماید. در محیط محاسبات ابری می‌بایست امنیت بین فراهم‌کننده و مصرف‌کننده سرویس ایجاد شود. بنابراین، کاربران برای ارتباط با موجودیت‌ها و سایر مولفه‌های موجود نیازی مبنایی به اعتماد خواهند داشت [۱۷]. بنابراین، می‌توان اینگونه بیان کرد که اعتماد، یکی از مهم‌ترین موضوعات برای سیستم‌های پردازش ابری است. همانگونه که در ابتدا ذکر گردید، کاربران برای به‌دست آوردن اعتماد، معمولاً با چالش‌هایی روبرو خواهند بود که نشأت گرفته از پویایی محیط تعامل است. بر اساس تحقیقات انجام شده در [۱]، چالش‌های اصلی سیستم‌های ابری در زمینه ایجاد اعتماد عبارتند از:

۱. زنجیره ترکیبی از اعتماد.

۲. ارزیابی مجدد اعتماد.

۳. شفافیت در برابر ارزیابی اعتماد.

هر زمان که وضعیت زنجیره اعتماد موجودیت‌ها تغییر پیدا کند، همه روابط مربوط به این موجودیت‌ها باید دوباره بر اساس تغییر روابط، تصمیم‌گیری و بروزرسانی شود. به علت ماهیت پویای سیستم‌های توزیعی و همچنین تغییراتی که در سیستم و رفتار موجودیت‌ها ایجاد خواهد شد، ممکن است چندین سازوکار در ارزیابی مجدد اعتماد آغاز شود. به علت اینکه اعتماد موجودیت‌ها از دیدگاه افراد مختلف ممکن است متفاوت باشد، نیاز است اعتماد موجودیت‌ها دوباره ارزیابی گردد. دلیل نیاز به این فرآیند این است که، شخصی می‌تواند امروز مورد اعتماد ما باشد اما با گذشت زمان دیگر مورد اعتماد نباشد. یا ممکن است موجودیتی مورد اعتماد یک شخص خاص باشد اما ازدیدگاه افراد دیگر حاضر در محیط محاسباتی، مورد اعتماد نباشد. بنابراین، کاربران ممکن است زمان زیادی را برای تصمیم‌گیری اعتماد صرف کنند که ممکن است منجر به قطع موقتی خدمات نیز شود.

۳- بررسی کارهای مرتبط

بسیاری از کارهای تحقیقاتی انجام گرفته در حوزه اعتماد، در مورد شناخت، طبقه‌بندی، اعتبارسنجی و کلی‌سازی دلایل مناسب برای تولید اعتماد هستند. این حجم عظیم کار صورت گرفته منتهی به مجموعه وسیعی از طبقه‌بندی‌ها و نوع‌نگاری‌های متفاوت برای حالات مختلف اعتماد شده است. یکی از گسترده‌ترین روش‌های به کار گرفته شده در حوزه اعتماد، استفاده از شبکه‌های بیزی است[۱۹و۲۰]. دلیل این موضوع نیز سادگی و انعطاف‌پذیری بسیار زیاد این ساختار احتمالی برای به دست آوردن میزان اعتماد از روی نشانه‌های آن است. اما اگرچه این روش‌ها دارای زیرساخت قدرتمند ریاضیاتی و احتمالی بوده و امکان تعریف گرافیکی مدل به همراه ساختاری انعطاف‌پذیر را می‌دهند، ولی کاهش مفهوم اعتماد به یک پیشگویی صرف با ذاتی احتمالی و در نظر نگرفتن ذات نسبی اعتماد به خصوص در محاسبه اعتبار نظر کاربران می‌تواند بزرگترین نقاط ضعف این روش‌ها باشد.

معرفی و استفاده از منطق ذهنی[۱۱] را می‌توان یک تغییر بزرگ در ارائه تعاریف صوری از اعتماد دانست. تا پیش از معرفی استفاده از این منطق که به تبع آن منطق فازی نیز مورد استفاده قرار گرفت، اعتماد را به صورت مفهومی عینی[۱۲] مدل‌سازی می‌کردند. در منطق ذهنی، نظرات معمولاً به صورت ω_x^A نشان داده می‌شوند که در آن A مشخص‌کننده فرد دارای نظر و x تعیین‌کننده گزاره‌ای است که نظر در مورد آن داده می‌شود. اگر فرض کنیم که x یک گزاره باشد، یک نظر دودویی در مورد صحت گزاره x به صورت یک چهارتایی $\omega_x = (b, d, u, a)$ نمایش داده می‌شود که در آن b مشخص‌کننده میزان باور، d مشخص‌کننده میزان بی‌اعتقادی، u مشخص‌کننده میزان عدم قطعیت و در نهایت a نیز تعیین‌کننده اعتقاد پایه است که در هنگام نبود مدرک از آن به عنوان باور مبنا استفاده می‌شود[۲۱-۲۳]. مزیت روش‌های مبتنی بر منطق ذهنی در نظر گرفتن ذات فردی، شخصی و غیرقطعی نظرات انسانی و نیز وجود زیرساخت صوری قوی و منطبق بر منطق است. اما قاعده انتقال در این منطق، مفهومی بسیار دانه درشت و انتزاعی است که شرط‌های انتقال اعتماد را در نظر نمی‌گیرد. همچنین، قاعده اجماع نظرات، معمولاً شامل میانگین‌گیری، یا میانگین‌گیری وزن‌دار بوده که در حالت کلی نمی‌تواند نمایش‌دهنده صحیحی از مجموع نظرات باشد.

گونه دیگری از مدل‌ها، مدل‌های مبتنی بر نظریه‌های ریاضیاتی مدرک[۱۳]هستند. نظریه دمپستر- شیفر یک نظریه ریاضیاتی از مدرک است. این نظریه اجازه می‌دهد که مدارک دریافت شده از منابع اطلاعاتی مختلف با یکدیگر ادغام شده و فرد بتواند به درجه مشخصی از اعتقاد نسبت به موضوع برسد (این درجه اعتقاد، توسط یک تابع اعتقاد مشخص خواهد شد که تفاوت‌هایی اساسی با توابع احتمالی و رویکردهای مبتنی بر آن دارد). این نظریه، یک کلی‌سازی از نظریه احتمال بیزی ذهنی است. با این تفاوت که به جای مبتنی بودن بر توابع احتمالی، مبتنی بر توابع باور[۱۴] است که می‌توانند خصوصیت‌های ریاضیاتی توابع احتمالی را نداشته باشند. از کارهای اخیر انجام شده مبتنی بر این نظریه ریاضیاتی می‌توان به [۲۴-۲۶] اشاره کرد. استفاده از توابع باور به جای توابع احتمالی، که نگاشت طبیعی‌تر و منطقی‌تری را میان نظرات پیشنهاددهنده‌ها در حوزه اعتماد و قالب مدل‌سازی ارائه می‌دهد از بزرگترین مزیت این روش‌ها است. همچنین، تجمیع نظرات، به سادگی بر اساس قاعده رایج دمپستر انجام شده و در نظر گرفتن امکان وجود تناقض میان نظرات در این قاعده وجود دارد. اما از سوی دیگر، انتقادات زیادی مبنی بر درست کار نکردن قاعده اجماع دمپستر وجود دارد. به عنوان مثال نتایج نامناسب و غیرشهودی فراوانی در زمانی که ما به باورها به چشم محدودیت نگاه نمی‌کنیم به وجود می‌آید. همچنین به دلیل نرمال‌سازی نظرات متناقض در بسیاری از اوقات نتایج غیر شهودی برای زمانی که تناقضات میان مدارک زیاد است به وجود می‌آید.

از سوی دیگر، منطق فازی توانایی نمایش و تشریح عدم قطعیت و گنگی را به صورتی موثر دارد. همین موضوع باعث می‌شود که منطق فازی کاملاً برای تصمیم‌گیری و استدلال در حوزه اعتماد مفید باشد. استنتاج از طریق منطق فازی بر روی ورودی‌های غیرقطعی، بازه‌ای و کیفی قابل انجام است. تشریح متغیرهای ورودی می‌تواند به وسیله متغیرهای زبانی همانند «خیلی زیاد»، «تقریبا مناسب» و غیره انجام پذیرد. همین موضوع باعث شده است که یکی از گسترده‌ترین کاربردهای منطق فازی در حوزه اعتماد انجام شود. روش‌های بسیار زیاد و متنوعی از انواع روش‌های فازی در حوزه اعتماد به کار بسته شده است [۲۷-۲۹].

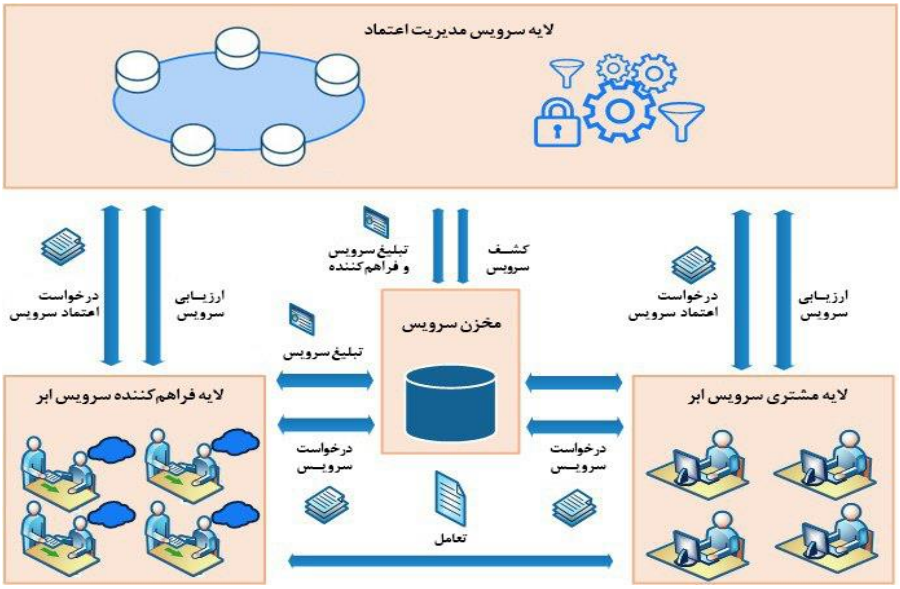
مدل‌های مارکوفی اعتماد نیز بر مبنای مدل‌های احتمالی اعتماد بنا شده‌اند[۳۰-۳۱]. پیشرفتی که مدل‌های مارکوفی به نسبت مدل‌های سنتی احتمالی دارند در پویایی آنها نهفته است. به عبارت بهتر، در مدل‌های سنتی احتمالی معمولاً از یک توزیع احتمالی ثابت (همانند توزیع بتا یا دیریکله) استفاده می‌شود. در حالی‌که مدل‌های مارکوفی، با ارئه چارچوب احتمالی عمومی‌تری نسبت به آن مدل‌ها، می‌توانند رفتار متغیر و پویای نقش‌های اعتماد را مدل‌سازی کنند. در این مدل‌ها، رفتار یک نقش اعتماد p در زمان t توسط حالت مشخصی همانند q_t نمایش داده خواهد شد. اگر p رفتاری پویا از خود نشان دهد از آن حالت به وسیله یک گذر در مدل مارکوفی به حالت دیگری منتقل خواهد شد. به مدل مارکوفی ساخته شده (که

می‌تواند به عنوان مثال، یک مدل مارکوفی عادی یا یک مدل مارکوفی مخفی[15] باشد) مدل تخمینی رفتاری گفته می‌شود. از روی این مدل تخمینی، احتمال تقریبی خروجی حاصل از تعامل با نقش اعتماد محاسبه خواهد شد. استفاده گسترده از مدل‌های مارکوفی در کاربردهای علمی، که نشان از زیرساخت احتمالی قوی و انعطاف-پذیری بالای آن در حوزه‌های مختلف علوم دارد، وجود الگوریتمی کارا برای محاسبه احتمال رخداد وقایع با استفاده از پارامترهای موجود و نیز اضافه کردن پویایی به مدل‌های سنتی احتمالی از بزرگترین مزایای این روش‌ها است. اما از طرف دیگر، خاصیت بی‌حافظه‌گی موجود در مدل‌های مارکوفی چندان با طبیعت اعتماد سازگاری ندارد (فرض این خاصیت در حوزه اعتماد فرضی نه چندان واقعی است). همچنین، همانند همه مدل‌های مبتنی بر احتمال، به مفهوم اعتماد بسیار انتزاعی نگاه می‌کند و آنرا در سطح یک پیش-بینی از تابع توزیع احتمال کاهش می‌دهد و نیز باید در نظر داشت که مدل‌های مارکوف با پارامترهای زیاد، بسیار بزرگ و پیچیده خواهند شد.

۴- چارچوب کلی مدل پیشنهادی

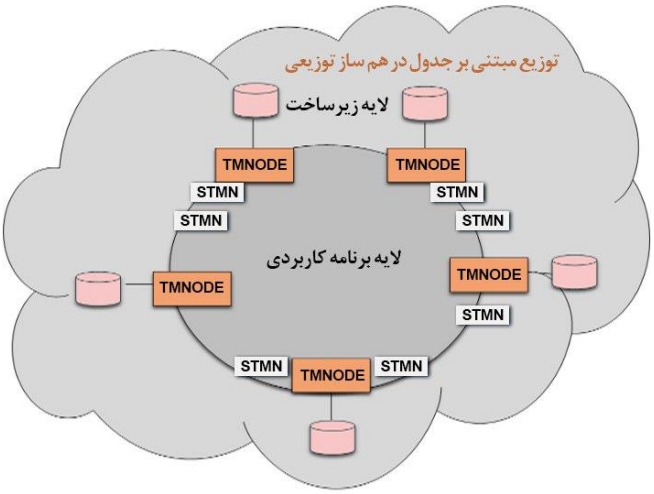
مشابه چارچوب‌های مدیریت اعتماد معرفی شده در [۳۵, ۳۶] در چارچوب ارائه شده در شکل ۱، چهار موجودیت مخزن سرویس[16]، مصرف‌کننده سرویس، فراهم‌کننده سرویس و سرویس مدیریت اعتماد ایفای نقش می‌کنند. مصرف‌کننده سرویس موجودیتی است که سرویس فراهم شده توسط فراهم‌کننده سرویس را استفاده می‌نماید، بنابراین، موجودیتی فراهم‌کننده سرویس تلقی می‌شود که حداقل یک سرویس ارائه نماید. مخزن سرویس مسئول ثبت مشخصات سرویس‌ها است. هر سرویس به محض ورود به سیستم باید در مخزن سرویس ثبت‌نام کند. سپس سرویس مذکور با توجه به نوع عملکردی که دارد در یک اجتماع[17] ذخیره می‌شود. اعضای موجود در اجتماع از نظر عملکرد مشابه هم هستند. سرویس مدیریت اعتماد از یک جدول درهم‌ساز توزیعی[18] استفاده می‌کند. برای همین منظور از زیرساخت‌های موجود در شبکه «پاستری»[۳۴][19]، جهت تخصیص گره‌های موجود در سیستم، استفاده خواهد شد. بدین ترتیب با بهره‌گیری از این الگو، سرویس‌های موجود، در گروه‌هایی که از نظر منطق عملکرد مشابه هم هستند قرار می‌گیرند. این کار سبب می‌گردد، مصرف‌کنندگان هنگامی که تمایل داشته باشند به سرویسی با عملکردی خاص دسترسی داشته باشند، به آن مجموعه مراجعه نموده و از کاوش در دیگر گروه‌ها خودداری کنند.

سرویس مدیریت اعتماد در واقع به عنوان یک دلال[20] در نظر گرفته می‌شود. زمانی که مصرف‌کننده‌ای برای اولین بار نیت استفاده از سرویسی را دارد، لازم است به سرویس مذکور اعتماد داشته باشد. در نتیجه، مصرف‌کننده برای این که سطح اعتماد خود را نسبت به سرویس فوق ارزیابی نماید، می‌تواند از نظارت بر معیارهای اعتماد مدنظر خود و بازخورد مشتریانی که پیش از این با این سرویس یا فراهم‌کننده‌های سرویس تعامل داشته‌اند استفاده نماید. بنابراین، با استفاده از سرویس مدیریت اعتماد می‌توان میزان اعتماد مصرف‌کنندگان با تجربه به فراهم‌کنندگان سرویس را ارزیابی کرد و حاصل این ارزیابی را در اختیار مصرف‌کنندگان سرویس قرارداد. بدین ترتیب مشتریانی که قبلاً از سرویس استفاده کرده‌اند، تجارب خود را از طریق جمع‌آوری تاریخچه فراخوانی به عنوان بازخورد در اختیار سرویس مدیریت اعتماد قرار می‌دهند.



شکل ۱: چارچوب کلی مدل پیشنهادی

سپس، سرویس مدیریت اعتماد از جمع‌بندی این بازخوردها جهت ارزیابی قابلیت اعتماد سرویس مذکور استفاده می‌کند. در انتها، سرویس مدیریت اعتماد در قالب یک سرویس دهنده وب، میزان قابلیت اعتماد را به عنوان یک سرویس به درخواست‌کننده ارسال می‌کند. محل ذخیره سازی ارزیابی‌ها در هر مدلی به معماری که در آن مدل برای سرویس مدیریت اعتماد در نظر گرفته می‌شود وابسته است. در مدل ارائه شده، یک سرویس مدیریت اعتماد با معماری نامتمرکز مبتنی بر جدول درهم‌ساز توزیعی و پروتکل پاستری در نظر گرفته شده است. استفاده از سرویس مدیریت اعتماد متمرکز دارای مشکلاتی مانند وجود یک نقطه شکست، پایین بودن کارایی و وجود گلوگاه بالقوه است. شکل ۲، معماری سرویس مدیریت اعتماد را نشان می‌دهد. در این معماری دو لایه برنامه کاربردی و زیرساخت در نظر گرفته شده است. در لایه برنامه کاربردی هر گره مدیریت اعتماد که به نوعی یک گره پاستری است، نه تنها مسئول ذخیره‌سازی بازخوردهای اعتماد بوده بلکه به عنوان یک همتا در شبکه همتا به همتا[۲۱] برای مسیریابی پیغام‌ها محسوب می‌شود (این گره ها در شکل با عبارت اختصاری TMN نشان داده شده‌اند). سرویس مدیریت اعتماد، با استفاده از توزیع مبتنی بر جدول درهم‌ساز توزیعی، محاسبه اعتماد سرویس‌هایی که بازخوردهای آنها را دریافت می‌کند را بر عهده دارد. به‌این ترتیب که با تقسیم بندی فضای آدرس در میان تعدادی همتا که با هم همکاری می‌کنند و همچنین با تکرار داده‌های ذخیره شده، باعث افزایش ظرفیت و دسترس‌پذیری خواهد شد.



شکل ۲: معماری کلی سیستم مدیریت اعتماد

بدین ترتیب،گره‌های زیر مجموعه یک گره مدیریت اعتماد، عملکردهای مشابه‌ای دارند (این گره‌ها با عبارت اختصاری STMN در شکل نشان داده شده‌اند). با پیروی از اصول پروتکل پاستری، گره‌های مدیریت اعتماد، نسبت به اعضای زیر مجموعه خود دارای شناسه‌ای نزدیکتر به شناسه اجتماع هستند. بنابراین، هر عضو جدید قبل از این که به عضویت گره جدید دربیاید، ابتدا باید در سرویس مدیریت اعتماد ثبت نام کند. به هر یک از گره‌های سرویس مدیریت اعتماد، آدرس IP نسبت داده شده است، که مقدار درهم شده آن، شناسه آن گره را در سیستم مشخص می‌نماید.

۵- مدل پیشنهادی

در این بخش به معرفی مدل پیشنهادی پرداخته می‌شود. به این منظور ابتدا تعاریف مبنایی مورد نیاز مدل آورده شده و سپس به بررسی بخش‌های مختلف مدل پیشنهادی پرداخته می‌شود.

۵-۱- تعاریف مبنایی

تعریف ۱ (فراهم‌کننده سرویس): در مدل ارائه شده فراهم‌کننده سرویس به موجودیتی گفته می‌شود که حداقل یک سرویس ارائه نماید. هر فراهم‌کننده سرویس خود می‌تواند در نقش یک مصرف-کننده سرویس نیز ظاهر شود، بنابراین، هر گره در سیستم می‌تواند مصرف کننده و یا کاربری معمولی باشد.

تعریف ۲ (مصرف‌کننده سرویس): در سیستم، موجودیت‌هایی می‌توانند وجود داشته باشند که هیچ سرویسی ارائه نمی‌دهند. به این افراد مصرف‌کننده سرویس گفته می‌شود. زیرا تنها درخواست سرویس می‌دهند.

تعریف ۳ (مقادیر اولیه اعتماد): یک سرویس به محض ورود به سیستم مقدار اولیه ۰/۵ را به خود می‌گیرد. به این معنی که یک سرویس در ابتدا هم قابل اعتماد و هم غیرقابل اعتماد است.

تعریف ۴ (زمان ارائه بازخورد): کاربران ممکن است در پاسخ به مصرف‌کننده زمان‌های متفاوتی را برای بازخوردهایشان داشته باشند. به بازخوردهای نزدیک به زمان ارزیابی، امتیاز بیشتری داده خواهد شد. بازخوردهایی که از یک بازه زمانی خاص به بعد ارسال می شوند در ارزیابی سرویس اعمال نمی‌گردند.

تعریف ۵ (اعتماد مستقیم): چنانچه کاربری تجربه استفاده از سرویس را داشته باشد، اعتماد مستقیم $Trust_{direct}$ گفته می شود. بنابراین، سرویس مدیریت اعتماد، درخواست را به گره پاستری که مسئول آن اجتماع است ارسال می‌کند. آنگاه گره پاستری موظف است تمامی رکوردهایی را که مربوط به اجتماع مشخص شده هستند و کاربر درخواست کننده آن‌ها را مورد ارزیابی قرار داده است را استخراج نماید. در صورتی‌که کاربر درخواست‌کننده بیش از یک بار سرویسی را ارزیابی کرده باشد، باید نتایج ارزیابی آن در مورد هر سرویس در هم ادغام شود. اعتماد مستقیم در مدل معرفی شده بر

اساس فرمول ۱ مورد محاسبه قرار می‌گیرد.

$$\mathrm{Trust}_{\mathrm{direct}}=\frac{\sum_{i=1}^{|v(m)|} Q_i\_Weight\times Q_i\_Rate}{\sum_{i=1}^{|v(m)|} Q_i\_Weight}\times e^{-\Delta t} \quad (۱)$$

که در آن $|v(m)|$ تعداد پارامترهای دخیل در ارزیابی است. همچنین، Q_i_Weight وزن پارامتر i ام دخیل در ارزیابی و Q_i_Rate نرخ ارزیابی کاربر از پارامتر i ام دخیل در ارزیابی است. اگر در گذشته سرویسی ارزیابی شده است، احتمال تغییر کیفیت سرویس آن وجود دارد. لذا برای بروزرسانی ارزیابی‌های کاربر در طول زمان، از پارامتر $e^{-\Delta t}$ استفاده می‌شود.

تعریف ۶ (اعتماد غیر مستقیم): چنانچه کاربر تجربه استفاده مستقیم از سرویس را نداشته باشد، تجربه غیر مستقیم $\mathrm{Trust}_{\mathrm{indirect}}$ گفته می‌شود. به منظورمحاسبه اعتماد غیر مستقیم همانند مراحلی که برای ارزیابی اعتماد مستقیم صورت گرفته است، باید تمامی سرویس‌هایی که مد نظر کاربر و مربوط به یک اجتماع خاص است استخراج شوند. بنابراین، درخواست به گره پاستری مسئول اجتماع ارسال خواهد شد. به منظور محاسبه اعتماد غیرمستقیم در مدل معرفی شده از فرمول ۲ که در زیر آورده شده است استفاده خواهد شد.

$$\mathrm{Trust}_{\mathrm{indirect}}=\frac{\sum_{i=1}^{|v(u)|} \mathrm{Worth}_i\times \mathrm{Cr}_i\times \mathrm{Feedback\_Agr}_i}{\sum_{i=1}^{|v(u)|} \mathrm{Worth}_i\times Cr_i} \quad (۲)$$

که در آن $|v(u)|$ تعداد کاربران مجزایی است که سرویس مورد نظر را ارزیابی کرده‌اند. پارامتر Cr_i میزان اعتبار کاربر i است و $\mathrm{Feedback\_Agr}_i$ میزان بازخوردهای ادغام شده کاربر i در ارزیابی سرویس مورد نظر است. پارامتر Worth_i ارزش بازخورد کاربر i است، که مقدارش متناسب با ارائه بازخوردهای مثبت و منفی، افزایش و کاهش پیدا می‌کند. مقدار Worth_i از رابطه ۳ به دست می‌آید. در مدل پیشنهادی به بازخوردهای منفی (بازخوردهایی که مقدارشان از مقدار خنثی ۰/۵ کمتر باشد)، ارزش بالاتری نسبت داده می‌شود.

$$\mathrm{worth}=\begin{cases}\mathrm{pos}=+0.3,\ \mathrm{total}_{\mathrm{pos}}=+\mathrm{pos}, & \textbf{if (feedback = positive) and (flag = positive)}\\ \mathrm{pos}=+0.1,\ \mathrm{total}_{\mathrm{pos}}=+\mathrm{pos}, & \textbf{if (feedback = positive) and (flag = negative)}\\ \mathrm{neg}=+0.4,\ \mathrm{total}_{\mathrm{neg}}=+\mathrm{neg}, & \textbf{if (feedback = negative) and (flag = negative)}\\ \mathrm{neg}=+0.2,\ \mathrm{total}_{\mathrm{neg}}=+\mathrm{neg}, & \textbf{if (feedback = negative) and (flag = negative)}\end{cases}$$

$$\mathrm{worth}=\mathrm{total}_{\mathrm{neg}}-\mathrm{total}_{\mathrm{pos}} \quad (۳)$$

بنابراین، سیاست‌هایی که در نحوه محاسبه اعتماد غیر مستقیم در نظر خواهیم گرفت از قرار زیر است:

۱. چنانچه کاربر، سرویسی را چندین بار مورد ارزیابی قرار دهد نیازمند این است که بازخوردهای ارسال شده با یکدیگر ادغام شوند.

۲. بازخوردهای ارسالی ممکن است توسط کاربران و فراهم کنندگانی ارسال شده باشد که درجه اعتبار متفاوتی دارند. بنابراین، بازخوردهای ارسالی متناسب با اعتبار کاربر ارزیابی می‌شوند.

۳. میزان همکاری موفق و ناموفق را باید در ارزش بازخوردها لحاظ نمود. به این ترتیب که هرکدام از بازخوردهای مثبت دنباله‌دار و بازخوردهای منفی دنباله‌دار، بیانگر تداوم در ارائه یک رویکرد هستند و باید مقدار به دست آمده در ارزش بازخوردهای کاربر لحاظ شود.

۴. در ارزیابی‌های غیرمستقیم باید این نکته را مدنظر داشت که کاربر i نباید همان کاربری باشد که دارای تجربه اعتماد مستقیم است.

در مدل ارائه شده سه پارامتر مهم جهت ارزیابی بازخوردها در نظر گرفته شده است. پارامتر $\mathrm{Med}_{\mathrm{time}}$ به عنوان یک بازه زمانی نزدیک به زمان ارزیابی، جهت افزایش اعتبار بازخوردهای رسیده و جلوگیری از اعمال بازخوردهای قدیمی در ارزش‌دهی سرویس، در نظر گرفته شده است. در صورتی که تعداد کاربران مجزایی که سرویس مورد نظر را ارزیابی می‌کنند کم باشد، مثلاً سرویسی به تازگی شروع به کار کرده و نسبتاً ناشناخته به حساب می آید، نیاز است که این سرویس توسط کاربران مجزایی، مورد ارزیابی قرارگیرد.

بنابراین، به همین منظور پارامتر $\mathrm{Med}_{\mathrm{difuser}}$ در نظر گرفته شده است.

از طرف دیگر، در صورتی که تعداد بازخوردهای رسیده از حد معمول کمتر باشد، اعتماد کافی برای ارزیابی اعتماد سرویس مورد نظر وجود ندارد. پس برای ارزیابی سرویس مورد نظر، نیاز است که چندین مرتبه، سرویس مد نظر مورد ارزیابی قرار گرفته شده باشد. پارامتر $\mathrm{Med}_{\mathrm{feedback}}$ به عنوان تعداد بازخوردهای رسیده شده در نظر گرفته شده است. همچنین w_1، w_2 و w_3 وزن اهمیت هر کدام از این سه پارامتر را مشخص می‌کند که در مدل پیشنهادی این سه به ترتیب معادل ۰/۴،۰/۳ و ۰/۳ مقداردهی شده‌اند. میزان اولویت بازخورد دریافت شده با P نمایش داده شده که مطابق فرمول ۴ محاسبه می‌شود.

$$P=w_1 \times \mathrm{Med}_{\mathrm{time}} + w_2 \times \mathrm{Med}_{\mathrm{difuser}} + w_3 \times \mathrm{Med}_{\mathrm{feedback}} \quad (۴)$$

بنابراین، برای محاسبه اعتماد غیرمستقیم کلی به یک ارائه‌دهنده سرویس خواهیم داشت:

$$\mathrm{Total\_Trust}_{\mathrm{indirect}} = \mathrm{Trust}_{\mathrm{indirect}} \times p + \mathrm{Reputation} \times (1-p) \quad (۵)$$

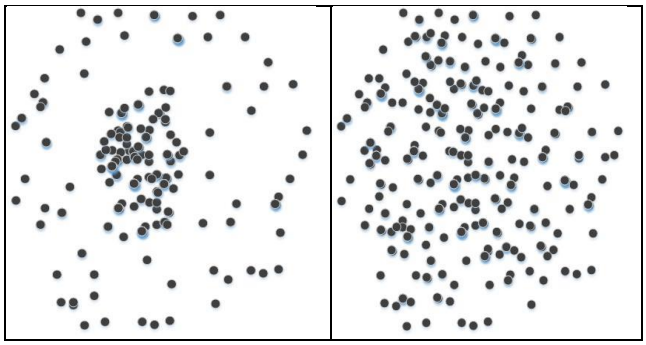
اعتماد یک سرویس، جمع وزن‌داری از تجربه‌های مستقیم خود کاربر و تجربه‌های غیرمستقیم سایر کاربرانی است که در گذشته از سرویس استفاده نموده‌اند. در نتیجه کاربر می‌تواند وزن اهمیت هریک از تجربه‌های مستقیم و غیرمستقیم را در درخواست خود تنظیم نماید و یا از مقدار پیش فرض آن استفاده نماید. این موضوع در فرمول ۶ نمایش داده شده است.

$$\mathrm{Trust}_{\mathrm{service}} = \mathrm{Trust}_{\mathrm{direct}} \times w_{\mathrm{Direct}} + \mathrm{Trust}_{\mathrm{indirect}} \times w_{\mathrm{Indirect}} \quad (۶)$$

بازخوردهایی که توسط فراهم‌کنندگان مختلف برای یک سرویس خاص ارسال می‌شود ممکن است در یک بازه زمانی مشخص اتفاق افتاده باشد و هرکدام از ارسال‌کنندگان در مورد سرویس تجربه خاصی داشته باشند. میزان تفاوت و فاصله بازخوردها از یکدیگر نماینگر تفاوت دیدگاه‌های مختلف خواهد بود که می‌تواند نشانه‌ای برای بدخواه بودن ارسال‌کنندگان بازخورد باشد. همچنین، بازخوردهای دریافتی ممکن است به یکدیگر نزدیک و یا پراکنده باشند. بنابراین، میزان نزدیکی بازخوردها بیانگر این مطلب خواهد بود که دیدگاه‌های کاربران به یکدیگر نزدیک است. اما از سوی دیگر چنانچه فاصله بازخوردهای موجود از حد مشخصی بیشتر باشد، کاربر به دلیل تفاوت در دیدگاه‌های مختلف به سرویس مورد نظر اعتماد کمتری می‌نماید. بنابراین، می‌توان اینگونه بیان کرد که کیفیت سرویسی که فراهم‌کننده سرویس در بازه‌های زمانی مختلف و برای کاربران مختلف ارسال می‌نماید، نقش بسیار مهمی در تعیین سرویس باکیفیت دارد. در نتیجه، همانطور که در رابطه ۷ نشان داده شده است، برای بدست آوردن میزان پراکندگی بازخوردها، از جذر مثبت واریانس S^2 استفاده می‌کنیم.

$$\partial=\sqrt{S^2} \quad (۷)$$

به منظور بررسی اعتبار کاربران، منوط به نوع پراکندگی بازخوردها، از دو معیار نظر اکثریت و نظر میانه بازخوردها استفاده خواهد شد. به این ترتیب که هرچه بازخورد ارسالی کاربران به معیار نظر اکثریت و یا معیارنظر میانه نزدیکتر باشد میزان اعتبار آنها بیشتر است. شمای کلی این دو معیار در شکل ۳ نمایش داده شده است.



شکل ۳: شمای کلی پراکندگی بازخوردها در روش نظر اکثریت (شکل راست) و روش نظر میانه (شکل چپ)

در روش نظر اکثریت، جهت ارزیابی میزان اعتبار کاربر نه تنها تمامی سرویس‌هایی که کاربر آنها را ارزیابی کرده است در نظر گرفته می‌شود، بلکه میزان اهمیت هر کدام از سرویس‌ها نیز در نظر گرفته خواهد شد. به این دلیل تمامی سرویس‌ها به همراه میزان اهمیت هر یک در نظر گرفته می‌شود. این کار به این دلیل است که از فعالیت افرادی که نیت تبانی دارند و بخواهند با اهداف مخرب نظر اکثریت را تحت تاثیر قرار دهند، جلوگیری شود. بنابراین، در این روش اعتبار کاربران بیش از اندازه کاهش پیدا نمی‌کند. به همین ترتیب کاربران نمی توانند با ارسال بازخوردهای صحیح در مورد سرویس‌های کم اهمیت میزان اعتبار خود را افزایش دهند. در محاسبه نظر اکثریت، به بازخوردهای ارسالی هر کاربر به میزان اعتبار آن اهمیت داده شده و در این محاسبات تنها بازخورد ارسالی کاربر در نظر گرفته نمی شود.

در روش نظر میانه جهت ارزیابی اعتبار کاربر، تنها تعداد محدودی از کاربران مورد توجه قرار خواهند گرفت. همانطور که توضیح داده شد، انتخاب این کاربران از میان آن دسته از ارسال‌کنندگان بازخوردی هستند که دیدگاهی نزدیک به هم دارند. این انتخاب بر اساس تعداد بازخوردهای ارسالی خواهد بود. در نتیجه هرچه تعداد

ارسال‌کنندگان بازخورد زیاد باشد، به نسبت آن کاربران انتخاب شده، جهت استفاده در روش میانه زیاد خواهند شد. در روش نظر اکثریت به علت این که بازخوردها به هم نزدیک هستند، همه بازخوردها در نظر گرفته می‌شوند اما در روش نظر میانه، به دلیل اینکه بازخوردهای ارسالی پراکنده هستند و ممکن است با هدف ضربه زدن ارسال شده باشند، تنها تعداد محدودی از کاربران انتخاب خواهند شد. در محاسبه نظر کاربران، به بازخوردهای ارسالی هر کاربر به میزان اعتبار آن اهمیت داده می‌شود، و در این محاسبات تنها بازخورد ارسالی کاربر در نظر گرفته نمی شود. رابطه زیر روش محاسبه نظر کاربران را نشان می‌دهد.

$$M = \frac{\sum_{i=1}^{|v(n)|} Cr_i \times Feedback\_Agr_i}{\sum_{i=1}^{|v(n)|} Cr_i} \qquad (۸)$$

که در آن $|v(n)|$ تعداد سرویس‌های مجزایی است که توسط کاربر مورد ارزیابی قرار گرفته است، Cr_i اعتبار کاربران، و $Feedback\_Agr_i$ مجموع بازخوردهایی است که یک کاربر در خصوص یک سرویس ارسال می‌کند. پس از به دست آوردن میانه یا میانگین نیاز است فاصله نظر کاربر از این مقادیر به دست آید. چنانچه فاصله بازخورد کاربر با مقادیر مذکور زیاد باشد، از اعتبار کاربر کاسته خواهد شد و در ارزیابی سرویس تاثیر کمتری خواهد گذاشت. فاصله بازخورد کاربر از نظر سایر کاربران، از رابطه ۹ به دست می‌آید.

$$Distance_{feedback} = 1 - \frac{\sqrt{\sum_{j=1}^{|v(n)|} w_j \times (F_{ij} - M_j)^2}}{\sum_{j=1}^{|v(n)|} w_j} \qquad (۹)$$

که در آن $|v(n)|$ تعداد سرویس‌های مجزایی است که تا به حال کاربر آنها را ارزیابی کرده است. پارامتر F_{ij} بازخورد ارسالی کاربر i به سرویس j است و M_j معیار انتخاب کاربران در مورد سرویس j است. همچنین، w_j وزن اهمیت هر سرویس را نشان می‌دهد. کاربران در ابتدا مقدار اعتبار برابر ۰/۵ خواهند داشت.

یکی دیگر از پارامترهای تاثیرگذار در بحث اعتبار کاربران، پارامتر پایداری است. پایداری کاربران در سیستم نشان‌دهنده میزان تداوم کاربر در ارسال درست و یا نادرست بازخوردهایش است. هر چه تعداد بازخوردهای کاربر صحیح باشد، میزان پایداری کاربر بیشتر است و به همین ترتیب هرچه کاربر در ارائه بازخورد، نوسان داشته باشد، پایداری کمتری دارد. بنابراین در این پارامتر، چنانچه کاربری در ارائه بازخورد مثبت مسیر یکنواختی را طی نکند از اعتبارش کاسته می‌شود؛ چنین کاربرانی از اعتبار کافی برخوردار نخواهند بود و در نتیجه میزان تاثیرپذیری آنها در سیستم کم خواهد شد. فرمول‌بندی این پارامتر در رابطه ۱۰ نمایش داده شده است.

$$\text{persistence} = \begin{cases} \text{i} = +0.1\ , \text{j} = -0.1, \\ \text{total}_{pos} = \dfrac{\text{total}_{pos} + (\text{w} \times \text{i})}{2}\ , \text{total}_{neg} = \dfrac{\text{total}_{neg} + (\text{w} \times \text{j})}{2}, \\ \textbf{if}(\text{feedback} = \text{positive}) \\ \text{and}\ \ (\text{flag} = \text{positive}) \\ \\ \text{i} = \text{i} + 0.1, \text{flag} = \text{positive}, \\ \text{total}_{pos} = \dfrac{\text{total}_{pos} + (\text{w} \times \text{i})}{2}, \text{total}_{neg} = \dfrac{\text{total}_{neg} + (\text{w} \times \text{j})}{2}, \\ \textbf{if}\ (\text{feedback} = \text{positive}) \\ \text{and}\ \ (\text{flag} = \text{negative}) \\ \\ \text{j} = \text{j} + 0.1, \text{i} = \text{i} - 0.1, \\ \text{total}_{neg} = \dfrac{\text{total}_{neg} + (\text{w} \times \text{j})}{2}, \text{total}_{pos} = \dfrac{\text{total}_{pos} + (\text{w} \times \text{i})}{2}, \\ \textbf{if}\ (\text{feedback} = \text{negative}) \\ \text{and}\ \ (\text{flag} = \text{negative}) \\ \\ \text{j} = +0.2, \text{flag} = \text{negative}, \\ \text{total}_{neg} = \dfrac{\text{total}_{neg} + (\text{w} \times \text{j})}{2}, \text{total}_{pos} = \dfrac{\text{total}_{pos} + (\text{w} \times \text{i})}{2}, \\ \textbf{if}(\text{feedback} = \text{negative}) \\ \text{and}\ \ (\text{flag} = \text{positive}) \end{cases}$$

$$\text{persistence}_{feedback} = \text{total}_{neg} - \text{total}_{pos} \qquad (۱۰)$$

در نهایت میزان اعتبار کاربران از رابطه زیر به دست خواهد آمد:

$$Cr_i = \frac{(\alpha \times \text{persistence}_{feedback}) + (\beta \times \text{Distance}_{feedback})}{(\alpha + \beta)} \qquad (۱۱)$$

پارامترهای α و β بیانگر میزان اهمیت هرکدام از معیارهای پایداری بازخوردها و فاصله بازخوردها هستند. چنانچه بازخوردهای ارسالی کاربر زیاد باشد، مقدار α بیشتر و چنانچه بازخوردهای ارسالی کاربر کم باشد مقدار β بیشتر خواهد شد. لذا به منظور تعیین مقدار پارامترهای α و β، یک مقدار آستانه برای بازخوردها تعیین خواهد شد. این مقدار آستانه منطبق بر رابطه ۱۲ و به صورت زیر محاسبه خواهد شد.

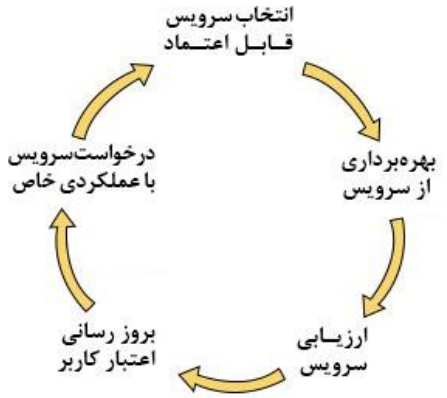
$$\text{balance} = \begin{cases} \alpha = 0/6، \beta = 0/4, & \textbf{if threshold} < \dfrac{\text{total}_{feedback}}{2} \\ \alpha = 0/4، \beta = 0/6, & \textbf{if threshold} \geq \dfrac{\text{total}_{feedback}}{2} \end{cases} \qquad (۱۲)$$

۶- ارزیابی مدل پیشنهادی

در این بخش به ارزیابی مدل پیشنهادی پرداخته می‌شود. به همین منظور ابتدا پیکربندی کلی ارزیابی‌های انجام شده در بخش ۵-۱ معرفی شده و سپس به بررسی نتایج پرداخته می‌شود.

۱-۶- پیکربندی ارزیابی‌های انجام شده

به منظور ارزیابی مدل اعتماد جهت انتخاب سرویس، ابتدا به شبیه سازی این محیط پرداخته شده است. رفتار کاربران، حالت ارائه دهندگان و مصرف‌کنندگان سرویس و نیز دسته‌بندی سرویس‌ها برمبنای سناریوی مرجع معرفی شده در کارهای مرتبطی همانند [۳۸] در نظر گرفته شده است. محیط شبیه‌سازی شده شامل فراهم‌کننده سرویس، سرویس‌ها و کاربران است. در این شبیه‌سازی ۲۰۰ گره در نظر گرفته شده است. ۲۰ درصد این گره‌ها تنها نقش مصرف‌کننده را در این شبیه‌سازی ایفا می‌نمایند و مابقی گره‌ها هر دو نقش مصرف‌کننده و فراهم‌کننده سرویس را دارا هستند. همچنین ۱۶۰ سرویس در نظر گرفته شده است. شکل ۴ روند کلی شبیه‌سازی را نشان می‌دهد.



شکل ۴: روند کلی درخواست سرویس در مدل پیشنهادی

کلیه شبیه‌سازی‌های انجام گرفته با استفاده از نرم‌افزار NetLogo که یک چارچوب شبیه‌سازی عامل-مبنا است پیاده‌سازی گردیده است. در این ارزیابی فرض می‌شود بازخورد کاربران در یک محیط بسته رخ می‌دهد و کاربرانی که در مخزن سرویس ثبت نام نشده‌اند تأثیری در نتیجه ارزیابی نخواهند داشت. همچنین، مقادیر در نظر گرفته شده برای دسته بندی‌ها و حالت‌ها به صورت موردی است و هیچ پیش فرضی در مورد مقادیر این پارامترها وجود ندارد. بنابراین، اعتماد کاربران بر اساس اطلاعاتی که در مخزن سرویس و سیستم مدیریت اعتماد ذخیره شده است محاسبه می‌گردد. اجرای شبیه-سازی برای ۲۰۰۰ تراکنش صورت گرفته است. به منظور انجام شبیه‌سازی، سرویس‌ها و فراهم‌کنندگان سرویس به ۵ دسته تقسیم شده‌اند. این تقسیم‌بندی بر اساس رفتارهای مختلف فراهم‌کنندگان سرویس صورت گرفته است. رفتار هر کدام از سرویس‌ها و یا فراهم کنندگان نمایانگر رفتار حقیقی سرویس‌ها است و براساس آن‌ها ارزیابی صورت خواهد پذیرفت. این سرویس‌ها شامل *سرویس‌های همواره خوب*، *سرویس‌های همواره بد*، *سرویس‌های ابتدا ضعیف و سپس خوب*، *سرویس‌های ابتدا خوب سپس ضعیف* و *سرویس‌های متغییر* است.

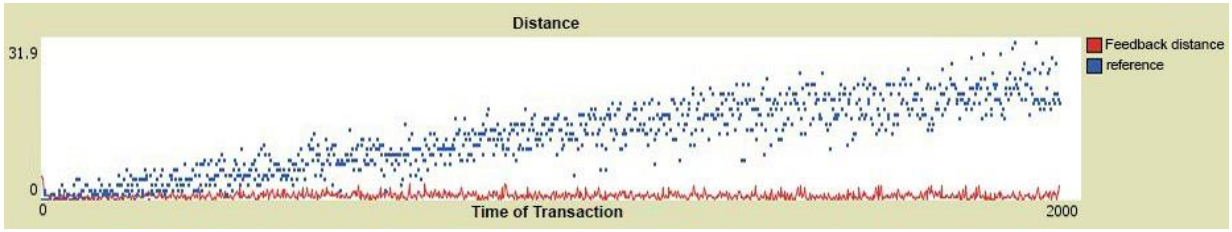
اما کاربران در این سیستم نیز خود به دو دسته تقسیم می‌شوند. دسته اول کاربرانی هستند که همواره صادقانه عمل می‌کنند. این کاربران در هنگام ارزیابی، میزان بازخوردی با کمتر از ۰/۱ اختلاف نسبت به واقعیت ارائه می‌نمایند. دسته دیگر کاربران بدخواه هستند. این کاربران بازخوردی که ارائه می‌نمایند با میزان واقعی اعتماد اختلاف زیادی دارد. در نتیجه این مقدار می‌تواند بیش از ۰/۲۵ باشد.

۲-۶- نتایج ارزیابی

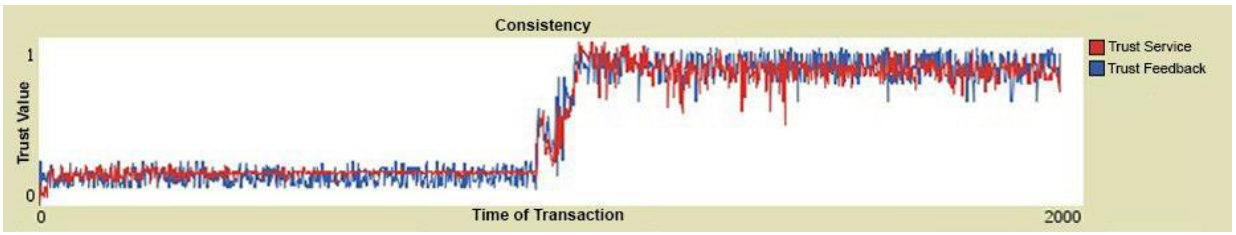
در این بخش نتایج ارزیابی مدل اعتماد پیشنهادی ارائه داده خواهد شد. برای این منظور کلیه فراهم‌کنندگان سرویس را به ۵ دسته مساوی (هر دسته ۲۰ درصد) تقسیم کرده‌ایم. رفتار هر کدام از دسته‌ها بر اساس ماهیت رفتاری که پیش از این توضیح داده شد خواهد بود. تعداد کاربران بدخواه ۴۰ درصد و تعداد کاربران صادق معادل ۶۰ درصد در نظر گرفته شده است. به منظور درک بهتر از ارزیابی صورت گرفته شده و همچنین به دلیل این‌که پارامتر میزان کاربران ارسال کننده بازخورد با مقادیر فاصله اعتماد مقایسه می‌شود، مقادیر فاصله اعتماد به دست آمده با مقیاس ۱۰ و میزان کاربران ارسال کننده بازخورد با مقیاس ۰/۵ در شمل ۵ نشان داده شده‌اند.

در این شکل ملاحظه می‌شود که با گذشت زمان، میزان پراکندگی بازخوردها نیز افزایش پیدا می‌کند و تعداد کاربران بیشتری (که با رنگ آبی نمایش داده شده‌اند) سرویس‌ها را ارزیابی نموده‌اند. بنابراین، با توجه به توضیحات داده شده و با تاکید بر نیمه دوم ارزیابی انجام شده در شکل ۶، مشاهده می‌گردد که مقدار ارزیابی با گذشت زمان به یک مقدار پایدار در مورد سرویس‌ها رسیده است. بنابراین شکل ۶ نمایش‌دهنده میزان فاصله ناچیز اعتماد بدست آمده از مدل پیشنهادی و اعتماد واقعی سرویس است که در بسیاری از نقاط ارزیابی این مقدار به صفر نیز رسیده است.

ملاحظه می‌شود که با انجام ۱۰۰۰ تراکنش، سرویس تغییر وضعیت داده ولی همچنان مدل توانسته است میزان اعتماد را به درستی تشخیص داده و مقدار اعتماد محاسبه شده را نزدیک به اعتماد واقعی ارزیابی نماید.



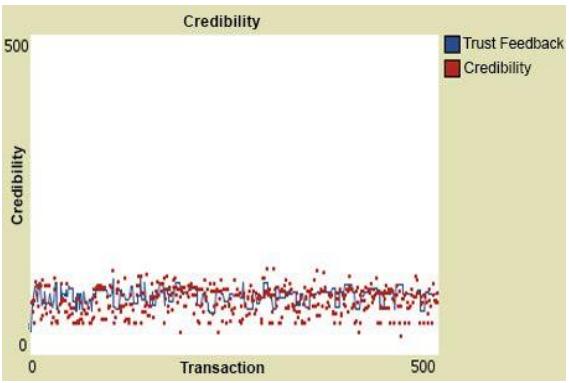
شکل ۵: تفاوت مقادیر فاصله اعتماد به دست آمده سرویس‌های همواره خوب، بر مبنای میزان کاربران ارسال‌کننده بازخورد



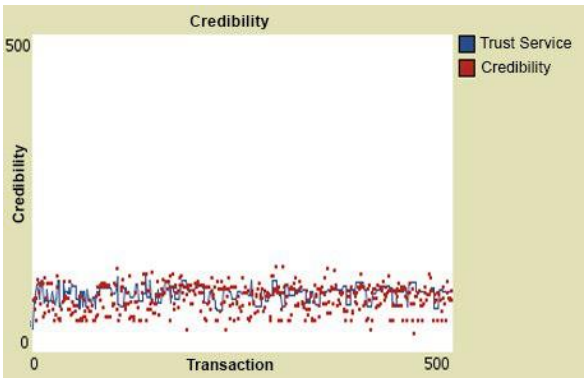
شکل ۶: تفاوت مقادیر اعتماد واقعی سرویس‌ها در برابر بازخوردهای به دست آمده در سرویس‌های با عملکرد ابتدایی ضعیف و انتهایی مناسب

در سناریوی دوم، نتایج ارزیابی مدل پیشنهادی در قبال سرویس های با عملکرد همواره بد مورد بررسی قرار می‌گیرد. این حالت ارزیابی دقیقاً عکس حالت سرویس‌های همواره خوب عمل می کند. تفاوت اعتبار محاسبه شده که با رنگ قرمز نشان داده شده، با مقادیر اعتماد واقعی در شکل ۷ (الف) و اعتماد ارزیابی شده در شکل ۷ (ب) بسیار ناچیز بوده و شاهد میزان اختلاف کم بین اعتبار محاسبه شده و و اعتماد سرویس (اعتماد واقعی سرویس و اعتمادی که توسط مدل حاصل شده) هستیم. نتایج بیانگر این مطلب هستند که با وجود اینکه سرویس‌ها همواره بد عمل می‌کنند و همچنین تعداد کاربران بدخواه موجود در سیستم ۳۰ درصد است، اما کماکان مدل اعتماد پیشنهادی توانسته کاربران بدخواه را شناسایی کرده و از تاثیرات بازخوردهای آن به سیستم جلوگیری نماید.

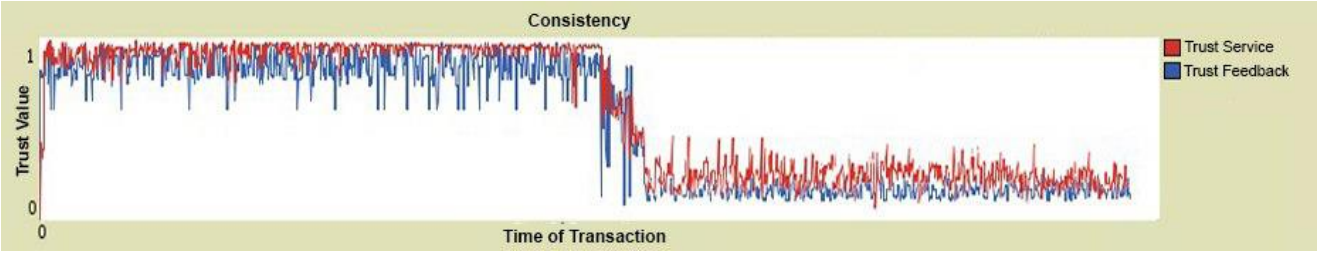
در شکل ۸ ملاحظه می‌شود که میزان اعتماد واقعی سرویس‌ها (رنگ آبی) در ۱۰۰۰ تراکنش ابتدایی در گستره ۰/۸ تا ۱ است و با گذشت زمان در ۱۰۰۰ تراکنش باقیمانده مقادیر در گستره ۰ تا ۰/۲ قرار می‌گیرد. بنابراین می‌توان نتیجه گرفت که سیستم توانسته است، بازخورد اعتماد به‌دست آمده از کاربران (رنگ قرمز) را نزدیک به واقعیت ارزیابی نماید. در انتهای شکل مذکور و در زمان تراکنش ۱۸۰۰ تا ۲۰۰۰ دیده می‌شود که میزان اعتماد واقعی سرویس‌ها و میزان بازخورد محاسبه شده توسط مدل به مقدار نزدیک به هم رسیده است که نشان‌دهنده این است که مدل توانسته است اعتماد سرویس را به درستی محاسبه نماید. به عنوان سناریویی دیگر، در شکل ۹ ملاحظه می‌شود که میزان اعتماد واقعی سرویس‌ها (رنگ آبی) در سراسر تراکنش به صورت کاملاً تصادفی عمل می‌کند.



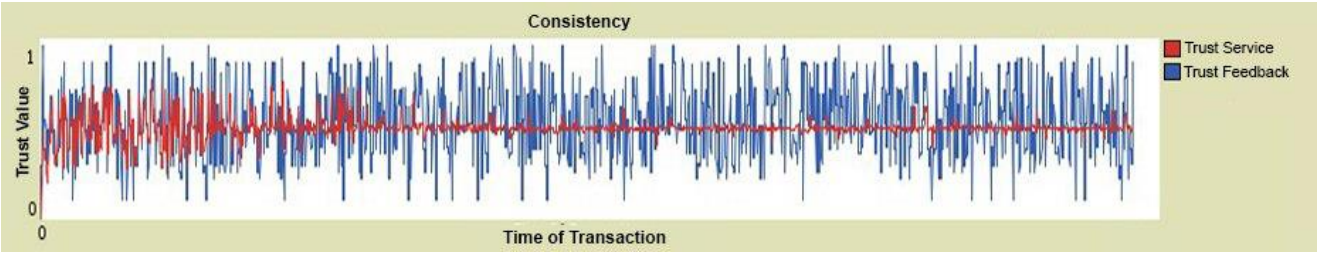
شکل ۷ (الف): تفاوت میزان بازخورد اعتماد محاسبه شده سرویس‌های همواره بد بر مبنای اعتبار محاسبه شده کاربران دخیل در ارزیابی



شکل ۷ (ب): تفاوت میزان اعتماد واقعی سرویس‌های همواره بد بر مبنای اعتبار محاسبه شده کاربران دخیل در ارزیابی



شکل ۸: تفاوت مقادیر اعتماد واقعی سرویس‌ها در برابر بازخوردهای به دست آمده در سرویس‌های با عملکرد ابتدایی مناسب و سپس ضعیف



شکل ۹: تفاوت مقادیر اعتماد واقعی سرویس‌ها در برابر بازخوردهای به دست آمده در سرویس‌های با عملکرد متغیر و تصادفی

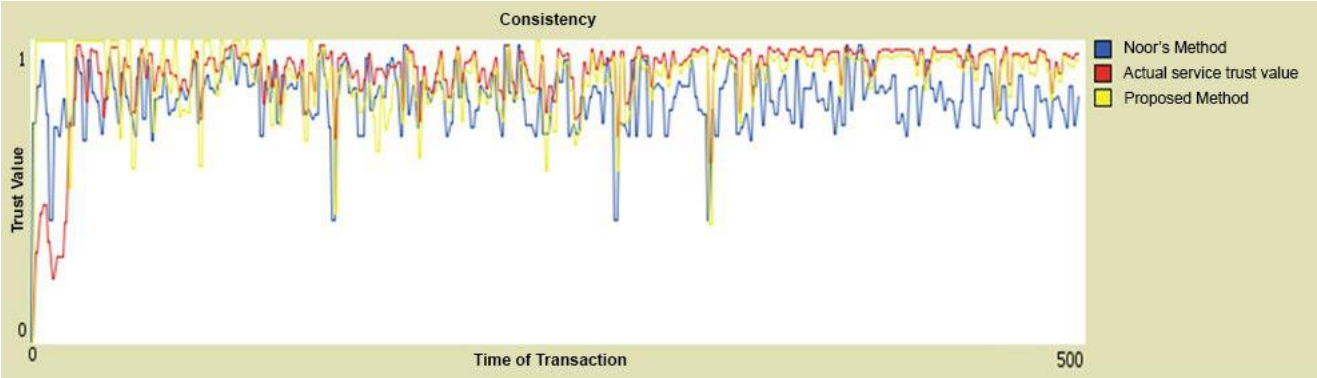
لذا سیستم توانسته است، بازخورد اعتماد به‌دست آمده از کاربران (رنگ قرمز) را نزدیک به واقعیت ارزیابی نماید. در انتهای شکل مذکور دیده می‌شود که میزان اعتماد واقعی سرویس‌ها به یک مقدار ثابت و پایدار رسیده است. این موضوع بیانگر این مطلب است که سیستم توانسته است رفتار سرویس‌ها را به درستی تشخیص داده و به یک حد وسط از بازخوردها دست پیدا کند و آن را به عنوان ملاکی برای محاسبه اعتماد قرار دهد.

در ادامه، روش ارائه شده با رهیافتی که توسط Noor و همکارانش[۳۵-۳۷]، ارائه شده است، مقایسه می‌شود. روش ارائه شده، اعتبارکاربران را به شیوه نظر اکثریت، برای ارزیابی سرویس‌ها در نظر گرفته است. این در حالی است که روش پیشنهادی این تحقیق برای محاسبه اعتبار کاربران از ارزش بازخوردها به همراه دو شیوه نظر اکثریت و نظر میانه استفاده نموده است. شکل‌های ۱۰ و ۱۱ نتایج این ارزیابی را برای سرویس‌های همواره خوب و سرویس-های همواره بد، نشان می‌دهند. در هر شکل سه منحنی کشیده شده است. منحنی‌ها به ترتیب، مقدار اعتماد محاسبه شده با بهره گیری از رهیافت [۳۵-۳۷]، مقدار اعتماد سرویس‌ها و مقدار اعتماد محاسبه شده توسط روش ارائه شده هستند.

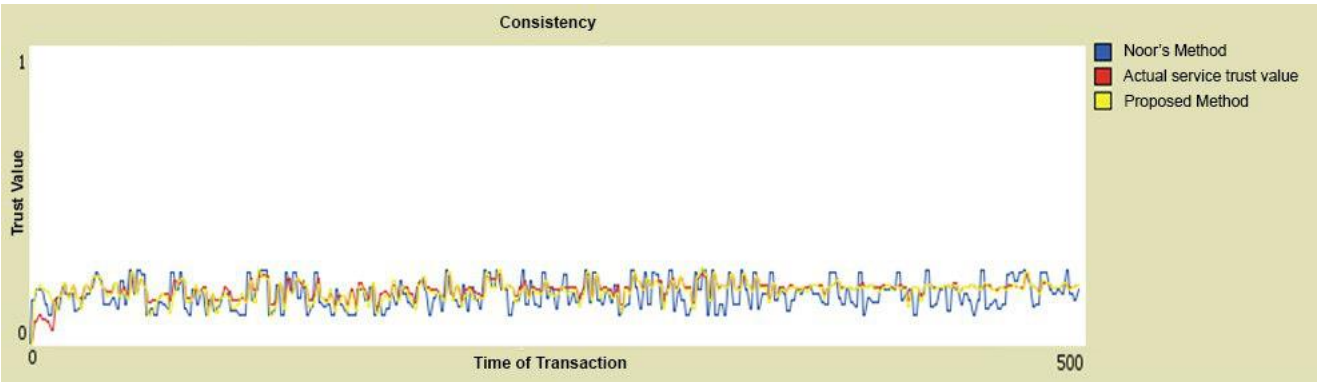
همانطور که ملاحظه می شود روش ارائه شده در این پژوهش با توجه به تغییر رویکردها توانسته سرویس‌های مختلف را به درستی شناسایی نماید و از اعمال نفوذ کاربران بدخواه به سیستم جلوگیری کند. با استفاده از رهیافت این پژوهش اختلاف اعتماد محاسبه شده نسبت به اعتماد مورد انتظار در حد قابل توجهی کمتر از اختلاف روش های مشابه است.

۷- نتیجه‌گیری

در این پژوهش سعی شد به یکی از مسائل پرکاربرد و مهم در علوم کامپیوتر که مسئله مدل‌سازی اعتماد است پرداخته شود. همانطور که در جوامع انسانی، اعتماد نشات گرفته از علوم اجتماعی بوده و بر مبنای تعاملات انسانی شکل می‌گیرد، منطقی است مدل‌سازی اعتماد در محیط‌های محاسباتی نیز بر اساس تعاملات بین موجودیت‌ها استوار باشد. بر این اساس در این تحقیق به ارائه یک مدل محاسباتی اعتماد مبتنی بر اعتبار بازخورد کاربران برای انتخاب سرویس پرداخته شد. در مدل ارائه شده برخلاف بسیاری از مدل‌های موجود، بر روی اعتبار کاربر تمرکز گردیده است. مدل اعتماد ارائه شده، یک مدل نامتمرکز و بر مبنای پروتکل پاستری است. بنابراین از مشکلات ناشی از سیستم‌های متمرکز مانند وجود یک نقطه شکست پرهیز شده است. در این مدل، برخی از چالش‌های امنیتی مانند ارزیابی‌های ناعادلانه، ارزیابی‌های چندباره، انحراف از کیفیت با گذشت زمان مد نظر قرار داده شده‌اند. این مدل در محاسبه اعتماد هر کاربر، تجربیات مستقیم و نیز تجربیات سایر کاربران را در نظر می‌گیرد. همچنین به ماهیت چند وجهی بودن اعتماد توجه شده است و هر کاربر می‌تواند اولویت خود را در زمینه هریک پارامترهای کیفیت سرویس مطرح کند. در انتها مقدار اعتماد با استفاده از وزن‌های داده شده، محاسبه خواهد شد. همچنین، مدل ارائه شده می‌تواند میزان اعتماد هر سرویس را با وجود کاربرانی که به ارزیابی‌های ناعادلانه می‌پردازد، تاحد مطلوبی به درستی و مشابه با مقدار مورد انتظار محاسبه نماید.



شکل ۱۰: مقایسه سرویس های همواره خوب در مدل پیشنهادی با مدل ارائه شده در Noor و همکاران [۲۲-۲۴]



شکل ۱۱: مقایسه سرویس های همواره بد در مدل پیشنهادی با مدل ارائه شده در Noor و همکاران [۲۲-۲۴]

مراجع

[1] A. S. Tanenbaum and M. Van Steen, *Distributed Systems: Principles and Paradigms*, Prentice-Hall, 2007.

[2] R. K. Ko *et al.*, "TrustCloud: A framework for accountability and trust in cloud computing," in *Proceedings of the 2011 IEEE World Congress on Services (SERVICES)*, U.S, Washington, 04-09 July, 2011, pp. 584-588.

[3] J. W. Rittinghouse and J. F. Ransome, *Cloud Computing: Implementation, Management, and Security*, CRC press, 2016.

[4] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in *Proceedings of the IEEE Grid Computing Environments Workshop(GCE'08)*, U.S, Austin, 16-18 November, 2008, pp. 1-10.

[5] M. Almorsy, J. Grundy and I. Müller, "An analysis of the cloud computing security problem," *arXiv preprint, arXiv:1609.01107*, 2016.

[6] K. Hildrum, J. D. Kubiatowicz, S. Rao, and B. Y. Zhao, "Distributed object location in a dynamic network," *Theory of Computing Systems*, vol. 37, no. 3, pp. 405-440, 2004.

[7] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, *A Scalable Content-addressable Network*, in *Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, U.S, California, October 2001, pp.161-172.

[8] X. Sun, G. Chang, and F. Li, "A trust management model to enhance security of cloud computing environments," in *Proceedings of the 2nd International Conference on Networking and Distributed Computing (ICNDC)*, China, Beiging, 21-24 September, *2011*, pp. 244-248.

[9] H. Yu, Z. Shen, C. Leung, C. Miao, and V. R. Lesser, "A survey of multi-agent trust management systems," *IEEE Access*, vol. 1, no. 2, pp. 35-50, 2013.

[10] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583-592, 2012.

[11] Z. Raghebi and M. R. Hashemi, "A new trust evaluation method based on reliability of customer feedback for cloud computing," in *Proceedings of the 10th International ISC Conference on Information Security and Cryptology (ISCISC)*, Iran, Yazd,29-30 August, 2013, pp. 1-6.

[12] W. Viriyasitavat and A. Martin, "A survey of trust in workflows and relevant contexts," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 3, pp. 911-940, 2012.

[13] J. Song and Q. Song, "Research and application on recommendation trust model in distributed network system," *Applied Mechanics and Materials*, 2014, vol. 687, pp. 2063-2066.

[14] N. H. Hussein and A. Khalid, "A survey of cloud computing security challenges and solutions," *International Journal of Computer Science and Information Security*, vol. 14, no. 1, p. 52, 2016.

[15] S. M. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in *Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, China, Shanghai, 16-18 November, 2011, pp. 933-939.

[16] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in *Proceedings of the IEEE 2nd International Conference on Cloud Computing, Technology and Science (CloudCom)*,U.S, Indiana, 30 November - 03 December, 2010, pp. 693-702.

[17] K. Gokulnath and R. Uthariaraj, "A Survey on Trust Models in Cloud Computing," *Indian Journal of Science and Technology*, vol. 9, no. 47, 2016.

[18] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 2, no. 1, pp. 1-9, 2013.

[19] G. D'Angelo, S. Rampone, F. Palmieri, "Developing a trust model for pervasive computing based on Apriori association rules learning and Bayesian classification," *Soft Computing*, vol. 21, no. 21, pp. 6297-6315, 2017.

[20] J. Jiang, G. Han, L. Shu, "A Trust model based on cloud theory in underwater acoustic sensor networks" *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 342-350, 2017.

[21] R. Costa Cardoso, A. Gomes, M. Freire, "A user trust system for online games: A subjective logic approach for trust inference" *IEEE Transactions on Computational Intelligence and AI in Games*, vol. 9, no. 4, pp. 354-368, 2017.

[22] S. Muhammad, L.Wang, B. Yamin, " Trust model based uncertainty analysis between multi-path routes in MANET using subjective logic," in *Proceedings of the China Conference on Wireless Sensor Networks*, China, Tianjin, 12-14 October, 2011, pp. 319-332.

[23] A. Koster, A. Bazzan, M. Souza, "Liar liar, pants on fire; or how to use subjective logic and argumentation to evaluate information from untrustworthy sources" *Artificial Intelligence Review*, vol. 48, no. 2, pp. 219-235, 2017.

[24] W. Zhang et al., "A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks" *The Journal of Supercomputing*, vol. 74, no. 4, pp. 1779-1801, 2018.

[25] V. Busi Reddy, S.Venkataraman, A. Negi, " Communication and data trust for wireless sensor networks using D–S theory" *IEEE Sensor Journal*, vol. 17, no. 12, pp. 3921-3929, 2017.

[26] K. Sharma et al., "Trust computation in VANET using TOEFV" *International Journal of Trust Management in Computing and Communications*, vol. 4, no. 1, https://doi.org/10.1504/IJTMCC.2017.089591, 2017.

[27] A. Kumai Jain, V. Tokekar, S. Shrivastava "Security enhancement in MANETs using fuzzy-based trust computation against black hole attacks" *Advances in Intelligent Systems and Computing Book Series*, vol. 5, no. 3, pp.39-47, 2017.

[28] K. Singh, A. Kumar Verma, " A fuzzy-based trust model for flying ad hoc networks (FANETs)" *International Journal of Communication Systems*, vol. 31, no. 6, pp. 341-453, 2018.

[29] Z.Yang, J. Luo, " A behavior trust model based on fuzzy logiv in cloud environments " *International Journal of Performability Engineering*, vol. 14, no. 4, pp. 665-672, 2018.

[30] J. Cho, I.R. Chen, " PROVEST: Provenance-based trust model for delay tolerant networks " *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 1, pp. 151-165, 2018.

[31] S. Das et al., " A Markov-based model for information security risk assesment in healthcare MANETs " *Information Systems Frontiers*, https://doi.org/10.1007/s10796-017-9809-4, pp. 1-19, 2017.

[32] Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking," *Security and Communication Networks*, vol. 9, no. 16, pp. 3059-3069, 2016.

[33] H. Toumi, A. Talea, B. Marzak, A. Eddaoui, and M. Talea, "Cooperative trust framework for cloud computing based on mobile agents," *International Journal of Communication Networks and Information Security*, vol. 7, no. 2, p. 106, 2015.

[34] A. Rowstron and P. Druschel, "Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems," in *Proceedings of the IFIP/ACM International Conference on Distributed Systems Platforms and Open Distributed Processing*, U.S, New York, 4-7 April, 2001, pp. 329-350.

[35] T. Noor and Q. Sheng, "Trust as a service: A framework for trust management in cloud environments," *Web Information System Engineering*, pp. 314-321, 2011.

[36] T. H. Noor, Q. Z. Sheng, A. H. Ngu, A. Alfazi, and J. Law, "Cloud armor: a platform for credibility-based trust management of cloud services," in *Proceedings of the 22nd ACM International Conference on Information & Knowledge Management*, U.S, San Fransisco, 27 October - 01 November, 2013, pp. 2509-2512.

[37] T. H. Noor, Q. Z. Sheng, and A. Alfazi, "Reputation attacks detection for effective trust assessment among cloud services," in *Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Austrailia, Melbourne, 16-18 July, 2013, pp. 469-476.

[38] Z. Malik and A. Bouguettaya, "RATEWeb: Reputation Assessment for Trust Establishment among Web Services," *The VLDB Journal*, vol. 18, No. 4, 2009, pp. 885-911.

زیرنویس‌ها:

[1] Coherent
[2] Single
[3] Transparency
[4] Openness
[5] Scalability
[6] Pervasive
[7] Data lock-in
[8] Disaster recovery
[9] Energy efficiency
[10] Multi-tenancy
[11] Subjective
[12] Objective
[13] Evidence
[14] Belief function
[15] Hidden Markov model
[16] Service repository
[17] Community
[18] Distributed hash table
[19] Pastery
[20] Broker
[21] Peer to Peer