Scientific Journal of Electronical & Cyber Defence
Vol. 10, No. 4, Winter 2023, Serial No. 40

A Trust Evaluation Model for Cloud Computing Using Baysian Network

M. Hosseinnezhad, M. Abdollahi Azgomi*, M. R Ebrahimi Dishabi

* Professor, Miyaneh Branch, Islamic Azad University, Miyaneh, Iran

(Received: 01/02/2022, Accepted: 31/05/2022)

ABSTRACT

In recent years, cloud computing has attracted much attention as a new computing model for providing infrastructure, platform, and software as a service. There is an important challenge in trust management between cloud providers, service providers, and service applicants due to the industry's rapid adaptation of cloud computing. Trust management has become very challenging in cloud computing since cloud service applicants need to choose effective, reliable, and low-risk services. One of the most important factors, which can be considered in the applicant's trust or distrust of service, is the various parameters of service. Therefore, it is necessary to use approaches to evaluate the trust of the cloud services considering their service quality parameters and their identified performance requirements. In this paper, a model is introduced to evaluate the trust for the cloud services using Bayesian network. Since the trust actually deals with probabilities, and the Bayesian network also uses probabilities to solve the problems, the Bayesian network can be used to assess the trust. The proposed method is compared with various data mining techniques to assess trust in cloud services. The results show that the accuracy, absolute error, root mean square error, and square error in the Bayesian network are 94/53, 0/037, 0/137, and 0/038, respectively. The proposed method is more efficient than different data mining techniques for trust assessment in cloud services.

Keywords: Trust, Cloud Computing, Cloud Service, Data Mining, Bayesian Network, Service Quality.

* Corresponding Author Email: Azgomi@iust.ac.ir

This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

Publisher: Imam Hussein University © Authors

نشریه علمی "پدافند الکترونیکی و سایبری"
سال دهم، شماره ۴، زمستان ۱۴۰۱، ص ۶۱- ۵۳

علمی – پژوهشی

یک مدل ارزیابی اعتماد برای رایانش ابری با استفاده از شبکه بیزی

میهن حسین‌نژاد گرگری[۱]، محمد عبداللهی ازگمی[۲*]، محمدرضا ابراهیمی دیشابی[۳]

۱- دانشجوی دکترا، ۲- استاد، ۳- استادیار، واحد میانه، دانشگاه آزاد اسلامی، میانه، ایران

(دریافت: ۱۴۰۰/۱۱/۱۲، پذیرش: ۱۴۰۱/۰۳/۱۰)

چکیده

در سال‌های اخیر، رایانش ابری به‌عنوان یک الگوی رایانشی جدید برای ارائه زیرساخت، سکو و نرم‌افزار به‌عنوان سرویس توجه زیادی را به خود جلب کرده است. با توجه به تطبیق سریع رایانش ابری در صنعت، چالش مهمی در مدیریت اعتماد میان ارائه‌دهندگان ابر، ارائه‌دهندگان سرویس و درخواست‌کنندگان سرویس به وجود آمده است. در حقیقت، با در نظر گرفتن نیاز مبرم درخواست‌کنندگان سرویس در محیط ابر برای انتخاب سرویس‌های مؤثر، قابل‌اعتماد و کمتر مخاطره‌آمیز، مدیریت اعتماد در رایانش ابری بسیار چالش‌برانگیز شده است. یکی از مهم‌ترین عواملی که می‌تواند در اعتماد یا عدم اعتماد به یک سرویس از طرف درخواست‌کننده مدنظر قرار گیرد، پارامترهای مختلف کیفیت سرویس مربوط به سرویس موردنظر است؛ بنابراین، رویکردهایی موردنیاز است که اعتماد مربوط به سرویس‌های ابری را با توجه به مقادیر پارامترهای کیفیت سرویس آن‌ها و با در نظر گرفتن نیازمندی‌های کارایی مشخص‌شده آن‌ها ارزیابی کند. در این مقاله، مدلی برای ارزیابی اعتماد به کمک شبکه‌های بیزی برای سرویس‌های ابری ارائه شده است. با توجه به اینکه اعتماد در واقع با احتمالات سروکار دارد، شبکه بیزی نیز برای حل مسائل از احتمالات استفاده می‌کند، پس شبکه بیزی می‌تواند به کمک ارزیابی اعتماد بیاید. در ادامه برای مقایسه، از فن‌های مختلف داده‌کاوی جهت ارزیابی اعتماد در سرویس‌های ابری استفاده شده است. نتایج حاصل از ارزیابی نشان می‌دهد که پارامترهای دقت، خطای مطلق، خطای ریشه میانگین مربع و خطای مربع، در شبکه بیزی به ترتیب برابر ۹۴/۵۳، ۰/۰۳۷، ۰/۱۳۷ و ۰/۰۳۸ هست و نسبت به فنون مختلف داده‌کاوی برای ارزیابی اعتماد در سرویس‌های ابری کارایی بهتری دارد.

کلیدواژه‌ها: اعتماد، رایانش ابری، داده‌کاوی، سرویس ابری، شبکه بیزی، کیفیت سرویس

۱- مقدمه

رایانش ابری یک مدل جدید برای خدمات فناوری اطلاعات ارائه می‌کند. در این مدل‌ها، منابع مقیاس‌پذیر و مجازی از طریق اینترنت ارائه می‌شوند [۱]. در چنین سیستمی، کاربران سعی می‌کنند بر اساس نیازهای خود و بدون توجه به محل قرارگیری یک سرویس و یا چگونگی تحویل آن، به سرویس دسترسی یابند. رایانش ابری ساختاری شبیه یک توده ابر دارد که از طریق آن کاربران می‌توانند به برنامه‌های کاربردی در هر جایی از دنیا دسترسی داشته باشند؛ بنابراین در رایانش ابری، ابر مجموعه‌ای از گره‌های توزیع‌شده است که منابع محاسباتی را بر اساس تقاضا یا سرویس‌های کاربران بر روی شبکه ارائه می‌کند. بدین ترتیب دنیای محاسبات به‌سرعت به سمت توسعه نرم‌افزارهایی پیش می‌رود که به‌جای اجرا بر روی کامپیوترهای مجرد، به‌عنوان یک سرویس در دسترس میلیون‌ها مصرف‌کننده قرار می‌گیرد [۲].

بااین‌حال، علی‌رغم مزایا و رشد سریع رایانش ابری، مسائل امنیتی، حفظ حریم خصوصی و اعتماد به وجود می‌آورد که نیاز به اقدام فوری دارند. اعتماد یک مفهوم و چالش مهم برای رایانش ابری است، چراکه مصرف‌کنندگان سرویس‌های ابری برای انتخاب سرویس‌های مقرون‌به‌صرفه، قابل‌اعتماد و کمتر خطرناک به آن نیاز مبرم دارند [۳]. مسئله اعتماد همچنین برای ارائه‌دهندگان خدمات برای تصمیم‌گیری در مورد ارائه‌دهنده زیرساخت که می‌تواند با نیازهای آن‌ها مطابقت داشته باشد، نیز مهم است و برای بررسی این‌که آیا ارائه‌دهندگان زیرساخت‌ها در زمان استفاده از خدمات خود موافقت خود را حفظ می‌کنند. در حقیقت، یک سیستم مدیریت اعتماد مؤثر به ارائه‌دهندگان سرویس‌های ابری و همچنین مصرف‌کنندگان کمک می‌کند که از مزایای فناوری رایانش ابری بهره‌مند شوند. علی‌رغم مزایای مختلف مدیریت اعتماد در رایانش ابری، چندین مسئله مربوط به مکانیسم ارزیابی اعتماد عمومی، بازخورد نادرست، شناسایی ضعیف بازخورد، حفظ حریم خصوصی شرکت‌کنندگان و عدم پیوستگی بازخورد هنوز باید موردتوجه قرار گیرد. رویکردهای مدیریت اعتماد سنتی مانند استفاده از توافق‌نامه سطح سرویس برای محیط‌های پیچیده ابر ناکافی است. مفاد مبهم و مشخصات

* رایانامه نویسنده مسئول: Azgomi@iust.ac.ir

* این مقاله یک مقاله با دسترسی آزاد است که تحت شرایط و ضوابط مجوز Creative Commons Attribution (CC BY) توزیع شده است.

ناشر: دانشگاه جامع امام حسین (ع) © نویسندگان

فنی نامشخص توافق‌نامه‌های سطح سرویس (SLA) می‌تواند مشتریان سرویس‌های ابری را در شناسایی سرویس‌های ابری قابل‌اعتماد ناتوان کند [۵ - ۴].

همچنین، با توجه به رشد روزافزون تعداد ارائه‌دهندگان سرویس‌های ابری و درنتیجه تعداد سرویس‌های ابری، می‌توان به این نتیجه رسید که سرویس‌های متعددی توسط ارائه‌دهندگان ابری مختلف ارائه خواهند شد که ازنظر عملکرد کاملاً شبیه هم بوده اما ازنظر پارامترهای کیفیتی متفاوت هستند، کیفیت سرویس یک مجموعه از خصوصیات غیرعملکردی است که کیفیت پیشنهادشده توسط یک سرویس را منعکس می‌کند. در یک سرویس، نیازمندی‌های کیفیت سرویس اساساً به کیفیت غیرعملکردی سرویس رجوع می‌کند [۶].

کیفیت سرویس سنتی شامل طیف وسیعی از تعاریف مانند زمان پاسخ، دسترس‌پذیری، قابلیت دسترسی و قابلیت اطمینان است. بااین‌حال، در محیط رایانش ابری، لازم است به‌طور عینی کیفیت سرویس با درک ذهنی کاربران مرتبط گردد؛ بنابراین، از دیدگاه مصرف‌کننده سرویس، برخی از محققان به این نتیجه رسیده‌اند که رابطه اعتماد بین مصرف‌کنندگان سرویس‌های ابری و ارائه‌دهندگان سرویس‌های ابری، خود یک معیار کیفیت مهم و ضروری است. با توجه به رابطه اعتماد، مصرف‌کنندگان سرویس های ابری می‌توانند ارائه‌دهندگان قابل‌اطمینانی را که باید با آن‌ها تعامل کنند و همچنین ارائه‌دهندگان غیرقابل‌اعتمادی را که باید از تعامل با آن‌ها اجتناب کنند، به‌راحتی شناسایی کنند. اعتماد، در یک محیط شبکه توزیع‌شده، به‌عنوان یک رابطه امن ضروری در نظر گرفته‌شده است. به‌طورکلی، اعتماد می‌تواند به‌عنوان نتیجه مشاهدات منجر به اعتقاد ذهنی شود که اقدامات دیگر ممکن است برای رسیدن به یک هدف در شرایط خطرناک مورداستفاده قرار گیرد. اعتماد در طول زمان از طریق تعاملات مستقیم یا اطلاعات ارائه شده توسط دیگران درباره تجارب آن‌ها به‌روز می‌شود.

در این مقاله برای ارزیابی اعتماد در سرویس‌های ابری از فنون مختلف داده‌کاوی استفاده شده است. این فنون با استفاده از مجموعه داده، کیفیت سرویس برای سرویس‌های ابری استفاده شده و سعی در تخمین اعتماد دارند.

۲- پیشینه پژوهش

نویسندگان در [۷] یک مدل ریاضی برای ارزیابی اعتماد از جهات مختلف بر اساس معیارهای عملکردی، چابکی، امنیتی، قابلیت استفاده با استفاده از فنون تصمیم‌گیری چند معیارِ و متدهای منطق فازی ترکیبی ارائه داده‌اند که با مقایسه نتایج به‌دست‌آمده به نظر می‌رسد که نتایج برای سازمان‌ها و کاربران کارآمدتر باشد. محققان در [۸] یک سیستم ارزیابی ریسک در محیط ابری با کمک شبکه بیزی، برای بررسی دزدی دریایی ارائه دادند. با توجه به اینکه دزدی دریایی یک تهدید بزرگ برای ایمنی دریا محسوب می‌شود و هیچ سازوکار و معادله ریاضی کامل و جامعی برای ارزیابی در این مورد موجود نبود؛ لذا برای تجزیه‌وتحلیل و آسیب‌پذیری، از مدل ابری با استفاده از شبکه بیزی استفاده شده است.

نویسندگان در [۹] یک سیستم ارزیابی اعتماد پویا را برای خدمات ابری پیشنهاد می‌کنند که به‌عنوان یک ابزار سودمند جهت بررسی مطمئن اعتماد از دید ویژگی‌های سرویس عمل می‌کند. در فرآیند ارزیابی، زمان را به‌عنوان یک معیار مهم تأثیرگذار در برآورد میزان اعتماد در نظر گرفته‌اند. ویژگی کیفیت در بازه‌های زمانی مختلف نظارت و اندازه‌گیری شده است. این سیستم از رویکرد وزن‌دهی پویا برای وزن دادن به بازه‌های زمانی استفاده می‌شود. این سیستم با ایجاد یک محیط ابری، اعتبارسنجی و پیاده‌سازی می‌شود و نتایج را موردبحث و بررسی قرار می‌دهد.

همچنین محققان در [۱۰] مدل جدیدی از قابلیت اعتماد محدود را برای کاهش تهدیدات نرم‌افزارهای مخرب و خدمات داخلی در محیط ابر فراهم آورده‌اند که مفاهیم شبکه‌های جریان را برای کاهش مقیاس نرم‌افزار یا سرویس‌های مخرب کاهش داده اند. مدل پیشنهادی می‌تواند به دو روش زیر مورداستفاده قرار گیرد: ۱) اداره انجمن اعتماد در میان سرویس‌های مهمان، همچنین برای ارزیابی تهدیدها از سرویس‌های مخرب ناشناس، و ۲) کاهش خطر مربوط به سرویس‌های اجاره‌شده در محیط‌های ابر و کاهش تخلیه منابع تحت تأثیر سرویس‌های مهمان مخرب. اگرچه این مدل می‌تواند به‌طور مؤثر مقیاس سرویس‌های مخرب را محدود کند و خطر حملات داخلی را به‌طور قابل‌توجهی کاهش دهد، اما مقیاس‌پذیر نیست و از قابلیت دسترسی پایین نیز رنج می‌برد.

به‌عنوان یک تحقیق دیگر [۱۱]، یک چارچوب مدیریت اعتماد برای سیستم‌های مبتنی بر سرویس ارائه شده است که قابل انطباق است. چارچوب پیشنهادی متشکل از یک مدل متا با یک‌زبان رسمی است که مناسب سیاست‌های امنیتی مربوط به وضعیت و دستگاه‌هایی برای استقرار و ایجاد عوامل برای ارزیابی و انجام تصمیمات اعتماد بر اساس قوانین امنیتی، اطلاعات وضعیتی و اعتبارات است. اگرچه این چارچوب، مقیاس‌پذیری، قابلیت دسترسی و کارایی را بهبود می‌بخشد، از کارایی پایین و هزینه زمان بالا رنج می‌برد.

همچنین، نویسندگان در [۱۲] یک مدل اعتماد جدید را بسته به اعتبارنامه‌های قبلی و توانایی‌های فعلی تأمین‌کننده منابع ابر معرفی کرده‌اند. برخی از موارد در محاسبه ارزش اعتماد شامل قابلیت اطمینان، یکپارچگی، قابلیت دسترسی و کارایی درگیر هستند. روش ترکیبی از قابلیت‌های کیفیت سرویس مشتریان و تأمین‌کنندگان منابع ابری که توسط یک توافقنامه سطح خدمات تهیه‌شده است، در این مقاله شرح داده‌شده است. این تحقیق قابلیت اطمینان و قابلیت دسترسی را افزایش می‌دهد، گرچه مقیاس‌پذیر نیست.

علاوه بر این، در [۱۳]، نویسندگان یک روش با مرز تعمیم‌یافته در نظر گرفته‌اند. الزامات هر دو تأمین‌کننده داده‌ها و مصرف‌کنندگان داده‌ها می‌تواند توسط این روش انجام شود. در این روش با تعمیم اقلام داده، می‌توان هر دو قابلیت استفاده و حریم خصوصی را به دست آورد. علاوه بر این، در این مقاله، یک مدل کنترل دسترسی به اطلاعات حریم خصوصی ارائه شده است که در آن ترکیبی از سیاست تصمیم‌گیری مبتنی بر اعتماد و سیاست کنترل دسترسی، یک سیستم محافظت امنیتی ایجاد می کند. علاوه بر این، مدل پیشنهادی روش‌های تعمیم مؤثری برای سیستم‌های کنترل دسترسی حفظ حریم خصوصی را ارائه می دهد. اگرچه این تحقیق می‌تواند قابلیت دسترسی و قابلیت اطمینان را بهبود بخشد، اما مقیاس‌پذیر نیست و همچنین از هزینه بالایی برخوردار است.

علاوه بر این، محققان در [۱۴] یک نمونه اولیه ایجاد کرده‌اند که به شکل منطقی یک راه‌حل برای ارزیابی و مدیریت اعتماد و اعتبار خدمات وب را فراهم می‌کند. مجموعه‌ای از بازخورد درخواست‌کننده سرویس، مدیریت اعتماد و ارزیابی اعتماد با یک نمونه اولیه پیشنهادی که به ارائه یک مسیر مؤثر برای انتخاب سرویس‌های قابل‌اطمینان برای درخواست‌کنندگان کمک می‌کند، یکپارچه‌شده است. به‌منظور مدل‌سازی هر چه دقیق‌تر اعتماد سرویس، یک بیان ریاضی برای انواع مختلف داده‌ها برای توصیف اعتماد سرویس ازجمله مقادیر احتمالی، مقادیر مختصر، ارزش فازی و مقادیر گسسته در این کار تحقیقی ارائه شده است. این تحقیق، میزان موفقیت پیاده‌سازی سرویس‌های قابل‌اعتماد و مقیاس‌پذیری را بهبود می‌بخشد، هرچند که از هزینه بالایی برخوردار است.

علاوه بر این، نویسندگان در [۳] چارچوبی برای ارتقای روش های مدیریت اعتماد در رایانش ابری ارائه کرده‌اند. در واقع، آن‌ها مدلی اعتباری ارائه کرده‌اند که نه‌تنها قادر به شناسایی اعتبارهای اعتماد مخرب از مهاجمان است، بلکه بین بازخوردهای معتبر اعتمادی نیز متمایز می‌شود. علاوه بر این، آن‌ها یک مدل تعیین بدل ارائه کرده‌اند که قادر است به‌صورت پویا تعداد بدل‌های سرویس مدیریت اعتماد را تشخیص دهد. اگرچه این تحقیق قابلیت دسترسی را افزایش می‌دهد، از هزینه‌های بالا و مقیاس پذیری پایین رنج می‌برد.

چیرگی و همکاران [۱۵] رویکردی را ارائه کرده‌اند که مقادیر اعتبار را برای سرویس‌های ابری ارزیابی کرده و سرویس‌های مورد اعتماد را در محیط‌های ابری شناسایی می‌کند. مقدار اعتبار با استفاده از سه پارامتر شامل قابلیت دسترسی، قابلیت اطمینان و توانایی ارزیابی می‌شود. همچنین در این کار تحقیقی یک روش برای سرویس‌های مورد اعتماد با استفاده از سه شاخص توپولوژیکی شامل درجه ورودی، درجه خروجی و اعتبار پیشنهاد شده است. روش پیشنهادی در این مقاله در شرایط مختلف چالش‌برانگیز مورد ارزیابی قرارگرفته است که نتایج به‌دست‌آمده نشان می‌دهد که دقت روش پیشنهادی با توجه به توصیه ارائه‌دهندگان ابری مورد اعتماد به کاربران، افزایش می‌یابد.

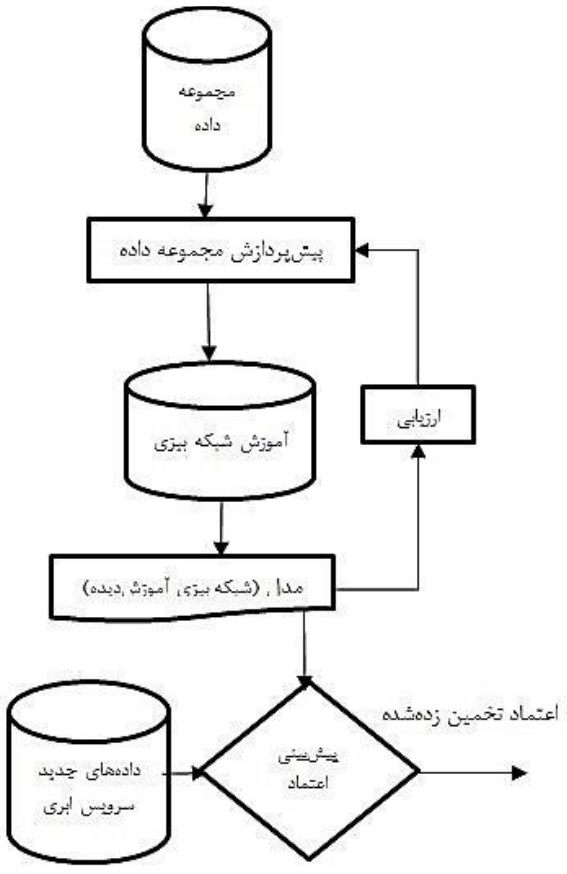
چونگ و همکاران [۱۶] یک معماری سیستم مدیریت اعتماد چند طرفه برای بازار رایانش ابری پیشنهاد کرده‌اند تا مشتریان را در شناسایی ارائه‌دهندگان مرود اعتماد پشتیبانی کند. این مقاله تهدیدهای مهم را برای یک سیستم مدیریت اعتماد و همچنین روش‌های مقابله با این تهدیدات را ارائه کرده است. در این مقاله مشخصه‌های بارز یک سیستم مدیریت اعتماد تعریف‌شده است. همچنین در این کار تحقیقی، اجزای امنیتی برای تشخیص میزان اعتماد و امانت‌داری شرکت‌کنندگان در تجارت الکترونیک برای کمک به مشتریان آنلاین برای تصمیم‌گیری در مورد انجام یا عدم انجام یک معامله مورداستفاده قرار می‌گیرد. بر اساس چارچوب ذکرشده، در این مقاله همچنین یک رویکرد برای فیلتر کردن بازخوردهای مخرب و یک متریک اعتماد برای ارزیابی میزان اعتماد و امانت‌داری ارائه‌دهندگان سرویس‌های ابری پیشنهادشده است. نتایج آزمایش‌ها مختلف شبیه‌سازی نشان می‌دهد که سیستم مدیریت اعتماد چند طرفه پیشنهادشده می‌تواند در شناسایی معامله-های خطرناک در بازارهای الکترونیکی بسیار مؤثر باشد.

در [۱۷] یک مدل ارزیابی اعتماد بر اساس نظریه شواهد D-S و پنجره‌های لغزان برای رایانش ابری ارائه شده است. به‌موقع بودن شواهد متقابل به‌عنوان شواهد دست‌اول، با معرفی پنجره های لغزان منعکس می‌شود. اعتماد مستقیم موجودیت‌ها بر اساس شواهد متقابل نظریه شواهد D-S محاسبه می‌شود. محاسبه اعتماد سازها بر اساس نظریه D-S با کمک مدارهای متقابل است. توصیه ارزش اعتماد از نهاده‌ای مختلف به‌عنوان شواهد دست‌دوم موردتوجه قرارگرفته است. ترکیبی از ارزش‌های

اعتماد توصیه‌شده اعتبار قلمرو را تشکیل می‌دهد. در نهایت، آزمایش‌ها برای ارزیابی اثربخشی و ضد حمله مدل پیشنهادی انجام شد. در [۱۸] نویسندگان، یک مدل مبتنی بر اعتماد با استفاده از شبکه بیزی برای شبکه‌های اجتماعی ارائه شده است. نتایج آزمایش‌ها و بررسی‌ها منجر به محاسبه دقیق‌تر اعتماد می‌گردد.

۳- ارزیابی اعتماد

همان‌طور که در بخش مقدمه نیز اشاره شد، ارزیابی اعتماد مربوط به سرویس‌های ابری یک موضوع حیاتی در رایانش ابری برای هر دو کاربران و همچنین ارائه‌دهندگان سرویس‌های ابری است. در این بخش مراحل مختلف مدل پیشنهادی این مقاله که یک مدل پیش‌بینی اعتماد برای سرویس‌های ابری با استفاده از شبکه بیزی است، ارائه می‌شود. شکل (۱)، مدل پیشنهادی برای ارزیابی اعتماد را نشان می‌دهد.



شکل (۱). مدل پیشنهادی ارزیابی اعتماد

۳-۱- آماده‌سازی داده‌ها

آماده‌سازی داده‌ها در داده‌کاوی مجموعه عملیاتی است که منجر به تولید مجموعه‌ای از داده‌های پالایش‌شده قابل کاوش می‌گردد. آماده‌سازی داده‌ها در حقیقت از دو مرحله استخراج داده‌ها و پیش‌پردازش داده‌ها تشکیل‌شده است که در ادامه این بخش هر دو مرحله در رابطه با مدل پیشنهادی ارائه می‌گردد.

مجموعه داده مورداستفاده باید حاوی مقادیر کیفیت سرویس مربوط به سرویس‌های مختلف ابری باشد. در [۱۹]، نتایج یک تحقیق جامع از سرویس‌های ابری موجود در وب انجام داده‌اند. آن‌ها یک موتور خزنده سرویس‌های ابری را توسعه داده‌اند که سرویس‌های ابری را جمع‌آوری، تائید و طبقه‌بندی کرده‌اند و تعدادی از مجموعه داده‌ها را تولید کرده‌اند که اطلاعات کیفیتی سرویس‌های ابری جمع‌آوری‌شده را ذخیره می‌کنند.

مجموعه داده‌های جمع‌آوری‌شده شامل متا داده‌های نزدیک به ۱۰۰۸۰ سرویس ابری واقعی است. پارامترهای کیفیت سرویس موجود در این مجموعه داده‌ها عبارت‌اند از: در قابلیت اطمینان[1]، امنیت[2]، زمان پاسخ[3]، دسترس‌پذیری[4]، سرعت[5]، فضای ذخیره‌سازی[6]، امکانات[7]، پشتیبانی فنی[8]، خدمات مشتری[9] و اعتماد[10]. در این مقاله از این مجموعه داده‌ها برای فنون داده‌کاوی مورداستفاده در مدل اعتماد پیشنهادی استفاده شده است.

در مرحله پیش‌پردازش داده‌ها نیز سلسله عملیاتی صورت می‌گیرد که موجب برطرف شدن مشکلات مختلف مجموعه داده مربوط به مسئله می‌گردد. با استفاده از این عملیات، داده برای انجام فرآیند

یادگیری مدل پالایش‌شده و آماده می‌شود. از بین عملیات پیش‌پردازش داده، در مدل پیشنهادی حذف نمونه‌های پرت و برای فن شبکه بیزی، گسسته سازی انجام می‌گیرد.

۳-۲- فنون داده‌کاوی استفاده شده

در این بخش مروری بر فنون داده‌کاوی استفاده شده برای ارزیابی اعتماد ارائه می‌شود.

۳-۲-۱- درخت تصمیم

درخت تصمیم یکی از مشهورترین و قدیمی‌ترین روش‌های ساختن مدل دسته‌بندی است. در الگوریتم‌های دسته‌بندی مبتنی بر درخت تصمیم، دانش خروجی به‌صورت یک درخت از حالات مختلف مقادیر ویژگی‌ها ارائه می‌شود. نمایش دانش به شکل درخت سبب شده است که دسته‌بندهای مبتنی بر درخت تصمیم کاملاً قابل تفسیر باشند. در **ساختار درخت تصمیم**، پیش‌بینی

[1] Reliability
[2] Security
[3] Response Time
[4] Accessibility
[5] Speed
[6] Storage Space
[7] Features
[8] Technical Support
[9] Customer Service
[10] Trust

به‌دست‌آمده از درخت در قالب یک سری قواعد توضیح داده می‌شود. هر مسیر از ریشه تا یک برگ درخت تصمیم، یک قانون را بیان می‌کند و در نهایت برگ باکلاسی که بیشترین مقدار رکورد در آن تعلق‌گرفته برچسب می‌خورد. در این نوع از درخت-ها برگ‌ها به‌جای کلاس مقدار واقعی را پیش‌بینی می‌کنند. الگوریتم برای تفکیک‌کننده‌ها، میزان مینیمم مربع خطا را جستجو می‌کند. در هر برگ، مقدار پیش‌بینی بر اساس میانگین خطای گره‌ها است. پارامترهای فنی درخت تصمیم مورداستفاده در این مقاله، در جدول (۱) و قسمتی از درخت تصمیم در شکل (۲) نمایش داده‌شده است.

مقدار پارامتر	پارامترهای درخت تصمیم
۱۰	Maximal Depth
۰/۱	Confidence level
۰/۰۱	Minimal Gain
۲	Minimal leaf size
۴	Minimal size for split
۳	Number of perpruning Alternatives

جدول (۱). پارامترهای درخت تصمیم

۳-۲-۲- جنگل تصادفی

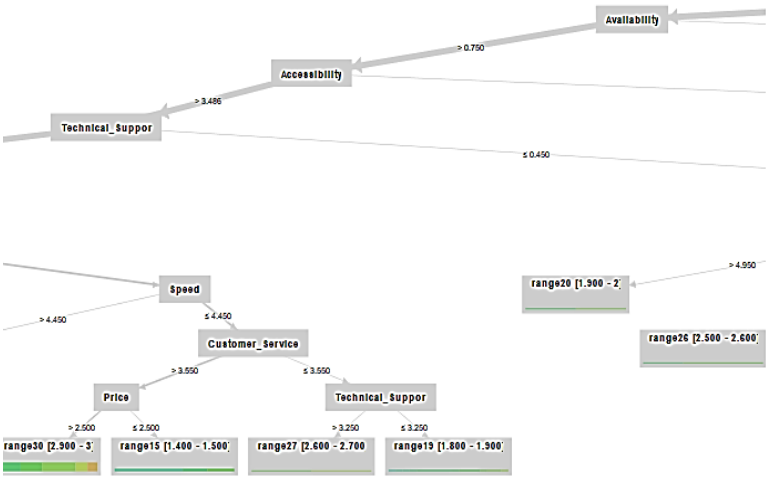
جنگل تصادفی یک الگوریتم ترکیبی هست که از درخت‌های تصمیم برای الگوریتم‌های ساده و ضعیف خود استفاده می‌کند. الگوریتم درخت تصمیم، می‌تواند به‌راحتی عملیات طبقه‌بندی را بر روی‌داده‌ها انجام دهد. حال در الگوریتم جنگل تصادفی از چندین درخت تصمیم (برای مثال ۱۰۰ درخت تصمیم) استفاده می‌شود. در واقع مجموعه‌ای از درخت‌های تصمیم، باهم یک جنگل را تولید می‌کنند و این جنگل می‌تواند تصمیم‌های بهتری را (نسبت به یک درخت) اتخاذ نماید. شکست دادن الگوریتم جنگل تصادفی در زمینه کارایی نیز امری دشوار است. البته، احتمالاً همیشه می‌توان مدلی را مانند شبکه عصبی پیدا کرد که عملکرد بهتری داشته باشد، اما این موارد احتمالاً نیازمند زمان توسعه بیشتری هستند. به‌طورکلی، جنگل تصادفی اغلب اوقات ابزاری سریع، ساده و انعطاف‌پذیر است که محدودیت‌های خود را دارد. در جدول (۲)، پارامترهای استفاده شده در این الگوریتم قابل مشاهده است.

جدول (۲). پارامترهای جنگل تصادفی

پارامترهای جنگل تصادفی	مقدار
Number of trees	۱۰۰
Criterion	Gain_ratio
Maximal depth	۱۰

۳-۲-۳- دسته‌بندی مبتنی بر قانون

دسته‌بندی‌های مبتنی بر قانون، دسته‌بندهایی هستند که دانش خروجی خود را به‌صورت یک مجموعه از قوانین «اگر- آنگاه» نشان می‌دهند. هر قانون یک بخش شرایط و یک بخش نتیجه دارد که این دو به شکل‌گیری قانون کمک می‌کنند.



شکل (۲). بخشی از درخت تصمیم شبیه‌سازی شده

۳-۲-۴- ماشین بردار پشتیبان

استفاده از بردارهای پشتیبان خطی در مسائل دسته‌بندی رویکردی است که در چند سال اخیر موردتوجه بسیاری قرارگرفته است. رویکرد ماشین بردار پشتیبان به این صورت است که در مرحله آموزش سعی دارد که مرز تصمیم‌گیری را به‌گونه‌ای انتخاب نماید که حداقل فاصله آن با هر یک از دسته‌های موردنظر بیشینه کند. این نوع انتخاب باعث می‌شود که تصمیم‌گیری در عمل، شرایط نویزی را به‌خوبی تحمل نموده و

پاسخ‌دهی مناسبی داشته باشد. این نحوه انتخاب مرز بر اساس نقاطی به نام بردارهای پشتیبان انجام می‌شود. پارامترهای ماشین بردار پشتیبان شبیه‌سازی‌شده در این مقاله در جدول (۳) نمایش داده شده است.

جدول (۳). پارامترهای ماشین بردار پشتیبان

پارامترهای جنگل تصادفی	مقدار
Kernel type	dot
Kernel cache	۲۰۰
C	۰/۰
Convergence epsilon	۰/۰۰۱
Max iterations	۱۰۰۰۰۰
L pos	۱
L neg	۱
Epsilon	۰/۰

۳-۲-۵- شبکه بیزی

امروزه بسیاری از مشکلات انسان‌ها، با کمک هوش مصنوعی حل می‌شود. یکی از مهم‌ترین خصوصیات این مشکلات وجود عدم قطعیت در آن‌ها است. روش‌های زیادی در هوش مصنوعی برای کنترل عدم قطعیت پیشنهاد شده‌اند که اکثر آن‌ها بر پایه نظریه احتمالات و نظریه فازی بنا نهاده شده‌اند. یکی از روش‌های معروف برای کنترل عدم قطعیت در مسائل که بر پایه نظریه احتمالات می‌باشد، شبکه بیزی است. [۱۸]. مدل‌های زیادی برای تحلیل داده‌ها شامل پایگاه‌های قاعده و درخت‌های تصمیم‌گیری وجود دارد. همچنین فنون متعددی برای تحلیل داده مانند دسته‌بندی، تخمین چگالی، رگرسیون و خوشه‌بندی وجود دارد. سؤالی که این وسط پیش می‌آید این است که باوجوداین فنون، چرا شبکه‌های بیزی برای حل چنین مسائلی به‌کاربرده می‌شوند. برای پاسخ به این سؤال می‌توان به دو ویژگی مهم از ویژگی‌های شبکه‌های بیزی اشاره کرد.

اولاً شبکه‌های بیزی مجموعه داده‌های ناکامل را بدون کوچک‌ترین مشکل بررسی می‌کنند، چراکه آن‌ها قادر به کشف وابستگی بین متغیرها هستند. زمانی که یکی از ورودی‌ها مشاهده نشود، اکثر مدل‌ها با یک تخمین ناصحیح کار خود را خاتمه می دهند. دلیل این موضوع این است که آن‌ها وابستگی بین متغیرهای ورودی را محاسبه نمی‌کنند. شبکه‌های بیزی یک روش طبیعی برای کدگذاری این وابستگی‌ها پیشنهاد می‌کنند.

ثانیاً هر شخص می‌تواند با استفاده از شبکه‌های بیزی درباره ارتباطات عِلّی یادگیری داشته باشد. دو دلیل مهم در رابطه با یادگیری درباره ارتباطات عِلّی وجود دارد. این فرآیند زمانی ارزشمند است که بخواهیم دامنه مسئله را درک کنیم، به‌عنوان نمونه زمان تحلیل داده‌های اکتشافی یا زمانی که یک عامل محیط را کاوش می‌کند. علاوه بر این در صورت وجود مداخله، شخص می‌تواند تخمین‌هایی با استفاده از دانش ارتباطات عِلّی انجام دهد.

۳-۳- یادگیری

پس از پیش‌پردازش داده‌ها در فرآیند داده‌کاوی، مجموعه داده موردنظر آماده اعمال به مرحله یادگیری مدل است. در مرحله یادگیری مدل، نظم حاکم بر داده‌های پیش‌پردازش شده، با توجه به تکنیک داده‌کاوی انتخاب‌شده شناسایی‌شده و مدل تولیدشده برای ارزیابی به مرحله بعد یعنی ارزیابی و تفسیر مدل منتقل خواهد شد. تکنیک‌های داده‌کاوی انتخاب‌شده در این مقاله برای ارزیابی اعتماد مربوط به سرویس‌های ابری شامل شبکه بیزی، درخت تصمیم، شبکه عصبی، درخت تصادفی، جنگل تصادفی، ماشین بردار پشتیبان (SVM) و دسته‌بندی مبتنی بر قانون هستند. در این مقاله از فن داده‌کاوی دسته‌بندی استفاده می‌شود که روی یک مجموعه داده اعمال و با ساخت چندین مدل برای مجموعه داده، دقت مدل‌ها موردبررسی و ارزیابی قرار می‌گیرد در ضمن برای انجام این کار (ساخت مدل‌ها، بررسی دقت مدل‌ها و ...) از نرم‌افزار رپیدماینر[1] استفاده شده است. رپیدماینر قوی‌ترین و آسان‌ترین نرم‌افزار برای تحلیل داده‌ها به‌صورت عددی و نمایش گرافیکی نتایج حاصل از تحلیل داده‌ها است. فرآیندهای ایجادشده در نرم‌افزار رپیدماینر به‌عنوان نمونه برای تکنیک شبکه بیزی در شکل (۳) نشان داده‌شده است.

۴- ارزیابی کارایی

برای ارزیابی مدل‌های اعتماد پیشنهادی در این مقاله، نتایج حاصل از اجرای آن‌ها بر روی مجموعه داده موردنظر در نرم‌افزار رپیدماینر مقایسه شده است. برای انجام تمامی آزمایش‌ها از یک کامپیوتر با پردازنده Core i5, 3 GH با حافظه اصلی 4 GB استفاده کردیم. برای مقایسه نحوه کار از معیارهای مختلف ذیل برای ارزیابی استفاده شده است:

۴-۱- معیار صحت

صحت[2] به نزدیک بودن یک مقدار اندازه‌گیری شده به یک مقدار استاندارد اشاره دارد. این رابطه کلیه مواردی را که می‌بایست یک دسته‌بندی رعایت کند تا بتواند عملکرد مطلوب را برای آن در نظر گرفت را نشان می‌دهد.

$$\text{Accuracy}=\frac{TP+TN}{\text{TP+TN+FP+FN}} \quad (۱)$$

[1] RapidMiner
[2] Accuracy

TN: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها منفی بوده و الگوریتم دسته‌بندی نیز دسته آن‌ها را به‌درستی منفی تشخیص داده است.

TP: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها مثبت بوده و الگوریتم دسته‌بندی نیز دسته آن‌ها را به‌درستی مثبت تشخیص داده است.

FP:بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها منفی بوده و الگوریتم دسته‌بندی دسته آن‌ها را به‌اشتباه مثبت تشخیص داده است.

FN: بیانگر تعداد رکوردهایی است که دسته واقعی آن‌ها مثبت بوده و الگوریتم دسته‌بندی دسته آن‌ها را به‌اشتباه منفی تشخیص داده است.

۴-۲- معیار خطای مطلق[1]

خطای مطلق بر اساس قدر مطلق تفاضل، مقدار اعتماد محاسبه شد با استفاده از روش پیشنهادی و مقدار واقعی اعتماد، محاسبه می‌شود.

$$\Delta x = |x_0 - x| \quad (۲)$$

در رابطه (۲)، x مقدار واقعی اعتماد، x_0 مقدار به‌دست‌آمده در روش پیشنهادی، Δx مقدار خطای مطلق را نشان می‌دهد.

۴-۳- معیار خطای ریشه میانگین مربع[2]

معیاری هست که اغلب به تفاوت بین مقادیر پیش‌بینی‌شده توسط یک مدل و مقادیر واقعی اشاره می‌کند.

$$\text{RMSE}=\sqrt{MSE}=\frac{\sqrt{\sum_{i=1}^{N}(X_i-\widehat{X_i})^2}}{N} \quad (۳)$$

در رابطه (۳)، X_iمقادیر مشاهده‌شده واقعی،$\widehat{X_i}$مقادیر تخمین زده در یک بازه زمانی و N تعداد داده‌های غیراشتباه را نشان می‌دهند. می‌توان گفت که خطای ریشه میانگین مربع یک ابزار خوبی برای مقایسه خطاهای پیش‌بینی‌شده توسط یک مجموعه داده است

۴-۴- معیار خطای مربع[3]

مربع تفاوت بین مقادیر واقعی (X) و تخمینی (X_i) تعریف می‌شود. به‌عنوان یک معیار ارزیابی مدل برای مدل‌های رگرسیونی استفاده می‌شود و مقدار کمتر نشان‌دهنده برازش بهتر است.

$$\text{SE}=(X - X_i)^2 \quad (۴)$$

بعد از استفاده از این معیارها، جدول شماره ۴ نتایج حاصل از ارزیابی رویکردهای داده‌کاوی را نشان می‌دهد. با دقت در نتایج حاصل‌شده، با توجه به اینکه کمترین میزان خطای مشاهده‌شده و بیشترین دقت ثبت‌شده مربوط به فن شبکه بیزی است، می‌توان به این نتیجه رسید که فن شبکه بیزی برای ارزیابی اعتماد مربوط به سرویس‌های ابری بهتر از سایر فنون عمل کرده است.

۵- نتیجه‌گیری و کارهای آتی

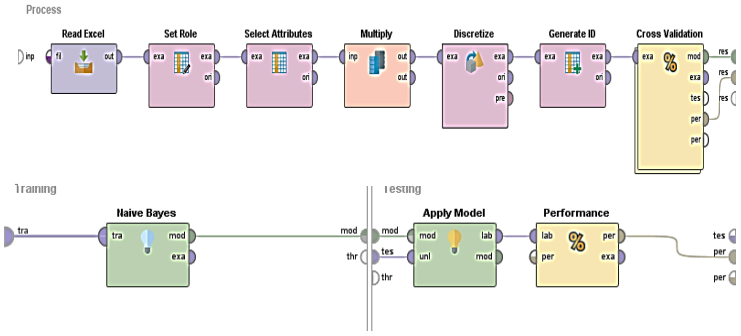
در این مقاله یک مدل اعتماد جدید مبتنی بر شبکه بیزی برای سرویس‌های ابری ارائه گردید. اعتماد نقش مهمی در تعیین کیفیت سرویس ابر برای طراحی سیستم‌های کارآمد و انعطاف‌پذیر بر اساس سرویس دارد. ماهیت غیرقطعی رایانش ابری به‌عنوان یک محیط سرویس‌گرا، بر عملکرد مدل‌های انتخاب سرویس ابر مبتنی بر اعتماد تأثیر می‌گذارد. پیش‌بینی ارزش اعتماد سرویس ابری یک مسئله طبقه‌بندی است که می‌تواند به‌عنوان یک‌راه حل مناسب برای انتخاب یک سرویس ابر مبتنی بر کیفیت با پیش‌بینی قابلیت اطمینان سرویس ابری بر اساس اطلاعات مربوط به کیفیت سرویس تاریخی خود مدل‌سازی شود.

با توجه به اینکه محیط ابری یک محیط کاملاً پویاست و مقادیر برخی از پارامترها در طول زمان دستخوش تغییر است، مدل پیشنهادی این امکان را فراهم می‌سازد که با تغییر در مقدار هر یک از پارامترهای موجود، مقادیر سایر پارامترها با استفاده از شبکه بیزی ساخته‌شده تخمین زده شوند. تخمین مقادیر جدید برای سایر پارامترها، کاربران را قادر می‌سازد که همیشه میزان اعتماد موردنیاز خود را هرچه دقیق‌تر محاسبه کنند. در این مقاله همچنین چندین مدل اعتماد با استفاده از فنون مختلف دسته‌بندی ارائه شد و نتایج حاصل از شبیه‌سازی بیانگر این بود که شبکه بیزی عملکرد بهتری از نظر ارزیابی اعتماد مربوط به سرویس‌های ابری دارد. ترکیب شبکه عصبی و شبکه بیزی می‌تواند به‌عنوان مدلی جدید و احتمالاً بهینه‌تر و دقیق‌تر برای محاسبه اعتماد پیشنهاد گردد.

[1] Absolute Error
[2] Root Mean Square Error
[3] Squared Error

جدول (۲). نتایج حاصل از ارزیابی فنون داده‌کاوی

فن طبقه‌بندی	صحت	خطای مطلق	خطای ریشه میانگین مربع	خطای مربع
شبکه بیزی	۹۴/۵۳	۰/۰۳۷	۰/۱۳۷	۰/۰۳۸
درخت تصمیم	۹۲/۵۱	۰/۰۶۱	۰/۲۱۲	۰/۰۵۷
درخت تصادفی	۹۳/۶۶	۰/۰۶۴	۰/۱۹۸	۰/۰۶۲
جنگل تصادفی	۹۲/۶۰	۰/۰۶۶	۰/۲۱۱	۰/۰۶۱
دسته‌بندی مبتنی بر قانون	۹۳/۴۵	۰/۰۵۶	۰/۱۸۷	۰/۰۵۲
ماشین بردار پشتیبان	۹۴/۰۳	۰/۰۴۸	۰/۱۵۲	۰/۰۴۵



شکل (۳). فرآیندهای ایجادشده در نرم‌افزار رپیدماینر برای شبکه بیزی

۶- مراجع

[1] M. Armbrust, & et al., "A view of cloud computing," Commun. ACM., vol. 53., no. 4, pp. 50-58, 2010.

[2] P. Mell & T. Grance, "The NIST definition of cloud computing", 2011.

[3] T. H. Noor, Q. Z. Sheng, & A. Bouguettaya, "Trust Management in Cloud Services," Springer, 2014.

[4] Y. Fu, Z. Hu, & Q. Zhang, "Bayesian Network based QoS Trustworthiness Evaluation Method in Service Oriented Grid," in Proceedings of the The 9th International Conference for Young Computer Scientists, pp. 293-298, Hunan China, Nov. 2008.

[5] S. Rizvi, K. Karpinski, B. Kelly, & T. Walker, "Utilizing Third Party Auditing to Manage Trust in the Cloud," Procedia Comput. Sci., vol. 61, pp. 191-197, 2015.

[6] A. Mani & A. Nagarajan, "Understanding quality of service for Web services," IBM Dev, 2002.

[7] D. Trabay, A. Asem, I. El-Henawy, & W. Gharibi, "A hybrid technique for evaluating the trust of cloud services," International Journal of Information Technology, vol. 13, pp. 687-695, 2021.

[8] Kefeng Liu, Lizhi Yang, & Ming Li, "Application of Cloud Model and Bayesian Network to Piracy Risk Assessment," Hindawi Mathematical Problems in Engineering," Vol. 2021, 2021.

[9] A Selvaraj, & S Sundararajan, "Dynamic Multi Attribute Trust Evaluation System for IaaS Services," in International Journal of Applied Science and Engineering, Volume 17, No. 1, pp. 1-10, March, 2020.

[10] Y. Wang, S. Chandrasekhar, M. Singhal, & J. Ma, "A limited-trust capacity model for mitigating threats of internal malicious services in cloud computing," Cluster Comput, vol. 19, no. 2, pp. 647-662, 2016.

[11] S. S. Yau, Y. Yao, & A. B. Buduru, "An adaptable distributed trust management framework for large-scale secure service-based systems," Computing, vol. 96, no. 10, pp. 925-949, 2014.

[12] D. Manuel, S. T. Selvi, & M. I. Abd-El Barr, "Trust management system for grid and cloud resources," in Advanced Computing, 2009. ICAC 2009. First International Conference on, Chennai India, pp. 176-181, 2009.

[13] M. Li, S. Yu, N. Cao, & W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in Distributed Computing Systems (ICDCS), 31st International Conference on, pp. 383-392, 2011.

[14] P. Zhang & Z. Yan, "A QoS-aware system for mobile cloud computing," in Cloud Computing and Intelligence Systems (CCIS), IEEE International Conference on, Beijing, China, pp. 518-522, 2011.

[15] M. Chiregi, & N.J. Navimipour, "Trusted services identification in the cloud environment using the topological metrics," Karbala Int. J. Mod. Sci. 2, pp. 203-210, 2016.

[16] S.K. Chong, J. Abawajy, M. Ahmad, & I.R.A. Hamid, "Enhancing Trust Management in Cloud Environment," Procedia - Soc. Behav. Sci. 129, pp. 314-321, 2014.

[17] X. Wu, R. Zhang, B. Zeng, & S. Zhou, "A Trust Evaluation Model for Cloud Computing," Procedia Comput. Sci. 17 (2013) 1170–1177.

[18] V. Hosseinnezhad, & A. A. pourhaji kazem, "Bayesian Networks Based Trust Model in Social Networks," Scientific Journal of Electronic and Cyber Defense, Vol. 6, No. 2, Serial No. 22, 2018. (In Persian)

[19] CloudArmmor Prohect Web Site, URL: https://cs.adelaide.edu.au/~cloudarmor/ds.html.