مجله علمی پژوهشی «پدافند الکترونیکی و سایبری»
سال ششم، شماره ۴، زمستان ۱۳۹۷؛ ص ۱۲۲-۱۰۵

روشی ترکیبی به‌منظور شناسایی فراهم‌کنندگان خدمات ابری قابل‌اعتماد با استفاده از فرآیند تحلیل سلسله مراتبی و شبکه‌های عصبی

سارا طبقچی میلان[۱]، نیما جعفری نویمی‌پور[۲]*

۱- دانشجوی کارشناسی ارشد، گروه مهندسی کامپیوتر، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران

۲- استادیار، گروه مهندسی کامپیوتر، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران

(دریافت: ۱۳۹۶/۱۱/۰۱ ، پذیرش: ۱۳۹۷/۰۳/۰۶)

چکیده

اخیرا فناوری رایانش ابری توانسته است در مدت‌زمان کوتاهی محبوبیت گسترده‌ای بیابد. لذا با توجه به این محبوبیت شمار قابلیت‌ها و ویژگی‌های خدمات ابری نیز رو به افزایش می‌باشد. در محیط‌های ابری به‌منظور یافتن ارائه‌دهنده معتبر و انتخاب بهترین منابع در زیرساخت‌های ناهمگن ابری، اعتماد نقش مهمی را ایفا می‌کند. عدم اعتماد مشتریان به ارائه‌دهندگان خدمات ابری بزرگ‌ترین مانعی است که اغلب برای پذیرش خدمات ابری در نظر گرفته می‌شود. در این پژوهش سعی بر تدوین مدل شناسایی ارائه‌دهندگان خدمات ابری نامعتبر خواهد بود که با استفاده از ویژگی‌های ارزیابی اعتماد به ارائه‌دهندگان ابری، اعتبارسنجی انجام خواهد گرفت. در رویکرد پیشنهادی به‌منظور تشخیص فراهم‌کنندگان ابری ترکیب روش شبکه عصبی با وزن‌دهی سلسله مراتبی ارائه شده است و علت به‌کار گرفتن شبکه عصبی، قابلیت پیدا کردن و تشخیص مقادیر بهینه آن می‌باشد. نتایج شبیه‌سازی حاکی از آن است که درصد خطای این روش ۰/۰۰۵٪ می‌باشد که به‌نسبت روش‌های رایج دیگر دارای دقت بیشتری است.

واژه‌های کلیدی: خدمات ابری، اعتماد، شبکه عصبی، تحلیل سلسله مراتبی

۱- مقدمه

رایانش ابری، فناوری مبتنی‌بر اینترنت است که از طریق آن منابع محاسباتی توزیع‌شده، توسط کاربران مورد دسترسی قرار می‌گیرد [۲-۱]. در دنیای مدرن، داده‌ها در مراکز داده مختلف پراکنده می‌گردد و برنامه‌های کاربردی در سرورهای آن‌ها قرار می‌گیرند. فناوری رایانش ابری داده‌های پراکنده و برنامه‌های کاربردی را در قالب مجازی‌سازی ارائه می‌دهد و ایده‌ی اصلی آن دسترس‌پذیری زیرساخت‌های محاسباتی و ذخیره‌سازی برای کاربران ابری صرف‌نظر از زمان و مکان می‌باشد. به‌منظور رساندن این فناوری به عرصه‌ی تجارت، کاربران ابری می‌بایست کاملاً به ارائه‌دهندگان خدمات ازلحاظ تکمیل کارهای ارسالی مطابق توافقنامه سطح خدمات[۱] اعتماد داشته باشند [۴-۳]. مدل‌های ارائه‌دهنده ابری، براساس نیازهای کاربران منابع موردنیاز آنها را تحت عنوان خدمات ابری ارائه می‌دهند [۵]. زیرساخت‌های ابری از سه نوع خدمات ابری پشتیبانی می‌نمایند که عبارت‌اند از نرم‌افزار به‌عنوان خدمت [۷-۶]، زیرساخت به‌عنوان خدمت [۸] و بستر به‌عنوان خدمت [۹].

مسائل و چالش‌های اعتماد در رایانش ابری به‌طور گسترده از منظرهای مختلف مورد بحث می‌باشد و از قابلیت‌های ارائه‌دهنده منابع ابری محسوب می‌شود چراکه توسط آن کاربران بهترین منابع از زیرساخت‌های ناهمگن ابری را انتخاب می‌نمایند [۱۰]. در [۱۱]، از اعتماد تحت عنوان بزرگ‌ترین مسئله در رایانش ابری یادشده است و علت آن تضمین وجود اعتماد داده‌ها به‌طور مؤثر در طول تعاملات بین کاربران و ابر می‌باشد که به‌سبب آن‌یک ارتباط قابل اعتماد متقابل بین کاربران و ارائه‌دهنده خدمات ابر با روش‌های کنترل دسترسی در محیط رایانش ابری به‌وجود می‌آید [۱۲]. سطح اعتمادِ یک ارائه‌دهنده خدمات ابری را می‌توان با اشاره به حفظ مدیریت با مدت اعتماد مصرف‌کنندگان

* رایانامه نویسنده مسئول: jafari@iaut.ac.ir

1- Service Level Agreement(SLA)

اندازه گرفت و برای حفظ آن ارائه‌دهنده ابری باید خدمات موردنیاز مشتری‌ها را متناسب با سطح مطالبات خود فراهم نماید. اگرچه برای انتخاب ارائه‌دهنده ابری طیف وسیعی از معیارها وجود دارد، بااین‌حال انتخاب نهایی در اختیار کاربر است [۱۳]. مسلماً در یک محیط رایانش ابری، تعداد زیادی ارائه‌دهنده خدمات برای توسعه و ارائه خدمات به کاربران وجود دارد. به‌رغم این واقعیت که با پیچیده شدن و غیرقابل پیش‌بینی شدن محیط ابری، خدمات ابری همیشه قابل اعتماد نیستند و حتی توافق‌نامه سطح خدمات هم ممکن است نیازهای کاربران را برآورده نکند [۱۴]، لذا ارائه‌دهندگان خدمات ابری برای مشتریان قابل اعتماد هستند؛ درنتیجه، ارائه‌دهندگان باید بتوانند از جاسوسی جلوگیری نموده و داده‌ها و برنامه‌های کاربردی کاربر را از هر آسیبی محافظت نمایند. خدمات ابری همواره باید در دسترس باشند و نیازهای دیگر کاربران ازجمله کیفیت خدمات را باتوجه به توافق‌نامه سطح خدمات (در یک خدمت ابری) برآورده سازد که نیاز به‌شواهد اعتماد چندبعدی است تا منعکس‌کننده جنبه‌های مختلف عملکرد خدمات ابری باشد.

به‌دلیل این اهمیت، در این پژوهش به شناسایی ارائه‌دهندگان معتبر و نامعتبر ابری با استفاده از شبکه عصبی پرداخته شده است که کاربران را در انتخاب فراهم‌کنندگان معتبر یاری می‌نماید. روش پیشنهادی شامل دو مرحله می‌باشد؛ در مرحله اول، مجموعه‌ای از داده‌های فرضی وجود دارد که تعداد منابع ابری معتبر و نامعتبر در آن مشخص بوده و شامل ماتریسی با تعداد مشخصی ابر و ویژگی می‌باشد. مدل شبکه عصبی در نظر گرفته‌شده محدود به سه لایه ورودی، پنهان و خروجی می‌باشد [۱۵]. میزان قابلیت اعتماد به هر منبع ابری با استفاده از روش وزن‌دهی سلسله مراتبی[1] برای هر ابر محاسبه‌شده و باتوجه به مقادیر تعریف‌شده ویژگی‌ها، تعداد وزن میانگین به‌وسیله ماتریس زوجی مشخص می‌شود. در مرحله دوم، برای به‌دست آوردن ارائه‌دهندگان ابر نامعتبر از شبکه عصبی، وزن‌های به‌دست‌آمده از روش فازی به‌عنوان ورودی شبکه عصبی در نظر گرفته‌خواهد شد. در ادامه نرخ خطا، نرخ یادگیری و میزان اعتماد ابر محاسبه‌شده و ابرهای قابل قبول شناسایی خواهند شد.

ادامه این مقاله به‌ترتیب زیر سازمان یافته است. در بخش دوم، به مطالعه و بررسی کارهای مرتبط پرداخته است. بخش سوم، به ارائه کامل روش پیشنهادی اختصاص یافته است، در بخش چهارم به معرفی محیط شبیه‌سازی و پارامترهای شبیه‌سازی و ارائه نتایج حاصل پرداخته‌شده است و درنهایت، در بخش پنجم نتیجه‌گیری و کارهای آتی ارائه شده است.

1- Analytical Hierarchy process(AHP)

۲- کارهای مرتبط

همان‌گونه که در بخش قبل اشاره شد برای انتخاب بهترین منابع در زیرساخت‌های ناهمگن ابری، اعتماد نقش مهمی ایفا می‌کند و به‌دلیل قادر ساختن کاربران برای انتخاب بهترین منابع یکی از بزرگ‌ترین چالش‌های فناوری ابر به شمار می‌آید [۱۰]. لذا در این بخش، برخی از روش‌های مرتبط در این زمینه به همراه مزایا و معایب آن‌ها بررسی و ارائه می‌شوند.

در [۱۰]، مدل جدیدی از اعتماد مبنی‌بر اعتبار گذشته و قابلیت‌های موجود در ارائه‌دهندگان منابع ابری ارائه شده است. در این روش، مقدار اعتماد با استفاده از چهار ویژگی قابلیت دسترسی[2]، قابلیت اطمینان[3]، کارایی چرخشی[4] و تمامیت داده‌ها[5] محاسبه می‌شود و در کنار آن یک سامانه مدیریت اعتماد برای اجرای این مدل از اعتماد پیشنهاد شده است. این پژوهش چگونگی آمادگی توافق سطح خدمات که ترکیبی از خدمات موردنیاز کاربر و قابلیت‌های ارائه‌دهندگان منابع ابری است را توصیف می‌نماید. ابتدا کاربر ابر، فهرستی از الزامات کیفیت خدمات را تهیه نموده و با مرور کاتالوگ، خدمات منابع ابری مناسب را انتخاب می‌نماید و لیست این دو را در اختیار مدیر سامانه قرار می‌دهد. مدیر سامانه دسترسی منابع ابری را با خدمات کاتالوگ بررسی نموده و نیازهای کیفیت خدمات و منابع ابری مناسب را به مدیر سطح توافق خدمات ارسال می‌نماید. مدیر سطح توافق خدمات، مقادیر اعتماد را از مدیر اعتماد گردآوری نموده و سپس منابع ابری بر اساس مقادیر اعتمادشان مرتب می‌شوند. پس از سازش و مذاکره با کاربران ابر از طریق مدیر سامانه سطح توافق خدمات تهیه‌شده و توسط مدیر سطح توافق خدمات به مدیر سامانه ارسال می‌شود. مدیر سامانه به‌منظور زمان‌بندی منابع با مشاور زمان‌بند مشورت می‌نماید و سطح توافق خدمات را در اختیار ناظر خدمت قرار می‌دهد. ناظر خدمات و عامل میانی، منابع ابری موردنیاز را تهیه نموده و یک محیط کاری در قالب سامانه مجازی به کاربر ابر ارائه می‌دهند که توسعه و مدیریت سامانه‌های مجازی موردنیاز را نیز بر عهده‌دارند. مدیر سامانه به‌طور هم‌زمان سطح کیفیت خدمات را به بخش نظارت و محاسبه صورت‌حساب ارسال می‌کند و پس از محاسبه، برگ خرید را به کاربر ارسال می‌نماید. مدیر سامانه در کنار سطح کیفیت خدمات ۴ ویژگی در نظر گرفته‌شده را در رابطه با اجرای این کار به مدیر سطح کیفیت خدمات منتقل می‌نماید. مدیر سطح خدمات ۴ ویژگی اعتماد را به‌روز رسانی کرده و مدیر

2- Availability
3- Reliability
4- Turnaround Efficiency
5- Data Integrity

اعتماد، داده‌ها را در مخزن اعتماد ذخیره می‌نماید. پس از دریافت داده‌های پردازش‌شده از مدیر سامانه کاربر، داده و خدمات ارائه‌شده توسط منابع ابری را می‌آزماید و درنهایت مدیر اعتماد به‌نوبه خود داده‌ها را در مخزن اعتماد ذخیره می‌نماید و به انتخاب منبع مناسب کمک می‌کند. در این‌روش تک‌تک ویژگی‌ها با توجه به اهمیت و اولویت‌های آنها مورد بررسی قرارگرفته ولی با این‌وجود ویژگی‌های کمتری در آن به‌کار گرفته‌شده است؛ درحالی‌که می‌توانست ویژگی‌هایی همانند صداقت و امنیت نیز برای تکامل کیفیت خدمات در نظر گرفته شود.

مدل ترکیبی پویا برای محاسبه اعتماد به ارائه‌دهندگان ابری ارائه‌شده است که ارتباط اعتماد و کیفیت خدمات، دقت خدمات پیشنهادی را به‌طور قابل‌توجهی افزایش می‌دهد. مدل پیشنهادی به‌ترتیب شامل سه‌گام ثبت خدمات ابر، کشف خدمات ابر و فهرست خدمات تطبیقی می‌باشد. در ثبت خدمات ابری، خدمات ابر توسط کارگزار خدمات ابری به‌منظور به‌روزرسانی جزئیات خدمات در کاتالوگ خدمات ثبت می‌گردد، سپس کارگزار به‌آسانی ارائه‌دهنده مناسب را متناسب با نیاز کاربر می‌یابد. در گام کشف خدمات ابر، کاربران ابر پیش‌نیازهای خود را که شامل توضیحات عملیاتی و غیرعملیاتی می‌باشد به کارگزار ابر ارسال می‌کند. کنترل‌کننده‌ی درخواست‌های کاربر به‌منظور تعیین فهرستی از توصیفات خدمات مؤثر با رعایت موارد موردنیاز کاربران از مکانیسم مبتنی‌بر کشف معنایی استفاده می‌نماید. درنهایت، فهرستی از خدمات تطابقی ارائه می‌شود که در آن خدمات اعتماد با استفاده از مقادیر انطباقی کیفیت خدمات و بازخورد کاربران مرتب می‌شوند. واحد نظارت بر خدمات، میزان انطباقی کیفیت خدمات را به‌صورت پویا بررسی می‌نماید. ارزیاب اعتماد، اعتبار تمامی خدمات مورد رضایت را مرتب نموده و خدمت را با بیشترین میزان اعتماد به سمت گیرنده برمی‌گرداند. به‌طورکلی در این روش، ارزیابی و محاسبه اعتماد بر اساس ارزش انطباق و اعتبار صورت می‌پذیرد و امتیاز بازخورد کاربر محاسبه می‌شود که در مدل ترکیبی بهترین ارائه‌دهنده خدمات انتخاب می‌شوند. از مزایای این روش می‌توان به وجود اعتماد پویا به دلیل وجود انطباق، بهبود بخشیدن به انتخاب برنامه کاربردی و ارائه‌دهنده خدمات ابری، بی‌ثباتی کمتر و خطای کمتر اشاره نمود؛ هرچند انطباق و شهرت در ارزیابی و تصمیم‌گیری برای انتخاب ارائه‌دهنده خدمات ابری مناسب از معایب این روش می‌باشد.

ازآنجایی‌که مسائلی مانند در دسترس نبودن خدمات زمانی که به‌آن‌ها نیاز است، از رده خارج شدن خدمات ارائه‌شده به مشتریان توسط ارائه‌دهندگان و نگرانی‌هایی اعم از فقدان خدمات پشتیبانی مؤثر و باکیفیت به مشتریان ابری وجود دارند و از دلایل ناامیدی کاربران در اعتماد به خدمات ابری می‌باشند؛ لذا یک سامانه دقیق که کاربر بتواند بهترین ارائه‌دهنده خدمات را انتخاب نماید، موردنیاز است. در [۱۳]، مدل اعتماد در لایه خدمت رایانش ابری ارائه‌شده است که بهترین ارائه‌کننده خدمات را براساس نیاز کاربران می‌یابد. درروش پیشنهادی، ارائه‌دهنده خدمات ابری با توجه به خدماتی که ارائه می‌دهند، کیفیت‌شان ارزیابی می‌شوند. پارامترهای ارزیابی‌شده شامل تحمل‌پذیری خطا، تناوب به‌روز رسانی برنامه‌های کاربردی، تجربه خدمات به مشتریان و مدت‌زمان در دسترس نبودن سرویس می‌باشد. این پنج پارامتر جزء ویژگی‌های تمامی ارائه‌کنندگان خدمات ابری می‌باشد که به‌منظور ارائه خدمات در مؤسسات آموزشی در نظر گرفته شده است. وجه تمایز روش پیشنهادی، روی‌کرد انعطاف‌پذیری آن می‌باشد و کاربر می‌تواند مواردی که بیشتر نیاز به‌توجه دارند را اولویت‌بندی نماید به‌طوری‌که پارامترهای موردنیاز اولویتشان بیشتر از پارامترهای دیگر خواهد بود. اولویت‌ها را می‌توان براساس نیاز به آنها و دادن وزن بالا به پارامترهای اولویت‌دار و وزن کم به پارامترهای کم‌اهمیت‌تر مشخص نمود. دقیق نبودن اعتماد در انتخاب ارائه‌دهنده خدمات ابری به دلیل استفاده از ویژگی‌های کمتر از معایب این روش می‌باشد.

در [۱۷]، مدل اعتماد برای پیکربندی مجدد مؤثر و تخصیص منابع محاسباتی رضایت‌بخش در قبال نیازهای کاربران ارائه‌شده است. مدل پیشنهادی در این پژوهش، قابلیت اطمینان را مبنی‌بر اطلاعات تاریخی سرورها در مرکز داده ابر جمع‌آوری و تحلیل می‌کند؛ سپس بهترین منابع قابل‌دسترس برای هر خدمت درخواستی را فراهم نموده و بهترین منابع را برای کاربران ارائه می‌دهد. به‌منظور ارائه منابع باقابلیت اطمینان بالا نیاز به یک روش دقیق اندازه‌گیری و پیش‌بینی الگوهای استفاده از منابع محاسباتی می‌باشد که این الگوها در طول زمان تغییر می‌یابند. مدل اعتماد پیشنهادی، مجدداً سرورها را به‌صورت پویا پیکربندی نموده و منابع محاسباتی باکیفیت بالا را در اختیار کاربران قرار می‌دهد. اطلاعات تاریخی گره‌ها در محیط ابری استفاده می‌شود که این اطلاعات شامل مشخصات ویژگی گره‌ها، استفاده از منابع و زمان پاسخ می‌باشد. اگرچه درروش پیشنهادی قابلیت اطمینان و اعتماد بهبودیافته است ولی ویژگی‌هایی مانند صداقت و امنیت برای تکامل کیفیت خدمات مدنظر قرارگرفته نشده است.

در [۱۸]، یک مدل اعتماد مشترک امن ارائه شده است که سیاست‌های مختلف امنیتی برای حوزه‌های مختلف، بررسی محتوای تراکنش‌ها، محاسبه مقدار اعتماد به‌صورت پویا را دربر

می‌گیرد. مدل اعتماد پیشنهادی کاملاً با دیواره آتش[1] سازگار بوده و سیاست‌های کنترل محلی دیواره‌ی آتش را نقض نمی‌کند. ازآنجایی‌که ابر به دامنه‌های مستقلی تقسیم می‌گردد، مدل اعتماد بین گره‌ها در این پژوهش به دودسته تقسیم می‌شود اعتماد داخلی و بین دامنه‌ای. اعتماد داخلی براساس تراکنش‌های بین دامنه‌های مشابه می‌باشد و اعتماد بین دامنه‌ای براساس تراکنش گره‌های بین دامنه‌ای می‌باشد و برای هر یک استراتژی مختلفی در نظر گرفته شده است. تقسیم‌بندی ابرها در دامنه‌های مستقل براساس آدرس فیزیکی آنها خواهد بود. مقادیر اعتماد گره‌ها با گره‌هایی که در تبادل‌اند در جدول اعتماد نگهداری می‌شود؛ سپس هر دامنه مجموعه‌ای از عامل دامنه را در سه جدول که شامل جدول اعتماد دامنه داخلی، جدول اعتماد خارج از دامنه و جدول مقدار ریسک می‌باشد، نگهداری می‌کند. جدول اعتماد دامنه داخلی، مقادیر اعتماد تمامی گره‌های داخل دامنه را که در ارتباط هستند، ذخیره می‌کند. جدول اعتماد خارج از دامنه، تمامی مقادیر اعتماد را برای دامنه‌ای که مجاور با دامنه‌ای دیگری است و مقدارش برابر با میانگین وزن گره‌های اعتماد است را ذخیره می‌کند و مقدار جدول ریسک با ریسکی که تعریف‌شده محاسبه می‌شود. زمانی که یک کاربر منابع درخواست می‌نماید، عامل دامنه یک پیام به‌عامل همسایه در جدول دامنه داخلی منتشر می‌نماید و پس از دریافت موفق آن، عامل همسایه در تعامل با دیواره آتش یک پیام ارسال خواهد کرد سپس اعضای جدید ایجاد خواهد شد و درنهایت مقدار اعتماد بین گره‌ها محاسبه و در خاتمه گره مناسب انتخاب خواهد شد. ولی دراین روش محتوای تراکنش‌ها برای مقدار اعتماد ضروری است و ممکن است گره‌ها به چندین دامنه متعلق باشند و به‌علاوه، این‌که تلف شدن زمان نیز وجود دارد، اگرچه امنیت افزایش یافته است.

۳- روش پیشنهادی

در این بخش به معرفی مسئله، تشریح شبکه عصبی و درنهایت روش پیشنهادی پرداخته خواهد شد.

۳-۱- شبکه عصبی[2]

شبکه‌های عصبی از خانواده معماری‌های کاملاً موازی الهام گرفته‌شده از مغز انسان می‌باشد که قادر به یادگیری و تعمیم دادن از نمونه‌ها است. در این مدل شبکه، تجربه‌ی تولید راه‌حل بامعنا در مسائلی که حتی زمانی که داده‌های ورودی حاوی خطا و یا نواقص هستند، وجود دارد. اساساً، عوامل یک شبکه عصبی مشابه به سلول‌های عصبی[3] مغز انسان بوده و از عناصر محاسباتی خیلی ساده در لایه‌ها تشکیل‌شده است. یک شبکه عصبی معمولی شامل لایه‌ی ورودی[4]، لایه‌ی پنهان[5] و لایه خروجی[6] است [۱۹]. هر سلول عصبی در لایه ورودی مقدار یک متغیر مستقل را نشان می‌دهد. سلول‌های عصبی در لایه پنهان فقط برای اهداف محاسباتی هستند و درنهایت خروجی هرکدام از سلول‌های عصبی مقدار متغیر وابسته را محاسبه می‌کند [۲۰]. شاخصی به‌عنوان وزن در مجموعه‌ای از اتصالات بین سلول‌های عصبی[7] وجود دارد. این وزن‌ها، بارها در آموزش[8] شبکه‌های عصبی برای رسیدن به راه‌حل مناسب تنظیم می‌شود. اتصال[9] سلول‌ها باهم، رفتار شبکه عصبی را تعریف می‌نماید. ازآنجایی‌که شبکه‌های عصبی برتری خود را به دلایل بسیاری اثبات کرده‌اند، لذا این شبکه‌ها یک روش مؤثر در مدل‌سازی مشکلات طبقه‌بندی هستند که در آن مقادیر خروجی، رابطه مستقیم با ورودی‌های پیشین ندارد. عملکرد شبکه‌های عصبی در شرایطی مانند از دست‌دان ارتباط بین عصب‌ها، نویز و گم‌شدن، دشوار است. مراحل طراحی، اصول و روش در طراحی شبکه عصبی در همه حوزه‌ها کاربرد دارد [۲۱]. هدف اصلی این پژوهش، ساخت یک مدل قوی و مؤثر براساس شبکه‌های عصبی برای شناسایی ارائه‌دهندگان خدمات ابری نامعتبر است و ارائه ویژگی‌های مناسب برای آموزش شبکه‌های عصبی که در جهت اعتبارسنجی ارائه‌دهندگان خدمات ابری استفاده می‌شود. لذا با تعیین ساختار مناسب برای شبکه عصبی و همچنین نرخ یادگیری[10]، می‌توان بهترین عملکرد شناسایی ارائه‌دهندگان ابری را داشت.

۳-۲- روش ترکیبی پیشنهادی

روش پیشنهادی به‌منظور شناسایی ارائه‌دهندگان نامعتبر در ابر ارائه شده است. همان‌طور که در بخش قبل ذکر شد این مدل از شبکه عصبی دارای سه لایه می‌باشد. در مدل ارائه‌شده، ورودی شبکه عصبی مجموعه‌ای از داده‌ها است که شامل ماتریس ۲۸ × c بوده که c برابر با تعداد ابر و ۲۸ نشانگر ویژگی است که ۵۵٪ داده‌ها به‌صورت آموزش و ۴۵٪ به‌عنوان آزمایش به شبکه عصبی وارد می‌شود. مقادیر ویژگی‌ها با استفاده از تابع توزیع تصادفی در بازه ۰ تا ۱ توزیع‌شده‌اند. به‌صورت پیش‌فرض برخی از ابرها دارای مقادیر ۱ و برخی دیگر دارای مقادیر ۰ می‌باشند که با مقدار خروجی AND شده و ابر معتبر یا نامعتبر شناسایی

1- Firewall
2- Neural network

3- Neurons
4- Input layer
5- Hidden layer
6- Output layer
7- Nerve cell
8- Train
9- Connection
10- learning

می‌گردد. قابلیت اعتماد به‌هر منبع ابری با استفاده از روش وزن دهی سلسله مراتبی برای هر ابر و با توجه به مقادیر تعریف‌شده ویژگی‌ها مقدار وزن میانگین به‌وسیله ماتریس زوجی مشخص می‌شود. ضریب اعتماد در روش موردنظر ۵۰٪ است. برای به‌دست آوردن ابر نامعتبر با استفاده از شبکه عصبی، وزن‌های به‌دست‌آمده از روش سلسله مراتبی به‌عنوان ورودی شبکه عصبی در نظر گرفته‌شده است. یادگیری شبکه، ماتریسی است که به‌صورت تصادفی[1] از مقادیر عددی ۰ و ۱ پر می‌شود. برای به‌دست آوردن نرخ خطای شبکه، ابتدا ماتریس به‌دست‌آمده از فرآیند تحلیل سلسله مراتبی به‌ماتریس یادگیری ضرب می‌شود. سپس میانگین هر سطر، واریانس و انحراف معیار به‌دست می‌آید و درنهایت نرخ خطا از حاصل‌ضرب ماتریس فرآیند تحلیل سلسله مراتبی در انحراف معیار و نرخ یادگیری در پس انتشار با گشتاور[2] محاسبه می‌شود. آستانه خطای قابل‌قبول ۱۰٪ است. اگر ابری ضریب اعتماد بالای ۵۰٪ را کسب کند و هم‌زمان نرخ خطای آن کمتر از ۱۰٪ باشد به‌عنوان فراهم‌کننده ابر قابل‌قبول است. درنهایت برای شناسایی ارائه‌دهنده نامعتبر، ابرهای پذیرفته‌شده با ابرهای معتبر فرضی AND می‌شود. اگر حاصل ۰ شود به‌عنوان نامعتبر شناسایی می‌شود و اگر ۱ باشد به‌عنوان ابر معتبر شناسایی می‌گردد.

۳-۲-۱- جمع‌آوری داده‌ها

روش پیشنهادی شامل مجموعه داده‌های فرضی با **C** ارائه‌دهنده خدمات ابری معتبر و نامعتبر و ۲۸ ویژگی است. این داده‌ها ورودی‌های شبکه عصبی می‌باشند. مجموعه داده‌های فرضی به‌تعداد ۲۷۵ ارائه‌دهنده نامعتبر و به تعداد ۷۲۵ ارائه‌دهنده معتبر دارد. ۷۰٪ داده‌ها به‌عنوان آموزش شبکه عصبی و ۳۰٪ برای آزمایش است. مجموعه داده‌های جمع‌آوری‌شده دارای مقادیری هستند که در دوطبقه، معتبر و نامعتبر دسته‌بندی می‌شوند. این مقادیر می‌بایست به مقدار عددی بین ۰ و ۱ تبدیل شوند. به‌طوری‌که شبکه عصبی بتواند محاسبات خود را انجام دهد. درنتیجه مقادیر ۰ و ۱ به‌جای نامعتبر و معتبر جایگزین می‌شوند.

۳-۲-۲- ویژگی‌های شناسایی ارائه‌دهندگان خدمات ابری

انتخاب ساختار خدمات ابری در دست‌یابی به سطح اطمینان موردنیاز براساس یک وضعیت امنیتی خاص بسیار حیاتی خواهد بود. اعتماد از ضروری‌ترین و عمده‌ترین نیازهای اصلی یک ارائه‌دهنده خدمات ابری می‌باشد چراکه مشتریِ محصولات قابل‌فروش در ابر، از طریق ویژگی‌های مهم می‌تواند، ارائه‌دهنده معتبر را انتخاب نماید. روش پیشنهادی دارای ۲۸ ویژگی از ویژگی‌های ارائه‌دهندگان خدمات ابری است. نگرانی کاربر، اعتبارسنجی منابع و کنترل‌های امنیتی ارائه‌دهندگان خدمات ابری نمونه‌هایی از مواردی است که از دیدگاه کاربر مطرح است. رایج‌ترین نگرانی‌های کاربر، مربوط به کنترل دسترسی، شفافیت اعتماد، دید، مسئولیت‌ها و واکنش به‌رخدادها است. به‌عنوان‌مثال علاوه‌بر، وجود کنترل‌های امنیتی ارائه‌دهندگان خدمات ابری، توانایی ارائه‌دهندگان خدمات ابری را به‌منظور احراز هویت، امنیت نرم‌افزار، حفاظت از داده‌ها و امنیت ذخیره‌سازی داده‌ها را می‌توان افزایش داد. ویژگی‌های متعددی برای تشخیص ارائه‌دهندگان خدمات ابر نامعتبر وجود دارد. درروش پیشنهادی، ۲۸ ویژگی به‌کار گرفته می‌شود و مقدار این ویژگی‌ها یک مقدار دودویی خواهد بود که دلالت بر معتبر یا نامعتبر بودن ابر دارد؛ وجود یا عدم وجود ویژگی‌های درون‌ابر، مقدار نسبت داده‌شده را تعیین می‌کند. لازم به ذکر است که تمامی ویژگی‌ها از کارهای پیشین مطالعه شده در بخش ۲، انتخاب شده است. در ادامه، شرح مفصل و مدل ریاضی این ویژگی‌ها مورد ارزیابی قرارگرفته است.

قابلیت دسترسی: در دسترس بودن درجه‌ای است که یک سامانه و یا جزء عملیاتی به‌منظور استفاده در موقع نیاز در دسترس کاربران است. مقدار قابلیت دسترسی ارائه‌دهندگان از رابطه (۱) به‌دست می‌آید.

$$R_k(AV) = \frac{A_k}{N_k} \qquad (۱)$$

R تعداد منابع در دسترس، A تعداد کارهای پذیرفته‌شده دریک دوره زمانی و N تعداد کارهای به ثبت رسیده است [۱۰]. مقادیر در بازه **[۱و۰]** نرمال‌سازی خواهند شد و در ۴ گروه قرار خواهند گرفت. این چهار گروه عبارت‌اند از دسترسی بازمان مناسب، دسترسی در زمان متوسط، دسترسی بازمان کم و دسترسی با تأخیر که محدوده امتیازی هر یک از این موارد به ترتیب برابر با ۱، ۰/۷۵، ۰/۵، ۰/۲۵ خواهد بود که به ارائه‌دهندگان تخصیص خواهد یافت.

قابلیت اطمینان: قابلیت اطمینان یک جزء مهم از اعتماد می‌باشد. این ویژگی، میزان موفقیت نیز نامیده می‌شود. قابلیت اطمینان توانایی یک سامانه و یا یک جزء، برای انجام وظایف موردنیاز در یک دوره زمانی مشخص است. مقدار قابلیت اطمینان ارائه‌دهندگان از رابطه (۲) به دست می‌آید.

$$R_k(RE) = \frac{C_k}{A_k} \qquad (۲)$$

1- Randomize
2- Momentum

R تعداد منابع، **C** تعداد کارهای موفق انجام‌شده در زمان و **A** تعداد کارهای پذیرفته‌شده است. مقادیر در بازه **[۱و۰]** نرمال‌سازی خواهند شد [۱۰] و در ۴ گروه قرار خواهند گرفت. این چهار گروه عبارت‌اند از انجام وظایف در زمان خوب، انجام وظایف بازمان متوسط، انجام وظایف بازمان کم و انجام وظایف با تأخیر تقسیم‌بندی می‌شود که محدوده امتیازی هر یک از این موارد به ترتیب برابر با ۱، ۰/۷۵، ۰/۵، ۰/۲۵ خواهد بود.

تمامیت داده‌ها: امنیت یک مسئله کلیدی است که نیاز به‌توجه ویژه در ابرها دارد. تمامیت داده‌ها، یک اصطلاح گسترده است که شامل امنیت، حریم خصوصی و دقت داده‌ها می‌باشد. تمامیت داده‌ها به حفظ و حصول اطمینان از دقت و انسجام داده‌ها هرگونه سامانه ازجمله: فروشگاه‌ها، فرآیندها و بازیابی اطلاعات دلالت دارد. تمامیت داده‌های ارائه‌دهندگان از رابطه (۳) قابل‌محاسبه خواهد بود.

$$R_K(DI) = \frac{D_k}{C_k} \qquad (۳)$$

D تعداد کارهای موفق، به‌وسیله منبع R انجام‌شده و C تعداد یکپارچگی داده‌های حفظ‌شده به‌وسیله منبع R است [۱۰]. مقادیر در بازه [۱و۰] نرمال‌سازی خواهند شد و در ۴ گروه قرار خواهند گرفت که عبارت است از هر سه پارامترِ تمامیت داده‌ها را داشته باشد، دو پارامتر داشته باشد، یک پارامتر داشته باشد و درنهایت هیچ‌کدام را نداشته باشد که محدوده‌ی امتیازی هر یک از این موارد برابر با ۱، ۰/۷۵، ۰/۵، ۰ خواهد بود.

بهره‌وری چرخشی: زمان چرخش واقعی، زمان دقیق بین ارسالِ یک‌کار توسط یک‌کاربر و تحویل کار تکمیل‌شده به کاربر است. زمان چرخش، از زمان مورد انتظار وعده داده‌شده، توسط ارائه‌دهنده منابع در هنگام ارسال یک کار و تحویل کار به کاربر است. برای‌این ویژگی، مقدار بازده چرخش زمانی ۱ خواهد بود که زمان چرخش وعده داده‌شده بیشتر از زمان چرخش واقعی باشد و زمانی ۰ خواهد بود که زمان چرخش وعده داده‌شده کمتر از زمان چرخش واقعی باشد. بهره‌وری چرخشی شامل قدرت محاسبات و سرعت شبکه می‌باشد. مقدار بهره‌وری چرخشی ارائه‌دهندگان از رابطه (۴) قابل‌محاسبه می‌باشد [۱۰].

$$TE_{(job,Rk)} = \frac{\text{زمان چرخشی وعده داده شده منبع } R_k \text{ در SLA}}{\text{زمان چرخشی واقعی منبع } R_k \text{ برای تکمیل کار}} \qquad (۴)$$

ارزیابی اعتبار منبع[1]: ارزیابی اعتبار منبع، از عامل اجرای وظیفه ضروری‌تر است. یک سازمان معتبر، به‌منظور حفظ شهرت خوب خود، معمولاً به سامانه و یا وظایف سایر کاربران آسیب نمی‌زند. با فرض این‌که منبع همیشه به‌خوبی رفتار کرده و هرگز رفتار و کارهای حاوی کدهای مخرب انجام نداده است؛ بنابراین، رفتار آینده آن به‌طورکلی معتبر است. مقدار ارزیابی اعتباری منابع ارائه‌دهندگان از رابطه (۵) به‌دست می‌آید.

$$S_i = \sum_{k=1}^{m} S_{k,i}(-t_{k,i}) \qquad (۵)$$

$t_{k,i}$ درجه رفتار مخرب از کدهایی که در عامل اجرای وظیفه وجود دارد و $S_{k,i}$ مقیاس محاسباتی وظایف و m اشاره به زمانی دارد که وظایف به منبع داده‌شده است [۱۴]. بیشینه مقدار زمانی خواهد بود که کدها عادی و بدون هیچ‌گونه رفتار مخرب باشند؛ آنگاه امتیاز برابر با ۱ خواهد بود و درصورتی‌که کدهایی برای حمله به‌کل محیط فرستاده شود امتیاز برابر با کمینه مقدار یعنی ۰ خواهد بود.

سابقه[2]: سابقه اعتبار ارائه‌دهندگان خدمات ابری مختلف، مهم است و ارزیابی اعتبار مالک به‌صورت استاندارد، با توجه‌به پیشینه ارائه‌دهنده و سوابق تاریخی آن‌است. مقدار سابقه ارائه‌دهندگان از رابطه (۶) به‌دست می‌آید.

$$H_j = \sum_{k=1}^{n} (-x_{k,i}) \qquad (۶)$$

$x_{k,i}$ درجه‌ی رفتار مخرب گره j ام و n مدت‌زمانی ست که اجرا می‌شود [۱۴]. بیشینه مقدار زمانی خواهد بود که کد عادی، بدون هیچ‌گونه رفتار مخرب در آن رخ دهد که برابر با ۱ خواهد بود و درصورتی‌که کدهای مخرب برای حمله به‌کل محیط فرستاده شوند برابر با مقدار کمینه یعنی ۰ خواهد بود.

شفافیت[3]: برای به‌دست آوردن اعتماد به ارائه‌دهنده خدمات، کاربران ابر باید اطمینان حاصل کنند که خدمات ارائه‌شده در توافق‌نامه سطح خدمات، واقعی و تضمین شده است [۱۶]. انجام شرایط و ضوابط در توافق‌نامه بین ارائه‌دهنده و کاربر، می‌تواند خدمات را قابل اعتمادتر نماید.

پرسش‌نامه خودارزیابی[4]: به صورت فهرست[5] در دسترس عموم می‌باشد. در پرسشنامه‌های طرح ارزیابی اجماع[6] یا ابر کنترل

1- Source Credibility
2- History
3- Transparencies
4- Self-assessment questionnaires
5- Registery
6- CAIQ

ماتریس[1] ارائه‌دهندگان خدمات ابر اجازه برای انتشار یک خودارزیابی و کنترل‌های امنیتی خوددارند. طرح ارزیابی اجماع شامل بیش از ۱۴۰ سؤال در یک صفحه گسترده است [۱۶]. ارائه تعدادی از سؤالات، بله/ خیر که کاربران ابر و یا حسابرسان ممکن است مایل به پرس‌وجو باشند. این پرسشنامه وسیله‌ای برای ارزیابی شایستگی ارائه‌دهندگان با ویژگی‌های مختلف است. همچنین ارزیابی قابلیت‌های امنیتی ارائه‌دهنده ابر را فراهم می‌نماید. اگر فراهم‌کنندگان ابری از پرسشنامه طرح ارزیابی اجماع یا ابر کنترل ماتریس استفاده نمایند ارزش عددی برابر با ۱ خواهد بود و درصورتی‌که از پرسشنامه‌ها استفاده نکند ارزش عددی برابر با ۰ خواهد بود.

حسابرسی[2]: ارائه‌دهندگان ابر استفاده از استانداردهای مختلف حسابرسی را در مورد خدمات و سیستم عامل‌های ارائه‌شده برای کاربران تضمین می‌کند. استانداردهایی برای سازمان‌های خدماتی توسط هیئت استاندارد حسابرسی[3] که موسسه انجمن آمریکایی حساب‌رسان رسمی می‌باشد[4] تعریف شده است [۱۶]. استاندارد گزارش تضمین[5]، استاندارد خودارزیابی[6]، یک رابط مشترک و فضای نام برای ارائه‌دهندگان برای تولید حسابرسی فراهم می‌کنند تا کاربران به‌طور خودکار از آن داده‌ها در فرآیندهای حسابرسی خود استفاده کنند. اگر فراهم‌کنندگان ابری استانداردهای حسابرسی به‌کاربرند ارزش این ویژگی برابر با ۱ خواهد بود و اگر فراهم‌کنندگان ابری از استانداردهای حسابرسی استفاده ننمایند ارزش این ویژگی برابر با ۰ خواهد بود.

اعتماد عینی[7]: برای یک کاربر خاص، مقادیر صفات توافق شده در مورد ارائه‌دهندگان خدمات ابری وجود دارد. مقادیر مشاهده‌شده از صفات فراهم‌کنندگان ابری، در طول تعامل با یک کاربر ابری به‌دست می‌آید [۱۶].

بازخورد کاربر[8]: کاربر، بعد از مصرف خدمات، امتیاز بازخورد را بر مبنای عملکرد خدمات ابر می‌دهد. امتیاز بازخورد، درک هر کاربر در مورد خدمات استفاده شده است. کاربر، بعد از هر تعامل با خدمات، امتیاز خود را که دلیل بر سطح رضایت اوست می‌دهد. ارزیاب اعتماد، امتیاز بازخورد را جمع‌آوری کرده و محاسبه می‌کند و درنهایت اعتبار خدمات را سنجیده و نمرات را در مخزن اعتماد به‌روزرسانی می‌کند. نمرات از رابطه (۷) به‌دست خواهد آمد.

1- CCM
2- Audit
3- ASB
4- AICPA
5- ISAE3402
6- STAR
7- Objective trust
8- User feedback

$$R(P_i,S_j)^x = \beta_{cur} \times F(P_i,S_j)^x + \frac{B_{pre}}{n} \times \sum_{k=1}^{n} PR_x(P_i,S_j)^x$$

$$RT(P_i,S_j) = \frac{1}{p} \times \sum_{l=1}^{p} R(P_i,S_j)^l \qquad (۷)$$

$$OT(P_i,S_j) = \omega_{ct} \times CT(P_i,S_j) + \omega_{rt} \times RT(P_i,S_j)$$

$F(P_i,S_j)^x$ بازخورد کاربر x در مورد سرویس S_j در تراکنش فعلی می‌باشد. N تعداد کل تراکنش‌ها و یا تعداد دفعاتی که کاربر x نرخ سرویس S_j را دارد و $PR_x(P_i,S_j)^x$ بازخورد کاربر x در k امین فعل‌وانفعالات است [۱۶]. نمرات به‌دست‌آمده، نقش مهمی در کشف خدمات ابری باز می‌کند و ارزش بازخورد، عددی در بازه ۰ و ۱ خواهد بود. ۱ به معنای رضایت شدید و ۰ به معنای نارضایتی شدید است.

پشتیبانی مشتری[9]: زمانی که مشتری نیاز به‌خدمات دارد می‌بایست از طرف ارائه‌دهنده ابری، پشتیبانی و کمک شود. سپس باید یک‌راهی برای حل‌وفصل موضوع موردنیاز مشتری وجود داشته باشد و ارائه‌دهنده آن را برآورده سازد. سازمان باید بهترین تجربه را به مشتریان خود با توجه به زمان، مکان و پشتیبانی موردنیاز آنها انجام دهد [۱۳]. اگر از طرف ارائه‌دهنده، خدمات پشتیبانی انجام شود امتیاز ۱ به آن تعلق می‌گیرد و اگر ارائه‌دهنده خدمات ابری، کاربر را پشتیبانی نکند امتیاز ۰ تعلق خواهد گرفت.

عملکرد در خدمات خاص: یک ارائه‌دهنده خدمات ابری ممکن است، شهرت[10] بسیار خوبی در ارائه یک خدمت خاص داشته باشد، پس در اولویت انتخاب قرار می‌گیرد. ازاین‌رو، لازم است مشتری، به‌جای‌اینکه ارائه‌دهندگان مختلف را انتخاب کند، همان ارائه‌دهنده را برای همان خدمت برگزیند [۱۳]. اگر ارائه‌دهنده خدمات شهرت خوبی در خدمت‌رسانی داشته باشد، امتیاز ۱ به آن تعلق می‌گیرد و اگر شهرت خوبی در خدمت‌رسانی نداشته باشد، امتیاز ۰ تعلق خواهد گرفت.

زمان تأخیر (زمان پاسخ‌دهی): زمانی که درخواست یا پرس‌وجویی به ارائه‌دهنده فرستاده می‌شود، ممکن است زمانی به‌اندازه چند دقیقه، یک ساعت و شاید چند روز طول بکشد تا پاسخ دهد و این بستگی به نوع درخواست دارد [۱۳]. وظایف مختلف ممکن است در زمان‌های مختلف حل و فصل شود و هر ارائه‌دهنده که در کمترین زمان به درخواست‌ها پاسخ دهد به‌عنوان ارائه‌دهنده‌برتر برگزیده می‌شود و در اولویت انتخاب است. ۴ ویژگی در نظر گرفته‌شده برابر خواهد بود با تأخیر بازمان مناسب، تأخیر بازمان متوسط، تأخیر بازمان کم و تأخیر بازمان

9- Customer support
10- Reputation

زیاد که امتیاز در نظر گرفته‌شده به ترتیب برابر با ۱، ۰/۷۵، ۰/۵، ۰/۲۵ می‌باشد.

تحمل خطا[1]: خطاهای بسیاری وجود دارد که سامانه با آنها روبه‌رو می‌شود، گاهی اوقات این خطاها به‌طور مستقیم بر روی خدمات در حال ارائه تأثیر می‌گذارد. هرگونه وقفه در خدمات، قابل‌تحمل نیست؛ بنابراین، می‌بایست یک برنامه قدرت جایگزینی برای اطمینان از دسترس بودن خدمات را داشته باشد. برای محاسبه تعداد شکست‌ها می‌بایست امتیاز برای قدرت جایگزینی، امتیاز برای پشتیبان‌گیری تسهیلات و امتیاز برای قابلیت تحمل خطا در نظر گرفته شود و درنتیجه، ارائه‌دهنده‌ای که کمترین شکست را داشت تحمل خطای بیشتری خواهد داشت و به‌عنوان ارائه‌دهنده برتر انتخاب می‌شود و مقدار ۱ می‌گیرد، در غیر این صورت مقدار ۰ می‌گیرد. محاسبه میزان تحمل خطای ارائه‌دهندگان توسط رابطه (۸) امکان‌پذیر خواهد بود.

(۸)

$$FTC = \frac{FT}{N}$$

که در آن، FT حاصل جمع امتیاز پشتیانی و توان جایگزینی است و N تعداد کل شکست‌ها است [۱۳].

به‌روزرسانی برنامه‌های کاربردی[2]: یکی از مهم‌ترین ویژگی‌های ارائه‌دهنده خدمات، به‌روزرسانی برنامه‌های کاربردی می‌باشد که این خدمت توسط، ارائه‌دهنده‌ها به مشتری ارائه می‌شود. قابلیت دسترسی برنامه‌های کاربردی و یا به‌روزرسانی نرم‌افزار و مدیریت آن از خدمات این ویژگی است. اگر نسخه به‌روزرسانی شده‌ی برنامه کاربردی در دسترس نباشد بر روی درجه‌بندی و شهرت سامانه تأثیر مستقیم و غیرمستقیم می‌گذارد [۱۳]. اگر مجموع به‌روزرسانی در زمان کمتری انجام شود ارائه‌دهنده امتیاز ۱ می‌گیرد، در غیر این صورت امتیاز ۰ می‌گیرد. نتایج در جدول (۱۲) قابل‌مشاهده می‌باشد.

خرابی[3]: فعال نگه‌داشتن همیشگی سامانه و ارائه خدمات مستمر به مشتریان امری بسیار ضروری است به‌خصوص درزمانی که به آن نیاز شدید می‌باشد و ساعات اوج نیاز است، خرابی باید به‌حداقل برسد و ارائه‌دهنده خدمات از قبل برای زمان خاموشی سامانه ، ارتقا، تعمیر و نگهداری برنامه‌ریزی نماید. ارائه‌دهنده برای خرابی چهار مؤلفه را در نظر می‌گیرد که شامل قطع و خرابی در اوج نیاز، قطع و خرابی در غیر اوج نیاز، قطع و خرابی ناخواسته در اوج نیاز و قطع و خرابی ناخواسته در غیر اوج نیاز است. درنهایت این مؤلفه‌ها باهم جمع گردیده و نسبت به‌کل زمان مصرفی، خرابی به‌دست می‌آید. اگر زمان کمتری داشته باشد، ارائه‌دهنده امتیاز ۱ می‌گیرد و اگر زمان تعمیر خرابی زیاد باشد مقدار ۰ می‌گیرد. مقدار خرابی ارائه‌دهندگان از رابطه (۹) به‌دست می‌آید.

$$TruA = \sum_{i=1}^{n} D_{pph(i)} \qquad (۹)$$

$D_{pph(i)}$ برابر با میزان ساعت‌های اوج خرابی واردشده توسط کاربر می‌باشد و n برابر با تعداد کاربران خواهد بود [۱۳].

ارزش اعتماد یک منبع[4]: ارزش اعتماد یک منبع از مجموع چهار وزن مثبت ویژگی‌های اعتماد است. این ویژگی‌ها؛ چرخش بهره‌وری *(TE)*، قابلیت اطمینان *(RE)*، یکپارچگی اطلاعات *(DI)* و در دسترس بودن *(AV)* است. مقدار ارزش اعتباری یک منبع از رابطه (۱۰) قابل‌محاسبه خواهد بود [۱۰].

$$\text{Trust Value of a resource} = w1 \times AV + w2 \times RE + w3 \times DI + w4 \times TE \qquad (۱۰)$$

w نشان‌دهنده وزن‌های اختصاص داده‌شده به هر ویژگی است که $w_1+w_2+w_3+w_4=1$ خواهد بود. اعتماد به منبع با استفاده از چهار ویژگی با وزن‌های مثبت به‌دست می‌آید. اگر منبع ابری دارای این چهار ویژگی باشد امتیاز ۱ خواهد گرفت و اگر منبع ابری دارای این چهار ویژگی نباشد امتیاز ۰ خواهد گرفت.

کیفیت خدمات[5]: کیفیت خدمات در کل، مجموع وزن‌های مثبت از ویژگی‌های اعتماد است. این ویژگی‌ها؛ قابلیت دسترسی *(AV)*، قابلیت اطمینان *(RE)*، یکپارچگی داده‌ها *(DI)*، چرخش بهره‌وری *(TE)* و منبع با بالاترین اطمینان *(TR)* می‌باشد. مقدار کیفیت خدمات منابع ارائه‌دهندگان از رابطه (۱۱) قابل‌محاسبه خواهدبود [۱۰, ۲۲].

$$\text{Quality of service} = w1 \times AV + w2 \times RE + w3 \times DI + w4 \times TE + w5 \times TR \qquad (۱۱)$$

w نشان‌دهنده وزن‌های اختصاص داده‌شده به هر ویژگی است که $w_1+w_2+w_3+w_4+w_5=1$ خواهد بود. کیفیت خدمات‌رسانی با استفاده از پنج ویژگی با وزن‌های مثبت به‌دست می‌آید. اگر منبع ابری دارای این پنج ویژگی باشد امتیاز برابر با ۱ خواهد بود و اگر منبع ابری دارای این پنج ویژگی نباشد امتیاز آن منبع برابر با ۰ خواهد بود.

1- Fault tolerance
2- Application update
3- Downtime
4- Trust Value of a resource
5- QualityOf Service

امنیت[1]: امنیت در سه سطح، احراز هویت (At)، مجوز (Au) و یکپارچگی داده‌ها (DI) است. احراز هویت درواقع بررسی نمودن ورود کاربر و به‌رسمیت شناخته شدن او در ابر است. مجوز، اشاره به قوانینی دارد که کاربر مجاز به انجام آن‌کارها است. مثال: ایجاد و حذف پایگاه داده، مجوز خواندن یا نوشتن است. یکپارچگی داده‌ها قبلاً توضیح داده‌شده است. محاسبه امنیت فراهم‌کنندگان ابری از رابطه (۱۲) محاسبه می‌شود [۲۳].

$$Security = w1 \times At + w2 \times Au + w3 \times DI \qquad (۱۲)$$

W، نشان‌دهنده وزن‌های اختصاص داده‌شده به هر ویژگی است که $w_1+w_2+w_3 =1$ خواهد بود. اگر فراهم‌کننده ابری هر سه پارامتر را داشته باشد امتیاز ۱ به آن تعلق خواهد گرفت. اگر دو پارامتر را داشته باشد امتیاز آن برابر با ۰/۷۵ خواهد بود. اگر یکی از پارامترها را داشته باشد امتیاز ۰/۵ و اگر پارامتری نداشته باشد برابر با ۰ خواهد بود.

توافق‌نامه سطح خدمات[2]: عامل مذاکره بین ارائه‌دهنده خدمات و مصرف‌کننده خدمات می‌باشد. موافقت‌نامه یکی از چندین نمونه برنامه‌هایی است که می‌تواند بسیاری از مشکلات کاربران را مهار نماید. مصرف‌کنندگان ابری، مشکلاتی از قبیل اقدامات امنیتی، در دسترس نبودن داده‌ها، هزینه‌های پنهان و زیرساخت‌های غیر شفاف دارد. یک ارائه‌دهنده خدمات ابری، می‌بایست خدمات خود را در توافق‌نامه سطح خدمات با اعتماد ثبت کند. در توافق‌نامه بین کاربر و ارائه‌دهنده خدمات ابری می‌بایست کیفیت خدمات ابری، تائید و نظارت بر سطح توافق خدمات لحاظ شود که به‌منظور نظارت بر توافق‌نامه‌ی خدمات، شخص ثالث حرفه‌ای نیاز است. میزان توافق‌نامه سطح خدمات فراهم‌کنندگان از رابطه (۱۳) محاسبه می‌شود [۲۳-۲۲].

$$SLA = w1 \times MV + w2 \times QOS \qquad (۱۳)$$

MV مجوز نظارت و QOS کیفیت خدمات فراهم‌کننده ابری خواهد بود. $\boldsymbol{w}$ نشان‌دهنده وزن‌های اختصاص داده‌شده به هر ویژگی است که $w_1+w_2= 1$ خواهد بود. اگر فراهم‌کننده دارای مجوز نظارت و کیفیت خدمات باشد امتیاز برابر ۱، اگر دارای مجوز نظارت باشد امتیاز برابر با ۰/۷۵، اگر دارای کیفیت خدمات باشد امتیاز برابر ۰/۵ و اگر هیچ‌کدام را نداشته باشد امتیاز برابر با ۰ خواهد بود.

شهرت: شهرت را می‌توان به کاربران جدید ابری و یا کاربرانی که در حال برنامه‌ریزی برای برخورداری از خدمات بسیار مفید هستند، توصیه نمود. باور کاربر ابری و نمرات شهرت وابسته‌به اعتماد کاربر، به‌طورمعمول در منبع اطلاعات یک کارگزار ابری خواهد بود. اعتماد و شهرت باهم مرتبط هستند؛ شهرت از خدمات ابری یا ارائه‌دهندگان ابری، تحت تأثیر انتخاب خدمات ابری توسط کاربران می‌باشد. شهرت ارائه‌دهندگان خدمات ابری نشان‌دهنده نمای کلی از یک جامعه است که به‌سمت آن هدایت‌شده است و به‌همین دلیل بیشتر برای کاربران ابری در انتخاب یک خدمت ابری از گزینه‌های بسیار خاص و مفید می‌باشد. ویژگی موردنظر ناکافی است و در کنار اعتماد به عملکرد خدمات و قابلیت اطمینان تکمیل خواهد شد. میزان شهرت ارائه‌دهندگان از رابطه ذیل قابل‌محاسبه خواهد بود [۲۲].

$$RP = w1 \times R + w2 \times P \qquad (۱۴)$$

R نشان‌دهنده قابلیت اطمینان و P نشان‌دهنده عملکرد بهینه است. $\boldsymbol{w}$ نشان‌دهنده وزن‌های اختصاص داده‌شده به هر ویژگی است که $w_1+w_2= 1$ خواهد بود. اگر اعتماد به عملکرد و قابلیت اطمینان باهم باشد امتیاز برابر ۱ خواهد بود. اگر یکی از پارامترهای عملکرد و قابلیت اطمینان باشد امتیاز برابر با ۰/۵ و اگر هیچ‌کدام نباشد برابر با ۰/۲۵ خواهد بود.

سیاست: از مکانیسم‌های اعتماد برای حمایت از امضای دیجیتال، صدور گواهی‌نامه‌های کلیدی و اعتبار می‌باشد که می‌تواند، یک بیانیه‌ی اساسی از استانداردهای پایه باشد و یک کلید عمومی را با یک موضوع پیوند دهد. اعتبارسنجی این ویژگی در اعتماد به مرجع صدور گواهی‌نامه[3] است [۲۲]. اگر امضای دیجیتال و صدور گواهی‌نامه از مرجع معتبر باشد، امتیاز ۱ به ارائه‌دهنده تعلق خواهد گرفت. اگر تنها صدور گواهی‌نامه از مرجع معتبر باشد امتیاز ۰/۷۵ و اگر امضای دیجیتال از مرجع معتبر باشد امتیاز ۰/۵ به آن تعلق خواهد گرفت.

گواهی‌نامه[4]: منابع ابری نیاز به صفات قابل‌اعتماد دارد. صدور گواهی‌نامه به‌منظور احراز هویت و مجوز استفاده می‌شود. ویژگی گواهی ازجمله هویت دسترسی و اطلاعات احراز هویت (نام کاربری، رمز عبور عضویت در گروه) را می‌توان مانند استانداردهای صدور گواهی‌نامه دریافت کرد. گواهینامه مدنظر IETFX.509 SSL خواهد بود [۲۲]. اگر گواهینامه ارائه‌کننده احراز هویت، مجوز هویت دسترسی و اطلاعات احراز هویت را داشته باشد امتیاز برابر با ۱ خواهد بود اگر دارای گواهی احراز هویت، مجوز، هویت دسترسی باشد امتیاز برابر با ۰/۷۵، دارای گواهی احراز هویت، مجوز باشد امتیاز برابر با ۰/۵ و درنهایت فقط دارای اطلاعات احراز هویت باشد امتیاز ۰/۲۵ تعلق خواهد گرفت.

1- Security
2- Service Level Agreement (SLA)
3- ETF/RFC 5280
4- Certified

قیمت: مقدار دلار برای به اشتراک‌گذاری از یک خدمت ابری می‌باشد [۱۰]. اگر در مقایسه باقیمت‌های گذاشته‌شده برای خدمات ابری، قیمت مناسبی داشته باشد امتیاز ۱ می‌گیرد و اگر گران‌تر باشد امتیاز ۰ می‌گیرد.

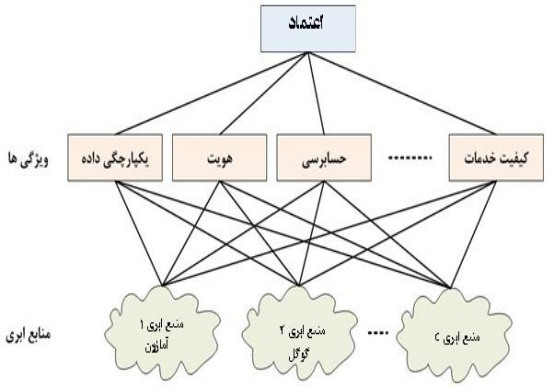
سرعت شبکه: سرعت شبکه دارای دو ویژگی پهنای باند و تأخیر شبکه است [۱۰]. اگر پهنای باند بالا و تأخیر شبکه کم باشد، امتیاز ۱ می‌گیرد. اگر پهنای باند کم و تأخیر زیاد باشد، امتیاز ۰ می‌گیرد.

هویت[1]: ارائه مجوز نشانه‌گذاری، احراز هویت open ID و مجوزسنجی open ID، تائید هویت شخصی از کارمندان، پیمان‌کاران و امنیت همگی تأییدیه استاندارد دارند [۱۰]. اگر ارائه مجوز نشانه‌گذاری، احراز هویت، تائید هویت و امنیت داشته باشد امتیاز ۱، اگر ارائه مجوز نشانه‌گذاری، احراز هویت، تائیدهویت داشته باشد امتیاز ۰/۷۵، اگر ارائه مجوز نشانه‌گذاری، احرازهویت داشته باشد امتیاز ۰/۵ و درنهایت اگر امنیت باشد امتیاز ۰/۲۵ خواهد بود.

۳-۲-۳- فرآیند تحلیل سلسله‌مراتبی

فرآیند تحلیل سلسله مراتبی به‌دلیل به‌دست آوردن نظرات کارشناسان و خدمت‌گیرندگان ابری به‌کار گرفته‌شده است ولی باوجود پیچیدگی‌ها و تردیدها در تصمیم‌گیری‌های دنیای واقعی فرآیند سنتی سلسله مراتبی به‌دلیل استفاده از اعداد دقیق در مقایسه‌های زوجی و وجود مقیاس‌های نامتوازن به‌درستی آنها را منعکس نخواهدکرد. به‌همین دلیل ارائه قضاوت‌های فازی با اعتماد بیشتری همراه خواهد بود چراکه قضاوت‌ها در محدوده بازه‌ای خواهند بود نه یک عدد ثابت [۲۴]. تعیین مقدار وزن، بخش مهمی از اندازه‌گیری میزان اعتبارسنجی در شناسایی شبکه عصبی خواهد بود چراکه نگاشت صحیح ورودی به خروجی نیاز به تعیین وزن مناسب دارد. فرآیند تحلیل سلسله‌مراتبی یک‌روش تجزیه تحلیل تصمیم‌گیری وزن سلسله‌مراتبی است. روش پیشنهادی بر اساس روش سلسله مراتبی فازی چانگ خواهد بود:

مرحله ۱: ۲۸ ویژگی اعتبارسنجی به‌عنوان معیار ارزیابی هستند. برای انتخاب، معیار تصمیم‌گیری وجود دارد. انتخاب معیار، بخش اول تجزیه‌وتحلیل بوده که خروجی آن‌یک نمودار سلسله‌مراتبی خواهد بود. شکل (۱) نمودار سلسله مراتبی بوده که به‌منظور انتخاب ارائه‌دهندگان مورد اعتماد ابری، از مجموعه داده‌های فرضی (۲۸ ویژگی) روش پیشنهادی استفاده شده است.



شکل (۱): نمودار تحلیل سلسله مراتبی فازی

مرحله ۲: تعریف اعداد فازی به‌منظور انجام مقایسه‌های زوجی خواهد بود که مطابق رابطه (۱۵) خواهد بود.

$$\tilde{a}_{ij} = \begin{cases} 1 & i = j \\ \tilde{1} & i \neq j \end{cases} \qquad (۱۵)$$

مرحله ۳: تشکیل ماتریس زوجی ($\tilde{A}$) با کمک اعداد فازی. ماتریس مقایسه زوجی مطابق (۱۶) خواهد بود.

$$\tilde{A} = \begin{bmatrix} 1 & \tilde{a}_{12} & \tilde{a}_{13} \cdots & \tilde{a}_{1n} \\ \vdots & & \ddots & \vdots \\ \tilde{a}_{n1} & \tilde{a}_{n2} & \tilde{a}_{n3} \cdots & 1 \end{bmatrix} \qquad (۱۶)$$

مرحله ۴: محاسبه وزن (S_i) برای هر یک از سطرهای ماتریس مقایسه زوجی که با استفاده از رابطه (۱۷) خواهد بود.

$$S_i = \sum_{j=1}^{n} M \otimes \left[\sum_{i=1}^{n}\sum_{j=1}^{m} M\right]^{-1} \qquad (۱۷)$$

که در این رابطه، i نشانگر شماره سطر، j بیانگر شماره ستون، M اعداد فازی مثلثی ماتریس‌های مقایسه زوجی می‌باشد.

مرحله ۵: مقایسه نتایج بردار وزن با بازه‌ها به‌منظور محاسبه اعتماد بعد از محاسبه وزن‌ها بازه اعتماد روش پیشنهادی به شرح جدول (۱) خواهد بود [۲۵].

جدول (۱): بازه اعتماد ارائه‌دهنده خدمات ابری

بازه	میزان اعتماد	توضیح
۰ - ٪۲۵	خیلی کم	اگر نتیجه قابلیت اعتماد در این بازه قرار گیرد منبع غیرقابل پذیرش است.
٪۲۵ -٪۵۰	کم	اگر نتیجه قابلیت اعتماد در این بازه قرار گیرد قابلیت پذیرفته شدن ندارد.
٪۵۰ - ٪۷۵	خوب	اگر نتیجه قابلیت اعتماد در این بازه قرار گیرد پذیرفته‌شده است.
٪۷۵ - ٪۱۰۰	خیلی خوب	اگر نتایج قابلیت اعتماد در این بازه قرار گیرد کاملاً پذیرفته است.

1- Identity

۴-۲-۳- یادگیری شبکه عصبی

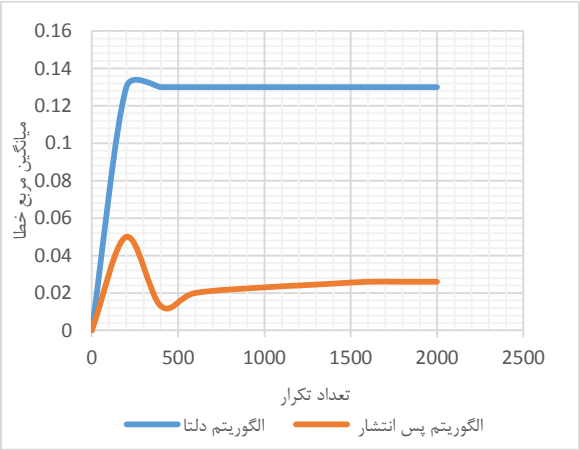
تعیین صحت ورودی و خروجی، نیاز به تعیین وزن مناسب برای شبکه‌های عصبی دارد. به‌روزرسانی وزن‌ها با آموزش و یادگیری شبکه در ارتباط هستند. شبکه با تطبیق قدرت وزن و بررسی الگوهای آموزشی ارائه‌شده بر اساس یک الگوریتم آموزشی خاص، یاد می‌گیرد. هدف اصلی از آموزش شبکه عصبی، کاهش خطا در خروجی شبکه با تنظیم وزن است. دو روش یادگیری برای یادگیری شبکه عصبی را می‌توان مورداستفاده قرارداد. برای یادگیری شبکه عصبی ازجمله: روش نظارت‌شده[۱] و نظارت‌نشده[۲] وجود دارد. در رویکرد نظارت‌شده، مجموعه‌ای از مثال‌های آموزشی همراه با خروجی موردنظر هر مثال دیده می‌شود. درحالی‌که درروش بدون نظارت، مثال‌های آموزشی بدون هیچ‌گونه اطلاعات در مورد خروجی، آن را فراهم می‌کند. رویکرد یادگیری نظارت‌شده که در آن‌یک خروجی مدنظر است و شناسایی و بهره‌وری شبکه را می‌توان با مقایسه خروجی شبکه موردنظر محاسبه کرد [۲۱]. برای شناسایی ارائه‌دهنده نامعتبر ابری، از روش نظارت‌شده زمانی استفاده می‌شود؛ چرا که خروجی موردنظر با هر نمونه آموزش ارائه شده است. درروش پیشنهادی یادگیری شبکه به‌این‌ترتیب است که یک ماتریس ۲۸ × **c** به‌صورت تصادفی با مقادیر ۰ و ۱ پر می‌شود. ۱ نشان‌دهنده وجود ارائه‌دهنده‌های ابری معتبر و ۰ نشان‌دهنده ارائه‌دهنده ابری نامعتبر است. قطر اصلی این ماتریس همیشه ۱ است. این ماتریس به‌صورت زیر است:

$$\begin{array}{c} \\ 1 \\ \vdots \\ C \end{array}\begin{array}{c} \begin{array}{ccc} 1 & \dots & 28 \end{array} \\ \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix} \end{array} \qquad (۱۸)$$

روش یادگیری به‌کار گرفته‌شده در این روش به‌دلیل داشتن دقت بالا در شبکه‌های چندلایه‌ای، یادگیری پس انتشار[۳] می‌باشد که بر اساس gradient descent، مربع خطای بین خروجی‌های شبکه و تابع هدف به‌حداقل خواهد رسید [۲۶]. این آموزش شامل سه مرحله می‌باشد:

۱- پیش‌خور نمودن الگوی آموزشی
۲- محاسبه و پس انتشار نمودن خطاها
۳- تنظیم وزن‌ها

شکل (۲) نتایج مقایسه حاصل از میانگین مربع خطای الگوریتم‌های یادگیری با نظارت چند لایه‌ای که شامل روش یادگیری دلتا و پس انتشار خطا می‌باشد را نشان می‌دهد [۳۰] و حاکی از آن می‌باشد که در روش پس انتشار خطا میزان میانگین مربع خطا کاهش یافته است و از دلایل اصلی انتخاب این روش می‌باشد.



شکل (۲): مقایسه میانگین مربع خطا الگوریتم یادگیری با نظارت دلتا و پس انتشار خطا

۵-۲-۳- پارامترهای شبکه عصبی

هدف اصلی از یادگیری شبکه، تعیین بردار وزن است. اندازه تنظیم برای وزن یادگیری، یک تابعی از پارامترهای مجموعه شبکه است. پارامترهای شبکه ازجمله: نرخ یادگیری[۴]، ارزش حرکت[۵] و آستانه خطا[۶] است. تنظیم وزن مدل پیشنهادی، توسط روش تحلیل سلسله‌مراتبی است. در [۲۱] به شرح پارامترهای شبکه عصبی پرداخته است که به شرح زیر است:

نرخ یادگیری: اتصال واحد مابین دو عصب است که پارامتری متناسب با هر ویژگی تعریف می‌شود و در گرادیان ضرب می‌شود. اگر اهمیت هر نمونه زیاد باشد این پارامتر باید نزدیک به ۱ باشد و اگر اهمیت هر نمونه کم باشد، این پارامتر باید کمتر باشد.

ارزش حرکت: معمولاً در طول فرآیند یادگیری یک وزن خاص افزایش می‌یابد؛ سپس تا آخر تنها افزایش می‌یابد و بالعکس. این پارامتر اینرسی حرکتی برای تغییر وزن‌هاست که سبب می‌شود با تعداد نمونه کمتر و در زمان کمتری سامانه به مرحله هم‌گرایی[۷] برسد.

اندازه دوران: مجموعه‌ای از عصب‌های ورودی در شبکه عصبی است که برای ورود به شبکه عصبی یا همان لایه ورودی شبکه انتخاب می‌شوند. تعداد دوران[۸] در دست کاربر است. منظور از

1- Supervised
2- unsupervised
3- Back Propagation

4- Learning rate
5- Momentum value
6- Error threshold
7- convergence
8- epoch

دوران یک گذر روبه‌جلو و یک گذر به عقب از تمام نمونه‌های آموزشی می‌باشد. درروش پیشنهادی مقدار اولیه برای این پارامتر صفر است.

آستانه خطا: عددی است که مقدار خطا با آن مقایسه می‌شود. در این روش آستانه خطا برابر با ۱۰٪ است. اگر نرخ خطای به‌دست‌آمده از شبکه عصبی از آستانه خطا بیشتر باشد، فراهم‌کننده ابری نامعتبر است و اگر کوچک‌تر باشد، فراهم‌کننده به‌عنوان معتبر طبقه‌بندی می‌شود.

مجموعه‌ای از پارامترها را باید از ابتدا به‌منظور ساخت یک مدل درست مشخص کرد. متأسفانه، شناسایی ساختار شبکه برای یک کاربرد خاص سخت است؛ که می‌تواند به‌صورت آزمون‌وخطا باشد. به‌طورکلی دستیابی به یک مجموعه داده‌ی بدون خطا دشوار است؛ بنابراین یک خطای قابل‌قبول باید در ساختمان کلی مدل در نظر گرفته شود. در مدل پیشنهادی ورودی شبکه عصبی، ماتریس حاصل از وزن دهی AHP به‌صورت ماتریس زیر خواهد بود. این ماتریس دارای ۲۸ ستون، حاوی ویژگی‌های ارائه‌دهندگان ابری و **C** سطر حاوی ارائه‌دهندگان خدمات ابری است که مطابق (۱۹) خواهد بود.

$$\begin{matrix} & F_1 & \dots & F_{28} \\ c_1 \\ \vdots \\ c_{1000} \end{matrix} \begin{bmatrix} w_1 & \cdots & w_{28} \\ \vdots & \ddots & \vdots \\ w_{1000} & \cdots & w_{28} \end{bmatrix} \qquad (۱۹)$$

۳-۲-۶- مراحل روش پیشنهادی

درکل، شناسایی ارائه‌دهندگان نامعتبر ابری، در طی مراحل زیر انجام می‌شود.

گام اول: فراخوانی مجموعه داده‌ها از پایگاه داده

گام دوم: تعیین وزن برای هریک از سطرهای جدول داده‌ها با روش فرآیند تحلیل سلسله‌مراتبی

گام سوم: محاسبه اعتماد برای هر ارائه‌دهنده خدمات ابری

گام چهارم: ایجاد ماتریس یادگیری و پر شدن ماتریس با مقادیر ۰ و ۱ تصادفی

گام پنجم: محاسبه میانگین سطرها

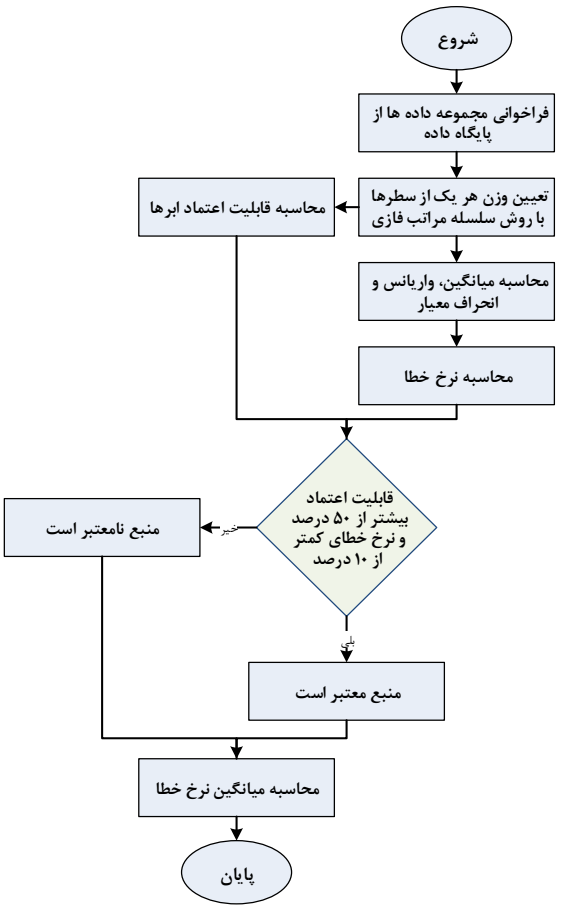
گام ششم: محاسبه نرخ خطای هر سطر

گام هفتم: اگر ارائه‌دهنده خدمات ابری دارای قابلیت اعتماد بالای ۵۰٪ و نرخ خطای زیر ۱۰٪ باشد، ارائه‌دهنده به‌عنوان پذیرفته‌شده معرفی می‌شود وگرنه پذیرفته نمی‌شود.

گام هشتم: تعداد ارائه‌دهنده‌های محاسبه‌شده با تعداد ارائه‌دهنده‌های معتبر فرضی AND می‌شود، اگر برابر با ۱ باشد، ارائه‌دهنده ابری معتبر است و اگر برابر با ۰ باشد نامعتبر است.

گام نهم: محاسبه میانگین نرخ خطای کل

نمودار روش پیشنهادی به‌صورت شکل (۳) است.



شکل (۳): نمودار روش پیشنهادی

۴- نتایج

در ادامه در این بخش به معرفی محیط شبیه‌سازی، پارامترهای شبیه‌سازی و نتایج حاصل پرداخته خواهد شد. در این پژوهش، به‌منظور شبیه‌سازی روش پیشنهادی نرم‌افزار کلاودآژور[1] به‌کار گرفته شده است؛ لازم به‌ذکر می‌باشد که عمل شبیه‌سازی در یک رایانه شخصی با حافظه اصلی چهار گیگابایتی و پردازنده ۲/۸GHz انجام گردیده است. با توجه به‌این‌که محاسبه مجموعه داده‌های نسبتاً بزرگ برای شناسایی ارائه‌دهندگان ابری دشوار است. از وزن‌دهی AHP برای دقت بالای وزن‌دهی و از شبکه عصبی برای شناسایی استفاده شده است. به‌منظور نمایش

1- Cloud Azure

خروجی امکانات اکسل و متلب به‌کار گرفته‌شده است. جهت انجام فرآیند شبیه‌سازی، راه‌کار پیشنهادی برروی تعداد مختلفی ارائه‌دهنده خدمات ابر فرضی، بررسی شده است. تمامی مقادیر مربوط به پارامترهای روش پیشنهادی، به‌صورت تصادفی تولید می‌شوند. درنهایت، راه‌کار پیشنهادی ازنظر درصد خطا و میزان دقت با سه روش مدیریت اعتماد برای محیط‌های چند ابری مبتنی‌بر ارائه‌دهندگان خدمات اعتماد [۱۴] و مدل ترکیبی برای ارزیابی پویا اعتماد در خدمات [۱۶] و تشخیص سرقت آنلاین[1] با استفاده از دامنه هدف [۲۷] مقایسه می‌گردد. پارامترهای شبیه‌سازی روش پیشنهادی در جدول (۲) نشان داده شده است. لازم به‌ذکر است که به‌منظور ارزیابی صحت نتیجه محاسبه‌شده با استفاده از روش پیشنهادی از مجموعه داده‌های شناخته‌شده cloud Amor[2] کمک گرفته شده است که از طریق آن ارائه‌دهنده‌های ابری شناسایی‌شده و براساس پارامترها مورد استفاده قرارگرفته است.

جدول (۲): پارامترهای شبیه‌سازی روش پیشنهادی

پارامتر	مقدار پارامتر	واحد
سرعت یادگیری	٪۸	درصد
ارزش حرکت	٪۱	درصد
ضریب اعتماد	٪۵۰	درصد
نرخ خطای مجاز	٪۱۰	درصد
epoch	۱۰۰۰	درصد
ویژگی‌ها	۲۸	عدد
ارائه‌دهندگان خدمات ابری(C)	۱۰۰۰	عدد

۴-۱- نتایج شبیه‌سازی

شبیه‌سازی بر روی مجموعه داده‌های فرضی که مقادیر پارامترها به‌صورت تصادفی تولید می‌شوند، در نظر گرفته شده است. مقادیر نرخ خطا و دقت سامانه با مدیریت اعتماد برای محیط‌های چند ابری مبتنی‌بر ارائه‌دهندگان خدمات اعتماد و مدل ترکیبی برای ارزیابی پویا اعتماد در خدمات ابری و تشخیص سرقت آنلاین با استفاده از دامنه هدف صورت می‌گیرد. برای محاسبه خطای احتمالی هر سطر باید میانگین هر سطر، واریانس و انحراف معیار آن محاسبه شود و درنهایت با حاصل‌ضرب ماتریس وزن‌دهی در ماتریس یادگیری، ضرب شود. برای محاسبه میانگین هر سطر از رابطه (۲۰) استفاده می‌شود [۲۸].

$$AVG(row) = \frac{\sum_0^1 x_i}{P} \qquad (۲۰)$$

که در آن، X نشان‌دهنده ارقام هر سطر، P تعداد ویژگی‌ها در مدل موردنظر است که برابر ۲۸ است.

برای محاسبه واریانس از رابطه (۲۱) استفاده می‌گردد.

$$S^2 = \frac{\sum_0^1 (x - \bar{x})}{N - 1} \qquad (۲۱)$$

و برای محاسبه انحراف معیار از رابطه (۲۲) استفاده می‌شود.

$$S.D = \sqrt{S^2} \qquad (۲۲)$$

و در نهایت محاسبه نرخ خطا از رابطه (۲۳) به‌دست می‌آید:

$$\text{Error rate= AHP_resualt[i] * (standard_dev) * (learnRate * momentum)) > (errorThresh))} \qquad (۲۳)$$

مربعات خطاها از رابطه (۲۴) به دست می‌آید:MSE

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(predicted\ valu - desired\ value)\, n \qquad (۲۴)$$

درواقع نتایج وزن‌دهی که از روش *AHP* به‌دست می‌آید را با انحراف معیار و سرعت یادگیری و ارزش حرکت محاسبه می‌کند. اگر نتایج حاصل، از آستانه خطا بیشتر باشد ارائه‌دهنده نامعتبر است و اگر کمتر از آستانه موردنظر باشد منبع معتبر است. نرخ خطای قابل‌قبول در این روش ٪۱۰ است. اگر خطای حاصل از شبکه عصبی از این آستانه تجاوز کند به‌عنوان منبع ابری نامعتبر تلقی می‌شود. درنهایت ارائه‌دهندگان ابری که قابل‌اعتماد هستند و نرخ خطای آن‌ها زیر ٪۱۰ است به‌عنوان ابر پذیرفته‌شده شناسایی می‌شوند. برای شناسایی معتبر بودن فراهم‌کنندگان ابری باید داده‌های ماتریس یادگیری که حاوی ۵۵۴ ابر معتبر است با ماتریس حاصل از تشخیص شبکه عصبی AND شود؛ اگر مقدار برابر با ۱ شود معتبر است و اگر برابر با ۰ باشد نامعتبر شناسایی می‌شود.

جدول (۳): معتبر و نامعتبر بودن فراهم‌کنندگان ابری

ارائه‌دهندگان ابری	مقادیر ماتریس یادگیری	مقادیر ماتریس حاصل از شبکه عصبی	حاصل AND
ارائه‌دهنده ۱	۰	۱	۰
ارائه‌دهنده ۲	۰	۱	۰
ارائه‌دهنده ۳	۱	۱	۱
ارائه‌دهنده ۴	۰	۱	۰
ارائه‌دهنده ۵	۰	۱	۰
⋮	⋮	⋮	⋮
ارائه‌دهنده C	۱	۱	۱

1- phishing
2- https://cs.adelaide.edu.au/~cloudarmor/ds.html

برای محاسبه میانگین نرخ خطای کل از رابطه (۲۵) استفاده می‌شود.

$$\text{AVG(Error rate)} = \frac{\sum(error\ rate(Row))}{N} \qquad (۲۵)$$

Error rate (Row) نشان‌دهنده نرخ خطای هر سطر است و N تعداد کل ابرها را نشان می‌دهد.

برای نشان دادن درصد خطای کمتر روش پیشنهادی، روش موردنظر را با نرخ یادگیری‌های مختلف، آزمایش می‌کنیم. روش پیشنهادی با نرخ یادگیری ۰/۸، درصد خطای ۰/۰۰۵ دارد. جدول (۴) نتایج حاصل را نشان می‌دهد.

جدول (۴): نتایج حاصل از نرخ یادگیری مختلف

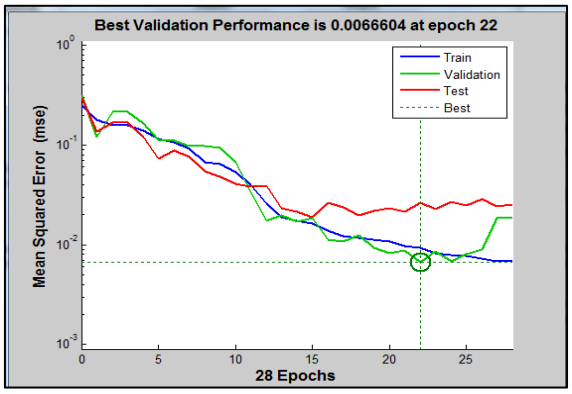
نرخ خطا	نرخ یادگیری
۰/۹۹	۰/۱
۰/۹۸	۰/۲
۰/۹۷	۰/۳
۰/۰۰۹	۰/۴
۰/۰۰۷	۰/۵
۰/۰۰۶	۰/۷
۰/۰۰۵	۰/۸

درصد خطا بستگی به معماری شبکه دارد. هرچقدر معماری شبکه بهتر باشد. درصد خطای کمتری به‌دست می‌آید. معماری‌های مختلف با تعداد نورون‌های پنهان مختلف آزمایش و اعتبارسنجی شده است تا بهترین شکل معماری به‌دست آید.

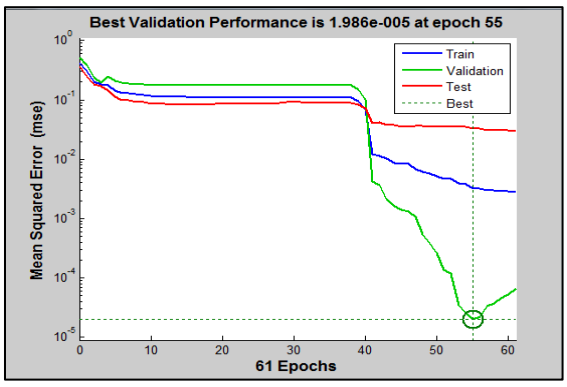
جدول (۵): نتایج حاصل از انواع معماری شبکه عصبی را نشان می‌دهد.

تعداد آموزش	تعداد عصب با لایه پنهان	میزان MSE
۷۷	۷	۷/۰۸۱
۵۵	۸	۱/۹۸
۲۳	۱۰	۰/۰۰۵
۲۲	۱۲	۰/۰۰۶
۱۷	۱۵	۰/۰۰۷
۲۶	۱۶	۰/۰۰۸

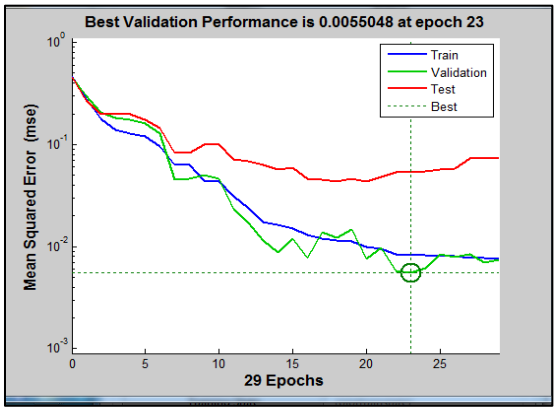
در ادامه آموزش شبکه با معماری‌های مختلف به شکل‌های زیر می‌باشد. شکل (۴) آموزش شبکه با ۲۲ دور را نشان می‌دهد در ادامه نتایج با دورهای مختلف از شکل‌های (۹-۵) نمایش داده می‌شود.



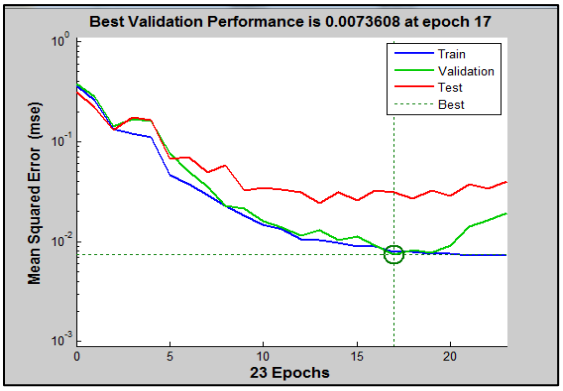
شکل (۴): آموزش با ۲۲ دور



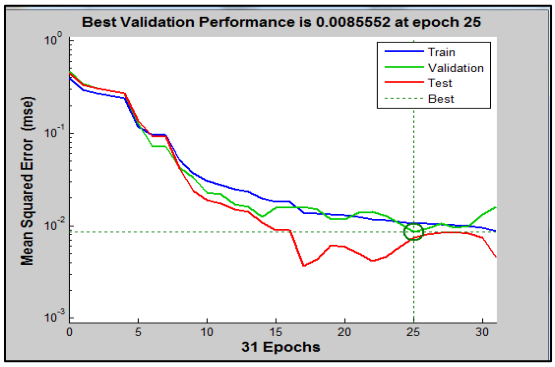
شکل (۵): آموزش با ۵۵ دور



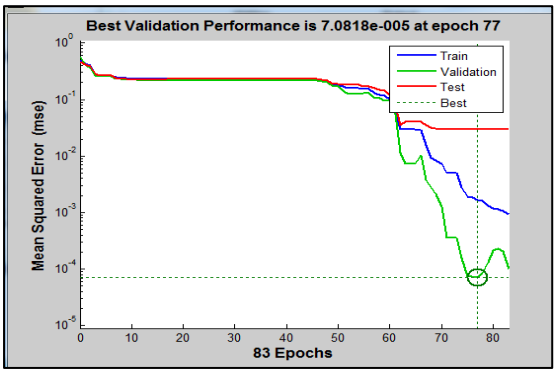
شکل (۶): آموزش با ۲۳ دور



شکل (۷): آموزش با ۱۷ دور

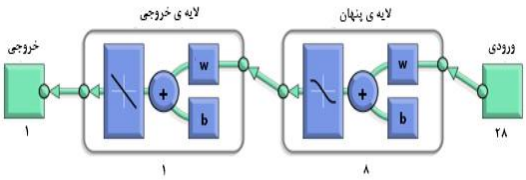


شکل (۸): آموزش با ۲۵ دور



شکل (۹): آموزش با ۷۷ دور

روش پیشنهادی در شکل (۳) با ۲۳ دور آموزش و دارای ۱۰ لایه پنهان و میانگین خطای مربع ۰/۰۰۵ را بهترین نوع معماری شبکه ارزیابی می‌کند. شکل (۱۰) شمای بهتری از معماری روش پیشنهادی است.



شکل (۱۰): شمای معماری با لایه پنهان

به‌منظور نشان دادن میزان دقت سامانه از سه معیار ارزیابی نرخ مثبت واقعی[1]، نرخ مثبت کاذب[2] و دقت[3] استفاده می‌شود که کارایی سامانه نام دارد [۲۷, ۲۹]. نرخ مثبت واقعی درروش پیشنهادی، تعداد ابرهای نامعتبری است که در طبقه‌بندیِ مجموعه داده‌ها درست شناسایی شده است. نرخ مثبت کاذب تعداد ابرهای معتبری هستند که اشتباه طبقه‌بندی شده‌اند. در ادامه، برای نشان دادن نرخ مثبت واقعی از رابطه (۲۶) استفاده می‌شود.

$$TPR = \frac{TP}{P} = \frac{TP}{(TP+FN)} \qquad (۲۶)$$

1- True positive rate
2- False positive rate
3- Accuracy

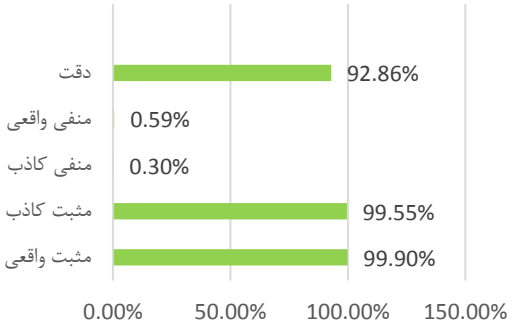
TP، تعداد ابرهای نامعتبر که درست تشخیص داده شده‌اند. P تعداد کل صفحات و FN تعداد از دست رفته‌ها را نشان می‌دهد. برای نشان دادن نرخ مثبت کاذب از رابطه (۲۷) استفاده شده است.

$$FPR = \frac{FP}{L} = \frac{FP}{(FP+TN)} \qquad (۲۷)$$

FP تعداد ابرهای معتبر هستند که اشتباه شناسایی شده‌اند. L تعداد ابرهای معتبر و TN ابرهایی که درست شناسایی شده‌اند؛ و درنهایت برای به‌دست آوردن دقت از رابطه (۲۸) استفاده شده است.

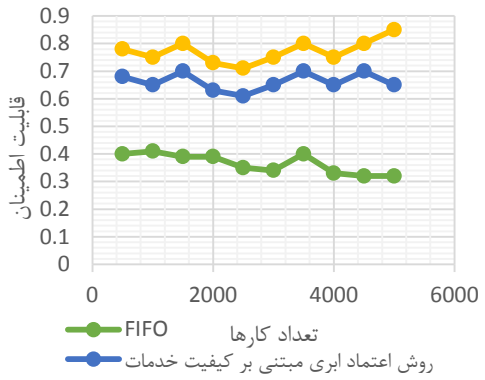
$$Acc = \frac{TP+TN}{P+L} \qquad (۲۸)$$

درروش پیشنهادی میزان، منفی واقعی[4] و منفی کاذب[5] صفر است و در نظر گرفته نمی‌شود. بهبود روش پیشنهادی با داشتن نرخ مثبت واقعی بالا و کاهش مثبت کاذب است. شکل (۱۱) کارایی سامانه را با توجه به سه معیار، نرخ مثبت واقعی، نرخ منفی واقعی و دقت نشان می‌شود.



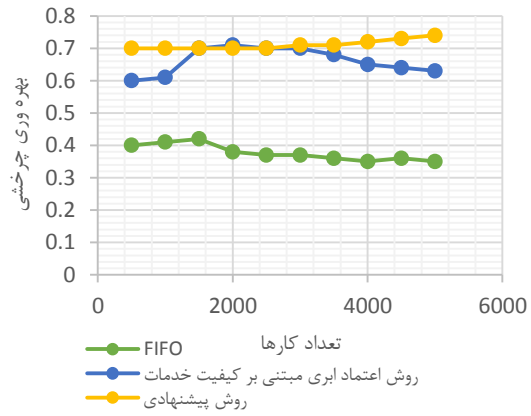
شکل (۱۱): کارآیی روش پیشنهادی

در ادامه مقایسه روش پیشنهادی از لحاظ کیفیت خدمات (شامل قابلیت اطمینان، بهره‌وری چرخشی و قابلیت دسترسی) با روش اعتماد مبتنی بر **FIFO** و روش مدل اعتماد ابری مبتنی بر کیفیت خدمات **[۱۰]** مقایسه گردیده (شکل‌های ۱۴-۱۲) که حاکی از بهبود کیفیت خدمات در روش پیشنهادی می‌باشد.

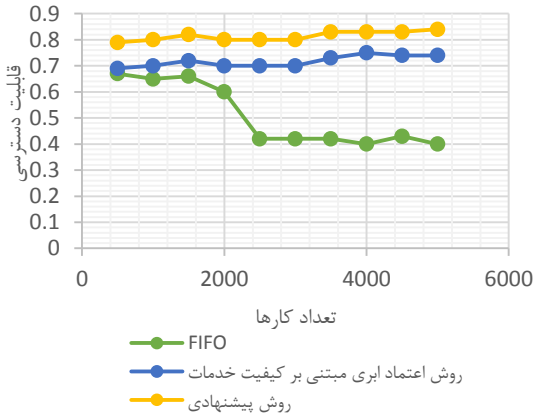


شکل (۱۲): مقایسه قابلیت اطمینان

4- True negative
5- False negative



شکل (۱۳): مقایسه بهره وری چرخشی



شکل (۱۴): مقایسه بهره وری چرخشی

۴-۲- مقایسه روش‌ها

مقایسه روش پیشنهادی با سه روش مدیریت اعتماد برای محیط‌های ابری مبتنی‌بر ارائه‌دهندگان خدمات اعتماد [۲۳]، مدل ترکیبی برای ارزیابی پویا اعتماد در خدمات ابری [۱۶] و روش مؤثر برای تشخیص صفحات جعلی وب از طریق دامنه [۲۷] است. تمامی مقادیر مربوط به پارامترهای روش پیشنهادی به‌صورت تصادفی تولید می‌شوند. در نهایت راه‌کار پیشنهادی ازنظر میزان خطا و دقت با روش‌های موجود مقایسه شده است.

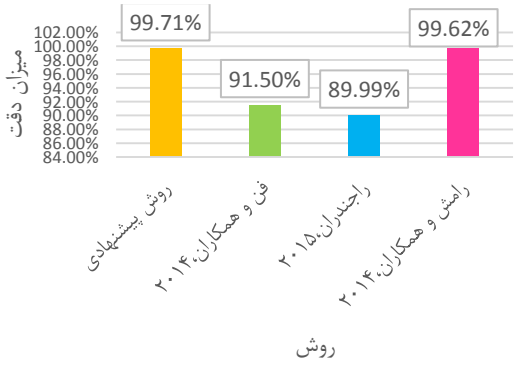
میزان خطا از رابطه (۲۹) به‌دست می‌آید.

$$\text{Error rate}=\left|\frac{computed\ trust-real\ trust}{real\ trust}\right| \qquad (۲۹)$$

مقایسه شبیه‌سازی نشان می‌دهد که درروش پیشنهادی میزان خطا نسبت به‌روش‌های مدیریت اعتماد برای محیط‌های چند ابری مبتنی‌بر ارائه‌دهندگان خدمات اعتماد و مدل ترکیبی برای ارزیابی پویا اعتماد در خدمات ابری و روش مؤثر برای تشخیص صفحات جعلی وب از طریق دامنه کمتر است. شکل (۱۵) نتایج حاصل را نشان می‌دهد که حاکی از آن می‌باشد که روش یادگیری در نظر گرفته‌شده در این شبیه‌سازی تأثیر به‌سزایی در کاهش نرخ خطا دارد.

شکل (۱۵): مقایسه نرخ خطا

دقت درروش پیشنهادی برابر ۹۹,۷۱٪ که نسبت‌به روش‌های مدیریت اعتماد برای محیط‌های چند ابری مبتنی‌بر ارائه‌دهندگان خدمات اعتماد و مدل ترکیبی برای ارزیابی پویا اعتماد در خدمات ابری و روش مؤثر برای تشخیص صفحات جعلی وب از طریق دامنه، به ترتیب ۹٪ و ۱۰٪ و ۰,۹٪ بیشتر است. شکل (۱۶)، نتایج حاصل را نشان می‌دهد.



شکل (۱۶): مقایسه دقت

بدین ترتیب روش پیشنهادی کمترین میزان خطا و بیشترین دقت را نسبت به سه روش مقایسه شده دارد.

۵- نتیجه‌گیری

در این پژوهش، راه‌کاری جدید به‌منظور شناسایی ارائه‌دهندگان ابری در جهت شناسایی ارائه‌دهنده نامعتبر ابری و اعتماد کاربران بر منابع ابری با درصد خطای کمتر ارائه شد. روش پیشنهادی در حالت کلی شامل دو مرحله می‌باشد؛ در مرحله اول، یک مجموعه داده فرضی وجود دارد و تعداد منابع ابری معتبر و نامعتبر

مشخص است که شامل ماتریس ۱۰۰۰*۲۸ بوده که دارای ۱۰۰۰ ابر و ۲۸ ویژگی است. مقادیر ویژگی با استفاده از تابع توزیع تصادفی در بازه ۰ تا ۱ تعریف گردیده‌اند. مدل شبکه عصبی در نظر گرفته‌شده محدود به سه لایه ورودی، پنهان و خروجی می‌باشد. به‌صورت پیش‌فرض برخی از ابرها دارای مقادیر ۱ و برخی دیگر دارای مقادیر ۰ می‌باشند که با مقدار خروجی AND شده و ابر معتبر یا نامعتبر مشخص می‌گردد. قابلیت اعتماد به هر منبع ابری با استفاده از روش وزن‌دهی سلسله مراتبی برای هر ابر محاسبه می شود، با توجه به مقادیر تعریف‌شده ویژگی‌ها، تعداد وزن میانگین به‌وسیله ماتریس زوجی مشخص می شود. قابلیت اعتماد درروش موردنظر ۵۰٪ است. در مرحله دوم، برای به‌دست آوردن ارائه‌دهندگان ابر نامعتبر از شبکه عصبی، وزن‌های به‌دست‌آمده از روش فازی به‌عنوان ورودی شبکه عصبی در نظر گرفته شده است. یادگیری شبکه، ماتریسی است که به‌صورت تصادفی از صفر و یک پر می‌شود. برای به‌دست آوردن نرخ خطای شبکه، ابتدا ماتریس به‌دست‌آمده از روش سلسله مراتبی را به ماتریس یادگیری ضرب می‌شود؛ سپس میانگین هر سطر، واریانس و انحراف معیار به‌دست می‌آید. و درنهایت نرخ خطا از حاصل ضرب ماتریس سلسله مراتبی در انحراف معیار در نرخ یادگیری در پس انتشار با گشتاور به‌دست می‌آید. آستانه خطای قابل‌قبول ۱۰٪ است. اگر ابری قابلیت اعتماد بالای ۵۰٪ را کسب کند و هم‌زمان نرخ خطای آن کمتر از ۱۰٪ باشد به‌عنوان ابر قابل قبول است. درنهایت برای شناسایی منابع ابری، ابرهای پذیرفته‌شده با ابرهای معتبر فرضی *AND* می‌شود. اگر حاصل ۰ شود به‌عنوان ابر نامعتبر شناسایی می‌شود و اگر ۱ باشد به‌عنوان ابر معتبر شناسایی می‌گردد. این روش با توجه به اینکه از چند معیار برای شناسایی منابع ابری استفاده می‌کند، ازاین‌رو امکان شناسایی با بهترین دقت را دارد؛ و از سوی دیگر با استفاده از این روی‌کرد میزان نرخ خطا کاهش و اعتماد به ارائه‌دهنده معتبر ابری افزایش می‌یابد. مهم‌ترین عیب روش بیش برازش[1] و آموزش بیش‌ازحد[2] می‌باشد.

به‌عنوان کارهای پژوهشی آینده به‌منظور بهبود عملکرد روش پیشنهادی می‌توان در طول مرحله یادگیری ضریبی تعریف شود به‌طوری‌که اگر وزن سلول عصبی ثابت بماند به‌تدریج آن را فرسوده و کم کند، به عبارتی داده‌هایی که مورداستفاده نیستند دچار نوعی فراموشی می‌شوند. به‌منظور کاهش سربار یادگیری، تعداد گره‌های هر لایه شبکه کم شود، به‌طوری‌که شبکه فضای کافی(حافظه کافی) برای به‌خاطر سپردن همه داده‌ها نداشته باشد و مجبور به تجزیه‌وتحلیل آنها شود و درنهایت به‌دلیل دشواری وزن‌دهی و به‌روزرسانی وزن‌ها، بهترین روش ممکن انتخاب شود.

1- Overfitting
2- Overtraining

۶- منابع

[1] F. J. Krautheim, "Building trust into utility cloud computing," University of Maryland, Baltimore County, 2010.

[2] F. N. Njeh, "Cloud Computing: An Evaluation of the Cloud Computing Adoption and Use Model," Bowie State University, 2014.

[3] I. M. Abbadi and M. Alawneh, "A framework for establishing trust in the Cloud," Computers & Electrical Engineering, vol. 38, pp. 1073-1087, 2012.

[4] F. Krautheim, D. Phatak, and A. Sherman, "Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing," Trust and Trustworthy Computing, pp. 211-227, 2010.

[5] N. Somu, K. Kirthivasan, and S. S. VS, "A computational model for ranking cloud service providers using hypergraph based techniques," Future Generation Computer Systems, vol. 68, pp. 14-30, 2017/03/01/ 2017.

[6] B. Keshanchi, A. Souri, and N. J. Navimipour, "An improved genetic algorithm for task scheduling in the cloud environments using the priority queues: Formal verification, simulation, and statistical testing," Journal of Systems and Software, vol. 124, pp. 1-21, 2017.

[7] F. Sheikholeslami and N. J. Navimipour, "Service allocation in the cloud environments using multi-objective particle swarm optimization algorithm based on crowding distance," Swarm and Evolutionary Computation, vol. 35, pp. 53-64, 2017/08/01/ 2017.

[8] A. Vakili and N. J. Navimipour, "Comprehensive and systematic review of the service composition mechanisms in the cloud environments," Journal of Network and Computer Applications, vol. 81, pp. 24-36, 2017/03/01/ 2017.

[9] M. Chiregi and N. J. Navimipour, "A comprehensive study of the trust evaluation mechanisms in the cloud computing," Journal of Service Science Research, vol. 9, pp. 1-30, June 01 2017.

[10] P. Manuel, "A trust model of cloud computing based on Quality of Service," Annals of Operations Research, vol. 233, pp. 281-292, October 01 2015.

[11] J. Urquhart, "The biggest cloud-computing issue of 2009 is trust," C-Net News, vol. 7, 2009.

[12] G. Lin, D. Wang, Y. Bie, and M. Lei, "MTBAC: A mutual trust based access control model in Cloud computing," China Communications, vol. 11, pp. 154-162, 2014.

[13] S. Jabbar, K. Naseer, M. Gohar, S. Rho, and H. Chang, "Trust model at service layer of cloud computing for educational institutes," The Journal of

[23] W. Fan and H. Perros, "A novel trust management framework for multi-cloud environments based on trust service providers," Knowledge-Based Systems, vol. 70, pp. 392-406, 2014/11/01/ 2014.

[24] Y.-M. Wang, Y. Luo, and Z. Hua, "On the extent analysis method for fuzzy AHP and its applications," European Journal of Operational Research, vol. 186, pp. 735-747, 2008/04/16/ 2008.

[25] H. Shakeri, A. G. Bafghi, and H. S. Yazdi, "Computing trust resultant using intervals," in 2011 8th International ISC Conference on Information Security and Cryptology, pp. 15-20, 2011.

[26] J. Leonard and M. A. Kramer, "Improvement of the backpropagation algorithm for training neural networks," Computers & Chemical Engineering, vol. 14, pp. 337-341, 1990/03/01/ 1990.

[27] G. Ramesh, I. Krishnamurthi, and K. S. S. Kumar, "An efficacious method for detecting phishing webpages through target domain identification," Decision Support Systems, vol. 61, pp. 12-22, 2014/05/01/ 2014.

[28] L. A. T. Nguyen, B. L. To, H. K. Nguyen, and M. H. Nguyen, "An efficient approach for phishing detection using single-layer neural network," In 2014 International Conference on Advanced Technologies for Communications (ATC 2014), pp. 435-440, 2014.

[29] K. Quinn, D. Lewis, D. O'Sullivan, and V. P. Wade, "An analysis of accuracy experiments carried out over of a multi-faceted model of trust," International Journal of Information Security, vol. 8, pp. 103-119, April 01 2009.

[30] K. Mahmood, A. Zidouri, and A. Zerguine, "Performance analysis of a RLS-based MLP-DFE in time-invariant and time-varying channels," Digital Signal Processing, vol. 18, pp. 307-320, 2008/05/01/ 2008.

Supercomputing, vol. 72, pp. 58-83, January 01 2016.

[14] X.-l. Xu, Q. Tu, N. Bessis, G. Yang, and X.-h. Wang, "SATVPC: Secure-agent-based trustworthy virtual private cloud model in open computing environments," Journal of Central South University, vol. 21, pp. 3186-3196, August 01 2014.

[15] M. R. Mosavi, M. Khishe, "The Use of Radial Basis Function Networks Based on Leader Mass Gravitational Search Algorithm for Sonar Dataset Classification," Journal Of Electronical & Cyber Defence, vol. 4, no. 2, 2016.(In Persian)

[16] V. Viji Rajendran and S. Swamynathan, "Hybrid model for dynamic evaluation of trust in cloud services," Wireless Networks, vol. 22, pp. 1807-1818, August 01 2016.

[17] H. Kim, H. Lee, W. Kim, and Y. Kim, "A trust evaluation model for QoS guarantee in cloud systems," International Journal of Grid and Distributed Computing, vol. 3, pp. 1-10, 2010.

[18] Z. Yang, L. Qiao, C. Liu, C. Yang, and G. Wan, "A collaborative trust model of firewall-through based on Cloud Computing," In The 2010 14th International Conference on Computer Supported Cooperative Work in Design, pp. 329-334, 2010.

[19] A. Sadeghi, M. R. Valavi, M. Asadi Vasfi, M. Barari, and G. Mohtashami, "A Method for Multilayer Computing of IT Services Availability," Journal Of Electronical & Cyber Defence,vol. 5, no. 3, 2017.(In Persian)

[20] S. Haykin, "Neural networks: a comprehensive foundation: Prentice Hall PTR," 1994.

[21] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Predicting phishing websites based on self-structuring neural network," Neural Computing and Applications, vol. 25, pp. 443-458, August 01 2014.

[22] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," Journal of Cloud Computing: Advances, Systems and Applications, vol. 2, p. 9, 2013.

Hybrid Method for Detecting Trustworthy Cloud Service Providers using Analytical Hierarchical Process and Neural Network

S. Tabaghchi Milan, N. Jafari Navimipour*

Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

(Received: 21/01/2018, Accepted: 27/05/2018)

ABSTRACT

Recently, cloud computing has become very popular. Due to this popularity, the number of cloud services' features is increasing continuously. To find a reliable provider in the cloud environment and select the best resources in the heterogeneous infrastructures, trust plays an important role. Customers distrust in cloud service providers is considered as a barrier to cloud service acceptance. This research develops a model for identifying invalid cloud service providers, in which validation is examined using cloud providers' trust evaluation features. In this approach, in order to detect cloud providers, the neural network method with a robust hierarchical weight estimation is proposed; analytical hierarchical process is being used for its capability in finding and detecting optimal values. The simulation results indicate an error rate of 0.055%, showing this method to be more accurate compared to the state-of-the-art methods.

Keywords: Cloud service, trust, neural network, analytical hierarchical process

* Corresponding Author Email: jafari@iaut.ac.ir