Semnan University

Journal of Modeling in Engineering

Journal homepage: https://modelling.semnan.ac.ir/

ISSN: 2783-2538

Research Article

Provide a Method for Recognizing Trust in Social Networks According to Individual and Personal Characteristics Using a Compatible Neural-Fuzzy Inference System Method

Mahsa Farhadi Savadkouhi[a] , Mahmood Deypir [b,*]

[a] *Department of Computer Engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran*
[b] *Associate Professor, Computer Faculty, Shahid Sattari Aeronautical University of Science and Technology, Tehran, Iran*

PAPER INFO

Paper history:

Received: 30 July 2022
Revised: 22 April 2023
Accepted: 13 June 2023

Keywords:

social networks,
trust,
fuzzy system,
trust reversal.

ABSTRACT

In this article, we presented a method to detect trust in social networks according to individual and personal characteristics with the help of the adaptive neuro-fuzzy inference system method. The current research required a dataset, for this purpose we designed an online questionnaire and collected 1000 records with the variables of age, gender, occupation, hours of activity in the virtual space, the type of use of the virtual space and the type of relationships in the virtual space, this dataset is as reference data can be used for similar analyzes and has a high level of data security. First, we evaluated and descriptively analyzed the data set, for this purpose we used Excel and SPSS software, we modeled and analyzed using MATLAB simulation. To introduce change limits and fuzzy behavior for variables, dataset parameters were introduced to the algorithm using Bayesian membership functions. Due to the uncertainty of the type of membership functions, coverage of the space under control, less computational volume, reduction of analysis time and increase of accuracy, we used the deductive clustering method and trained the network using feedforward neural network and trained the network with data. We continued the training until we reached full convergence. We entered the test and check data and using the squared error performance function, we came to the conclusion that with the method used in this research, it is possible to predict people's trust in each other in virtual space with an error of less than 1.5%.

DOI: https://doi.org/10.22075/jme.2023.27764.2310

© 2023 Published by Semnan University Press.
This is an open access article under the CC-BY 4.0 license.(https://creativecommons.org/licenses/by/4.0/)

*** Corresponding author.**
E-mail address: mdeypir@ssau.ac.ir

How to cite this article:
Farhadi Savadkouhi, M., & Deypir, M. (2023). Provide a method for recognizing trust in social networks according to individual and personal characteristics using a compatible neural-fuzzy inference system method. Journal of Modeling in Engineering, 21(75), 115-127. doi: 10.22075/jme.2023.27764.2310

مقاله پژوهشی

ارائه روشی برای تشخیص اعتماد در شبکه‌های اجتماعی با توجه به ویژگی‌های فردی و شخصی به کمک روش سیستم استنتاج عصبی–فازی سازگار

مهسا فرهادی سوادکوهی[۱،*]، محمود دی پیر[۲،*]

اطلاعات مقاله

دریافت مقاله: ۱۴۰۱/۰۵/۰۸
بازنگری مقاله: ۱۴۰۲/۰۲/۰۲
پذیرش مقاله: ۱۴۰۲/۰۳/۲۳

واژگان کلیدی:
شبکه‌های اجتماعی،
اعتماد،
سیستم فازی،
معکوس سازی اعتماد.

چکیده

در این مقاله به ارائه روشی برای تشخیص اعتماد در شبکه‌های اجتماعی با توجه به ویژگی‌های فردی و شخصی به کمک روش سیستم استنتاج عصبی-فازی سازگار پرداختیم. پژوهش حاضر نیاز به دیتاست داشته که برای این منظور یک پرسشنامه آنلاین طراحی و ۱۰۰۰ رکورد با متغیرهای سن، جنسیت، شغل، ساعات فعالیت در فضای مجازی، نوع استفاده از فضای مجازی و نوع روابط در فضای مجازی جمع‌آوری کردیم. این دیتاست به‌عنوان داده‌ای مرجع برای تحلیل‌های مشابه قابل‌استفاده است و به لحاظ تأمین امنیت داده از سطح بالایی برخوردار است. ابتدا به ارزیابی و تحلیل توصیفی دیتاست پرداخته‌ایم. برای این منظور از نرم‌افزارهای اکسل و اس‌پی‌اس‌اس استفاده نمودیم، با استفاده از شبیه‌سازی در متلب به مدل‌سازی و تحلیل پرداخته‌ایم. برای معرفی حدود تغییرات و رفتار فازی برای متغیرها، پارامترهای دیتاست با استفاده از توابع عضویت بیزین به الگوریتم معرفی شده‌اند. به دلیل عدم مشخص بودن نوع توابع عضویت، پوشش فضای تحت کنترل بیشتر، حجم محاسباتی کمتر، کاهش زمان تحلیل و افزایش دقت، از روش خوشه‌بندی کاهشی استفاده کرده‌ایم و به آموزش شبکه با استفاده از شبکه عصبی پس‌خور پرداخته‌ایم. آموزش شبکه را با داده‌های آموزش تا رسیدن به همگرایی کامل ادامه داده‌ایم. در ادامه، داده‌های تست و چک را وارد نموده‌ایم و با استفاده از تابع عملکرد مربع خطا به این نتیجه رسیده‌ایم که با روش به‌کار رفته شده در این پژوهش می‌توان با خطای زیر ۱/۵ درصد، اعتماد افراد را به یکدیگر در فضای مجازی پیش‌بینی نمود.

DOI: https://doi.org/10.22075/jme.2023.27764.2310

© 2023 Published by Semnan University Press.
This is an open access article under the CC-BY 4.0 license.(https://creativecommons.org/licenses/by/4.0/)

۱-مقدمه[۱]

اعتماد جنبه مهمی از رابطه بین دو نهاد است. چشم‌انداز اعتماد یک شبکه اجتماعی (چه کسی به چه کسی اعتماد می‌کند) نقش مهمی در حوزه اطلاعاتی و امنیتی دارد. اعتماد مبنایی را برای تشکیل ائتلاف‌ها تشکیل می‌دهد (جوامع قوی توسط نهادهایی تشکیل می‌شوند که به یکدیگر «اعتماد» دارند) که می‌تواند برای شناسایی گره‌های تأثیرگذار در یک شبکه خدمت کند و چگونگی جریان اطلاعات در یک شبکه اجتماعی را تعیین کند [۱]. جریان اطلاعات مداوم بین اعضاء می‌تواند رابطه اعتماد بین آن‌ها را تقویت کند. یک شبکه اجتماعی معمولی شامل بازیگران (افراد) و نوعی ارتباط بین آن‌ها است که می‌تواند تماس‌های تلفنی، ایمیل‌ها، پست‌های وبلاگ و غیره باشد [۲]. افراد ملاقات می‌کنند و روابط اعتماد ایجاد می‌کنند، بدون هیچ‌گونه تماس چهره به چهره در فعالیت‌ها شرکت می‌کنند. درنتیجه تعامل بین افراد در شبکه اجتماعی

* پست الکترونیک نویسنده مسئول: mdeypir@ssau.ac.ir
۱. کارشناسی اشد، دانشکده فنی و مهندسی، دانشگاه آزاد اسلامی واحد تهران جنوب
۲. دانشیار، دانشکده مهندسی کامپیوتر، دانشگاه هوایی شهید ستاری، تهران، ایران.

استناد به این مقاله:
فرهادی سوادکوهی، مهسا، & دی پیر، محمود. (۱۴۰۲). ارائه روشی برای تشخیص اعتماد در شبکه های اجتماعی با توجه به ویژگی های فردی و شخصی به کمک روش سیستم استنتاج عصبی-فازی سازگار. مدل سازی در مهندسی، ۲۱(۷۵)، ۱۱۵-۱۲۷. doi: 10.22075/jme.2023.27764.2310

نشانگر خوبی از روابط اجتماعی آن‌ها با هم است [۳ و ۴]. یک جنبه از اعتماد مبتنی بر مفهوم تعبیه است که نشان می‌دهد تعاملات بین افراد مبنایی را تشکیل می‌دهد که از آن، یک رابطه اعتماد ممکن است رشد کند [۵]. گاهی ممکن است این تعاملات نیازی به اعتماد نداشته باشد [۶]. با این‌حال، آن‌ها رابطه‌ای برقرار می‌کنند که می‌تواند برای ایجاد اعتماد مورداستفاده قرارگیرد [۷]. ویژگی‌های مختلف این روابط مانند تعادل در مشارکت و تداوم ارتباطات ممکن است نشانه شکل‌گیری یک رابطه اعتماد باشد [۸].

به‌طورکلی، زمانی که تصمیم می‌گیریم به یک فرد اعتماد کنیم یا نه، همه ما تحت تأثیر عوامل متعددی قرار می گیریم، مانند: ۱) استعداد خودمان برای اعتماد که به روانشناسی ما مرتبط است که خود تحت تأثیر رویدادهای مختلف قرار گرفته است. در طول عمر ما؛ این رویدادها می‌توانند کاملاً به شخصی که تصمیم داریم به او اعتماد کنیم یا اعتماد نکنیم، بی‌ارتباط باشند [۲ و ۹]. رابطه و تجربیات گذشته ما با فرد و دوستانش، ازجمله شایعات و واقعیات [۳ و ۱۰] و نظرات ما در مورد اعمال و تصمیماتی که فرد در گذشته گرفته است، در شکل‌گیری اعتماد مهم هستند. بنابراین، مشکل تخمین اعتماد در شبکه‌های اجتماعی بسیار جالب و چالش‌برانگیز است، زیرا هنوز به‌خوبی درک یا تعریف نشده است [۱۱]. برای اینکه بتوانیم میزان اعتماد را به دست آوریم و/یا آن را به صورت کمی در آوریم، باید روی برخی از ویژگی‌های خاص اعتماد، تمرکز کنیم که باید ساده شوند، به‌طوری‌که این ویژگی‌ها ممکن است به‌صورت الگوریتمی دریافت شوند [۱۲]. در این مقاله، هدف ما اندازه‌گیری کمی اعتماد دوتایی (اعتماد بین دو شخص) بر اساس مشخصات فردی، که سازنده¬ی رفتارهای ارتباطی آن‌ها است، با استفاده از مدل شبکه فازی عصبی تطبیقی است.

۲-پیشینه پژوهش

در [۱۳]، چالش‌های موجود در رابطه با سیستم‌های مدیریت اعتماد موردبررسی قرار گرفته است و در آن نحوه نمایش اعتماد در سیستم‌های برخط نیز نشان داده‌شده است. همچنین در رابطه با موضوع اعتماد، مقالات مروری مختلفی با تمرکز بر جنبه‌های خاص اعتماد، ارائه شده است. در [۱۴] جنبه امنیتی اعتماد در نظر گرفته شده است که در آن بر اساس رفتارهای مشاهده شده عمل می‌نمایند و در این رابطه [۱۵] نیز، مروری بر انواع حملات و دفاع‌های ممکن در سیستم‌های بر مبنای شهرت صورت گرفته است، در [۱۶] نیز مروری بر روش‌های استنتاج اعتماد انجام‌شده است. این روش‌ها، سازوکار خود جهت تعیین و استنتاج اعتماد درصورتی‌که ارتباط مستقیم بین کاربران وجود نداشته باشد، را ارائه داده‌اند.

در مدل‌سازی اعتماد، ابعاد مختلفی از آن می‌تواند در نظر گرفته شوند. یکی از این ابعاد، مقیاس است، اعتماد می‌تواند به‌صورت عددی و یا به‌صورت دسته‌بندی نمایش داده شود. مقادیر اعتماد نیز می‌توانند به‌صورت پیوسته و یا گسسته باشند. برای مثال، در سیستم‌هایی که از رتبه‌بندی استفاده می‌کنند، اعتماد به‌صورت گسسته بیان می‌شود [۱۷]. این‌گونه روش‌ها، تفاوتی بین اعتمادهای یک دسته قائل نمی‌شوند. بنابراین مقدار دقیقی را ارائه نمی‌کنند. در مقابل، در سیستم‌هایی که از معیار شباهت استفاده می‌کنند و یا از معیارهای احتمالی در محاسبه اعتماد بهره می‌برند، داده‌های اعتماد پیوسته به کار می‌روند [۱۷]. ازجمله چالش‌های این روش‌ها، تعیین معیارهای شباهت است که در حوزه‌های مختلف می‌توان معیارهای گوناگونی به کار گرفت.

یکی دیگر از راه‌های نمایش داده اعتماد به‌جای استفاده از مقادیر مشخص، استفاده از مقادیر بازه‌ای است. این روش نمایش اعتماد، در راه کارهایی که از منطق فازی استفاده می‌کنند، به کار گرفته می‌شود [۱۸]. در این پژوهش نیز به‌منظور دسته‌بندی کاربران از منطق فازی بهره برده شده است. یکی دیگر از ابعاد اعتماد، برچسب‌هایی است که می‌توان به آن زد. برای مثال، اعتماد می‌تواند در زمان‌های گوناگون، مقادیر مختلفی داشته باشد که بنابراین در این صورت، اعتماد دارای برچسب زمانی خواهد بود [۱۹].

روش‌هایی که اعتماد ارائه شده در آن‌ها دارای برچسب زمانی نباشند، کارایی لازم را در محیط‌های پویا ندارند. ازاین‌رو، در این پژوهش، بعد زمان نیز در محاسبه اعتماد لحاظ گردیده است. همچنین این برچسب‌ها می‌توانند به‌منظور دفاع در برابر برخی حملات مورداستفاده قرار گیرند [۲۰].

اعتماد یک ویژگی قطعی به‌حساب نمی‌آید و ازاین‌رو برخی از پژوهش‌ها [۲۱] رویکرد منطق فازی را جهت نمایش اعتماد به کار می‌برند. ساخت یک الگوریتم کارآمد برای شناسایی ساختار شبکه اجتماعی موبایلی، امری دشوار است. در [۲۲] تحقیقات اولیه‌ای درباره استفاده از روابط

فازی در تحلیل شبکه اجتماعی صورت گرفته است. یکی از کاربردهای شبکه‌های عصبی، افزایش کارآیی جریان‌سنج دوفازی با استفاده از روش‌های استخراج ویژگی حوزه‌ی فرکانس و شبکه عصبی در طیف خروجی آشکارساز می‌باشد [۲۳]. همچنین در سایر حوزه های مهندسی می‌توان به مدل‌سازی سیستم‌های تعادلی بخار-مایع و مایع-مایع با استفاده از مدل‌های ترمودینامیکی، ساختارهای فازی و شبکه‌های عصبی نوع GMDH [24] و بررسی و پیش‌بینی خواص فیزیکی و مکانیکی کامپوزیت کاه و گچ به کمک مدل شبکه استنتاج عصبی فازی تطبیقی [۲۵] به‌عنوان کاربردهای ساختارهای فازی و شبکه‌های عصبی اشاره کرد. در بررسی‌هایی که در زمینه‌های تخصصی نظیر ورود اینترنت اشیاء به پزشکی صورت پذیرفته است، نیز اعتماد بسیار حائز اهمیت است که در [۲۶] بیان شده است، حتی در سال ۲۰۲۲ که استفاده از اینترنت اشیاء و موفقیت‌های آن بسیار هویدا شده است، هنوز افراد در زمینه‌های درمانی، اعتماد کمی به بسترهای مجازی در این زمینه دارند. در [۲۷] نیز ابعاد دیگری از اعتماد در فضای مجازی مطرح شد و بیان گردید که مشخص نیست چگونه مردم وقتی چندین شاخص عملکرد به‌طور هم‌زمان ارائه می‌شود، به مدل ارتباطات در فضای مجازی اعتماد می‌کنند. برای رسیدن به پاسخ این سؤال آزمایشی تجربی صورت گرفت و مشخص شد که سطح امنیت بستر، به‌طور قابل‌توجهی بر اعتماد افراد تأثیر می‌گذارد. اما [۲۸] بیان نمود که در پیش‌بینی اعتماد باید همواره از هوش مصنوعی استفاده شود و تکیه‌بر مفاهیم آماری خطرزا خواهد بود. به همین منظور الگوریتم جعبه سیاه را برای پیش‌بینی اعتماد به داده‌های موجود در فرآیندهای بازارهای مالی ارائه شد. [۲۹] بیان نمود که استفاده از فضای مجازی در سال¬های اخیر اجتناب‌ناپذیر است و همین باعث وجود داده¬های اشتباه بسیار در این بستر می‌باشد که زمینه عدم اعتماد کاربران را بیشتر نموده است، این محققین بیان کردند که راه‌حل این مشکل، رفع تضادها در داده‌های منتشرشده از سوی چند شخص، با در نظر گرفتن خطر حریم خصوصی می‌باشد. در همین راستا [۳۰] نیز بیان نموده است که باید در بسترهای مجازی نظیر واتس‌آپ که کاربران بسیاری در جهان دارد، سیستم مدیریت برخورد با افراد ناشناس ارائه شود و برای همین منظور با استفاده از الگوریتم منطق ذهنی، یک برنامه تحت عنوان WhatsTrust ارائه داده است. برای به اشتراک‌گذاری امن داده‌ها، یک چارچوب اعتماد بر اساس علاقه و پارامترهای تعامل کاربر ارائه شده است. این تحقیق، روش جدیدی برای شناسایی اجتماعات مشابه ارائه داده است که حول ایده استفاده از شاخص مرکزیت برای یافتن مرزهای اجتماعی، ارائه شده است.

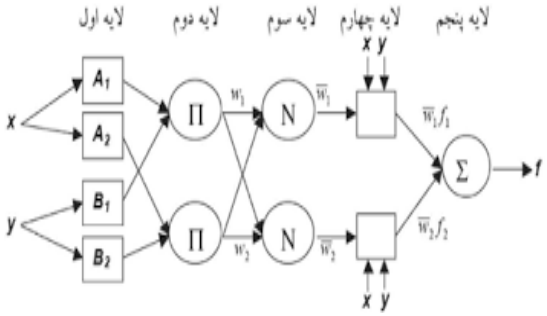
علاوه بر موارد فوق، پژوهش‌های مختلف که در زمینه استفاده از شبکه‌های فازی عصبی تطبیقی در پیش‌بینی اعتماد تلاش‌هایی را صورت دادند، نیز نشان دادند که این شبکه‌ها درصد خطای بسیار مناسبی در زمینه تشخیص اعتماد را ارائه نموده‌اند که در [۳۴ و ۳۵] به ترتیب این شبکه توانست با دقت ۹۴ و ۸۴ درصد تشخیص اعتماد را انجام دهد که البته در [۳۵] نوع شبکه عصبی استفاده‌شده از نوع RBF انتخاب شده بود. با بررسی نتایج، مشاهده می شود که الگوریتم ارائه شده در این مقاله توانست مناسب‌ترین دقت پیش‌بینی را در قیاس با موارد اشاره شده داشته باشد. همچنین در [۳۴] دقت روش‌های C4.5، رگرسیون لجستیک، ANN و شبکه بیزین بررسی گردید. بر اساس نتایج مشخص شد به ترتیب دقت این الگوریتم‌ها برابر با ۹۰.۷، ۹۱.۸، ۹۳.۲ و ۹۰ درصد بوده است. همچنین در [۳۶] برای تشخیص اعتماد در شبکه از روش‌های NB، MLP، RBFC، RBFN، AdaBoost، JRip و J48 استفاده نمود که از بین آن‌ها دو روش MLP و RBFN دقت بهتری را به دست آوردند.

۳- روش‌شناسی پژوهش

پژوهش حاضر با توجه به اهداف پیگیری شده، یک پژوهش کاربردی بوده و از منظر روش گردآوری داده‌ها نیز یک پژوهش میدانی می‌باشد. هدف، تعیین تشخیص اعتماد در شبکه‌های اجتماعی با توجه به ویژگی‌های فردی و شخصی است. پژوهش حاضر برای تحلیل، نیاز به داده افراد داشته که برای این منظور یک پرسشنامه آنلاین طراحی شد و در اختیار افراد گذاشته شد. در این فرم از افراد خواسته شد تا ویژگی‌هایی نظیر سن، جنسیت و شغل را وارد کنند. این دسته از ویژگی‌ها به‌صورت کیفی نبوده و افراد می‌توانند به‌صورت دقیق به این موارد پاسخ دهند. از آنجایی که در پرسشنامه آنلاین مشخصات افراد و پاسخ‌های داده‌شده مرتبط با هر فرد به صورت بی-نام تکمیل شد، از منظر تأمین امنیت داده از سطح بالایی برخوردار بوده و افراد با علم بر این موضوع می‌توانند به‌صورت واقعی و بدون ترس از قضاوت، مقادیر واقعی را تکمیل نمایند و از این حیث

پاسخ‌های دریافتی به‌صورت درستی خواهند بود و می‌توان از این داده به عنوان داده‌ای مرجع برای تحلیل‌های مشابه استفاده نمود. لازم به ذکر است که جامعه‌ی تحقیقاتی این پژوهش که به فرم آنلاین پاسخ‌دهی داشتند و در واقع دیتاست پژوهش را ساختند، افرادی بودند که بازه سنی بیشتر از ۱۸ سال داشته و عملاً با زندگی اجتماعی و ارتباط با فضای مجازی، آشنایی کافی و ارتباط کافی داشته‌اند. تلاش شد تا با استفاده از ارتباطات مختلف از گروه‌های مختلف سنی، این همکاری صورت پذیرد تا محیط شغلی و یا زندگی بر روی دیتاست و نتایج حاصل از آن نتواند اثرگذار باشد. برای این کار از گروه‌های رسمی مشاغل و اصناف، دانشگاه‌ها و غیره کمک گرفته شد تا در سریع‌ترین زمان به دیتاست مدنظر دست‌یافته شود.

مرحله بعد، ساخت مدل انفیس است که ساختار آن در شکل (۱) نشان داده‌شده است. لایه‌های مختلف این مدل به‌صورت زیر هستند:



شکل ۱- مدل ANFIS

لایه ۱: هر گره در این لایه، نشان‌دهنده‌ی درجه عضویت پارامترهای ورودی می‌باشد.

لایه ۲: هر گره این لایه با برچسب π نشان داده‌شده و داده‌های ورودی در آن به‌صورت زیر پردازش می‌شوند:

$$\overline{W_i} = \mu A_i(x)\,\mu B_i(y), \quad i = 1,2 \qquad (۱)$$

در رابطه بیان‌شده فوق، و میزان مقادیر درجه عضویت مجموعه فازی می‌باشند.

لایه ۳: امین گره این لایه با برچسب N نشان داده‌شده و از طریق فرمول زیر برآورد می‌گردد:

$$\overline{W_i} = \frac{W_i}{W_1 + W_2 + \ldots + W_i}, \quad i = 1,2,\ldots \qquad (۲)$$

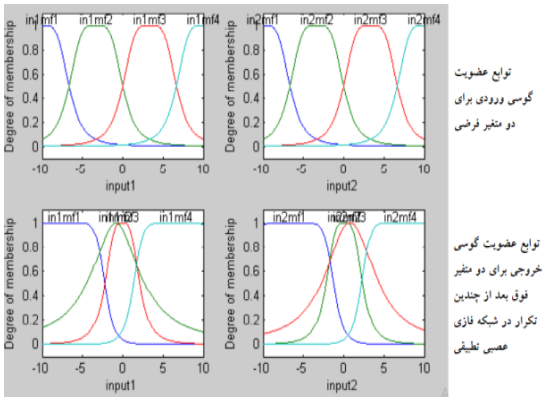
لایه ۴: در این لایه، داده‌ها از طریق معادله‌ی زیر پردازش می‌شوند:

$$\overline{W_i} f_i = \overline{W_i}\left(p_i x + q_i y + r_i\right) \qquad (۳)$$

لایه ۵: گره‌ها در این لایه با برچسب نشان داده‌شده و در آن با جمع تمام داده‌های ورودی، خروجی نهایی برآورد می‌گردد.

$$\sum \overline{W_i} f_i = \frac{\sum W_i f_i}{\sum W_i} \qquad (۴)$$

بدین منظور بعد از جمع‌آوری دیتاست برای این پژوهش، این پارامترها باید از طریق نقش‌ها و نیز توابع عضویت به الگوریتم معرفی گردد. به این منظور برای معرفی حدود تغییرات و رفتار فازی برای متغیرها، از تابع عضویت بیزین استفاده‌شده است که در آن متغیرها که هر یک بازه‌هایی را دارند، به‌صورت ترکیبی و فازی به الگوریتم ارائه شده-اند. در ادامه نمونه‌ای از این تابع عضویت را در شکل (۲) می‌توان مشاهده نمود.



شکل ۲- تغییر در توابع عضویت و بهینه‌سازی آن در مدل ANFIS

بعد از مشخص شدن اوزان هر یک از متغیرها و ویژگی‌ها، باید بررسی شود این اوزان درست انتخاب‌شده‌اند یا خیر. برای این منظور از توابع عملکرد استفاده‌شده است که در این پژوهش از مربع خطا به‌عنوان تابع عملکرد کمک گرفته شده است. خطا در این پژوهش میزان اختلاف خروجی به‌دست‌آمده از مقادیر واقعی موجود در دیتاست می‌باشد و طبیعتاً بهترین مقدار برابر صفر می‌باشد. این رابطه در ادامه بیان‌شده است. تعریف MSE بر اساس توصیف تخمین‌گر یا پیش‌بینی کننده، متفاوت است.

برای به دست آوردن خطای میانگین مربعات، از یک مجموعه یا n داده می‌توان از رابطه زیر استفاده کرد:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(Y_i - \overline{Y_i}\right)^2 \qquad (۵)$$

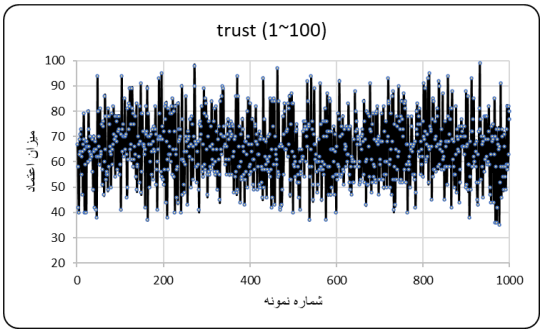
که در آن عمل میانگین‌گیری را انجام می‌دهد و مقدار مربع خطای هر داده را محاسبه می‌کند.

تعداد تکرار در این الگوریتم برابر عددی است که الگوریتم بعد از رسیدن به همگرایی، از آن خارج می‌شود. در این زمینه الگوریتم را تا رسیدن به همگرایی مناسب با دورهای مختلف اجرا نموده تا به جواب مناسب دست یافته و خطای تحلیل را نیز کاهش داد.

۴-یافته‌ها

تجزیه و تحلیل داده‌های پژوهش حاضر در دو سطح آمار توصیفی و بخش شبیه‌سازی صورت گرفت. در بخش توصیفی بررسی داده‌های موجود در دیتاست ارائه شده است. در گام بعد بررسی روند شبیه‌سازی در نرم‌افزار Matlab ارائه شده است.

۴-۱-تحلیل توصیفی



شکل ۳- تغییرات اعتماد در داده‌ها

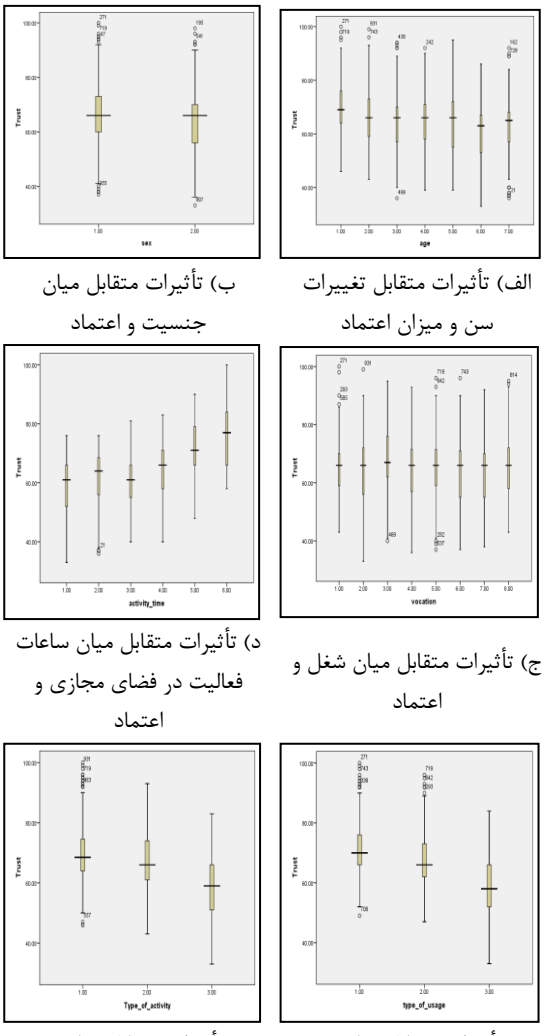
اغلب مردم اعتماد مناسبی به فضای مجازی دارند که به احتمال‌زیاد به دلیل سیاست‌گذاری‌های پلتفرم‌ها و سازمان های موجود در فضای مجازی و نیز وضع قوانین در این زمینه بوده است. اما با توجه به شکل (۳)، همچنان افراد با اعتماد بسیار کم و نیز اعتماد بسیار زیاد نیز مشاهده می شود. در ادامه، بررسی بر اساس میزان اعتماد میان گروه‌ها مختلف تحلیلی صورت پذیرفته است. ابتدا بررسی بر روی تغییرات میزان اعتماد در گروه‌های مختلف سنی و میزان اعتماد به افراد در فضای مجازی مورد ارزیابی قرار گرفته است که برای این منظور از نمودار جعبه‌ای مطابق شکل (۴) استفاده‌شده است.

الف) تأثیرات متقابل تغییرات سن و میزان اعتماد ب) تأثیرات متقابل میان جنسیت و اعتماد

ج) تأثیرات متقابل میان شغل و اعتماد د) تأثیرات متقابل میان ساعات فعالیت در فضای مجازی و اعتماد

ه) تأثیرات متقابل میان نوع فعالیت در فضای مجازی و اعتماد و) تأثیرات متقابل میان نوع روابط در فضای مجازی و اعتماد

رابطه اعتماد و متغیرهای ششگانه قبل از بررسی به وسیله شبکه فازی عصبی تطبیقی، در نرم‌افزار SPSS بررسی شده‌اند، تا ارتباط دسته‌بندی اعتماد بر اساس این متغیرها با اعتماد ارائه شده، بررسی گردد و درستی وجود این متغیرها نیز به نوعی تایید گردد. در جدول ۱ نتیجه تحلیل های آماری انجام شده بر روی ارتباط میان متغیرهای ششگانه برای پیش‌بینی اعتماد با میزان اعتماد افراد، ارائه شده است. با توجه به توزیع غیرنرمال داده‌ها که با استفاده از آزمون کلوموگروف‌اسمیرنوف بررسی شد ($p<0.05$)، از آزمون کروسکال‌والیس برای بررسی ارتباط میان متغیرها با اعتماد استفاده شده است.



الف) تأثیرات متقابل تغییرات سن و میزان اعتماد

ب) تأثیرات متقابل میان جنسیت و اعتماد

ج) تأثیرات متقابل میان شغل و اعتماد

د) تأثیرات متقابل میان ساعات فعالیت در فضای مجازی و اعتماد

ه) تأثیرات متقابل میان نوع فعالیت در فضای مجازی و اعتماد

و) تأثیرات متقابل میان نوع روابط در فضای مجازی و اعتماد

شکل ۴- اثرات متقابل معیارها و اعتماد

جدول ۱: تحلیل آماری ارتباط بین متغیرهای تحقیق

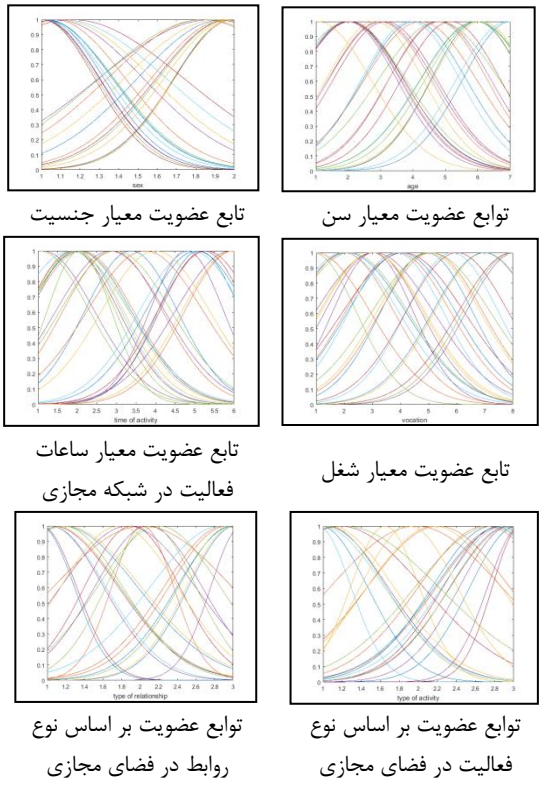
متغیر	زیرمتغیرها	میانگین اعتماد	انحراف معیار اعتماد	مقدار احتمال
جنسیت	زن	۶۶.۸۴۹	۱۱.۰۹۵	۰/۰۰۱>
	مرد	۶۴.۰۰۸	۱۱.۵۴۳	
سن	۱۸-۲۵	۷۰.۴۹۷	۱۰.۷۴۱	۰/۰۰۱>
	۲۵-۳۰	۶۶.۹۴۲	۱۱.۰۹۵	
	۳۰-۳۵	۶۴.۷۰۱	۱۰.۹۳۵	
	۳۵-۴۰	۶۵.۰۰۰	۱۰.۹۵۴	
	۴۰-۴۵	۶۵.۱۸۳	۱۱.۹۸۴	
	۴۵-۵۰	۶۱.۷۶۴	۱۱.۰۳۳	
	بیش از ۵۰	۶۲.۹۹۳	۱۱.۲۵۳	
وضعیت کاری	بیکار	۶۵.۵۱۹	۱۰.۳۲۵	۰.۰۵
	دانشجو	۶۵.۱۵۸	۱۱.۹۸۲	
	اداری	۶۸.۷۵۷	۱۱.۴۳۱	
	کارگری	۶۴.۲۸۷	۱۲.۱۷۱	
	مدیریتی	۶۵.۶۱۳	۱۰.۷۸۸	
	نظامی	۶۴.۵۳۰	۱۱.۹۴۵	
	خدماتی	۶۳.۸۴۶	۱۱.۳۲۷	
	سایر	۶۶.۰۵۱	۱۰.۶۳۹	
ساعات فعالیت	کمتر از ۱	۵۸.۶۰۰	۹.۳۰۲	۰/۰۰۱>
	۲_۱	۶۱.۵۵۶	۹.۳۱۲	
	۳_۲	۶۰.۴۸۸	۸.۶۰۹	
	۴_۳	۶۴.۴۰۵	۹.۲۶۷	
	۵_۴	۷۱.۴۳۸	۹.۱۷۲	
	بیشتر از ۵	۷۶.۹۸۸	۱۰.۳۳۴	
نوع استفاده	تفریح	۷۱.۲۰۷	۹.۶۱۴	۰/۰۰۱>
	ارتباطات جدید	۶۷.۴۶۳	۹.۹۴۵	
	کار	۵۸.۴۶۳	۱۰.۴۷۶	
نوع روابط	دوستانه	۶۹.۷۴۷	۹.۶۱۵	۰/۰۰۱>
	غریبه ها برای روابط جدید	۶۷.۴۶۴	۹.۹۴۵	
	کار	۵۸.۴۶۳	۱۰.۴۷۶	

براساس بخش‌های مختلف شکل (۴) و مقادیر ارائه شده در جدول ۱، مشاهده می‌شود که بیشترین اعتماد در گروه های سنی پایین مشاهده شده است و در بازه‌ی ۲۵ الی ۴۵ سال، تقریباً تغییرات میانگین اعتماد ثابت بوده است. پس می‌توان بیان نمود رابطه میان اعتماد و سن نمونه-های موجود در دیتاست تا حدودی به‌صورت معکوس بوده است. همچنین میزان اعتماد بانوان در قیاس با آقایان بیشتر بوده و این نکته از چارک‌های اول و چهارم نمودارهای جعبه‌ای قابل استنباط است. البته لازم به ذکر است که در میان هر دو گروه، افرادی با اعتماد بسیار بالا به دیگران در فضای مجازی وجود داشته‌اند. همچنین الگوهای رفتاری در هر رده شغلی کاملاً متفاوت بوده است. به‌طور مثال در گروه افراد بی‌کار بیشترین تغییرات در خارج از چارک چهارم بیشتر بوده و این رفتار تا حدود زیادی از روی رفتار طبیعی برای اعتماد به دیگران برای اعتماد برای فعالیت‌های نظیر یافتن کار و یا عدم اعتماد به دلیل اعتمادهای نافرجام برای گرفتن موقعیت‌های مناسب‌تر، بوده است. همچنین بیشترین بازه‌ی اعتماد در میان دانشجویان مشاهده می‌شود که اختلاف میان کمترین و بیشترین مقدار اعتماد، ۶۶ واحد بوده است. همچنین مشاهده شد که با افزایش ساعات حضور در فضای مجازی به‌صورت پیوسته، میزان اعتماد نیز بیشتر می‌شود و افرادی که با اهداف گذران اوقات و تفریح در فضای مجازی حضور داشته‌اند، میزان اعتماد بیشتری نیز به سایر افراد در این فضا داشته و افرادی که اهداف کاری داشته‌اند، کمترین میزان اعتماد را از خود نشان داده‌اند. همچنین افرادی که تنها با دوستان خود ارتباط داشته‌اند، بیشترین اعتماد را در میان گروه‌های دیگر داشته‌اند. سپس با اختلافی اندک افرادی به روابط با غریبه‌ها را برای ایجاد روابط جدید دنبال می‌نمایند، در جایگاه بعدی اعتماد بوده و افرادی که روابط کاری خود را در این فضا دنبال نموده‌اند، اعتماد کمتری در قیاس با دو گروه دیگر داشته‌اند.

۲-۴-شبکه فازی عصبی تطبیقی

در ابتدا باید برای الگوریتم فازی-عصبی داده‌ها را به سه گروه داده‌های آموزش، تست و بررسی تقسیم‌بندی نمود. بدین منظور در این پژوهش تصمیم بر این شد تا ۸۰۰ نمونه به‌عنوان داده‌های آموزش وارد شده و برای گروه‌های آزمون (تست) و بررسی هر کدام ۱۰۰ نمونه در نظر گرفته شده است. در ابتدا بعد از تخصیص این موارد، توابع مدل‌سازی اولیه صورت گرفته شده و باید مشخصات شبکه را در اختیار

نرم‌افزار متلب قرار داد. در این پژوهش از روش خوشه‌بندی کاهشی به دلیل کاهش زمان تحلیل در این روش در قیاس با روش پارتیشن‌بندی استفاده شده است. دلیل این کار نیز تعداد زیاد نمونه‌ها و متغیرهاست که باعث به وجود آمدن هزاران گره برای تحلیل در شبکه خواهد شد.



توابع عضویت معیار سن — تابع عضویت معیار جنسیت

تابع عضویت معیار شغل — تابع عضویت معیار ساعات فعالیت در شبکه مجازی

توابع عضویت بر اساس نوع فعالیت در فضای مجازی — توابع عضویت بر اساس نوع روابط در فضای مجازی

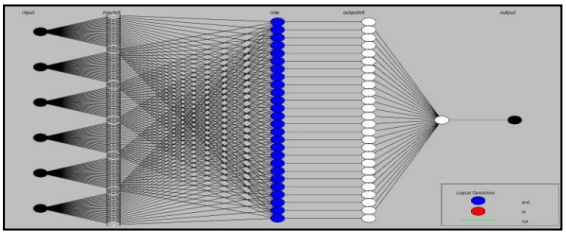
شکل ۵- توابع عضویت معیارهای ورودی

مطابق شکل (۵)، در این الگوریتم برای هر متغیر ۲۶ تابع عضویت ترسیم شده است که با توجه به ساختار الگوریتم که تمام نقش‌ها از & استفاده‌شده است، باید به تعداد توابع عضویت، نقش نیز معرفی گردد. لازم به ذکر است که این نقش‌ها بعد از آموزش شبکه به درستی تغییر نموده و ضرایب درستی را برای تشخیص ارائه خواهند داد.

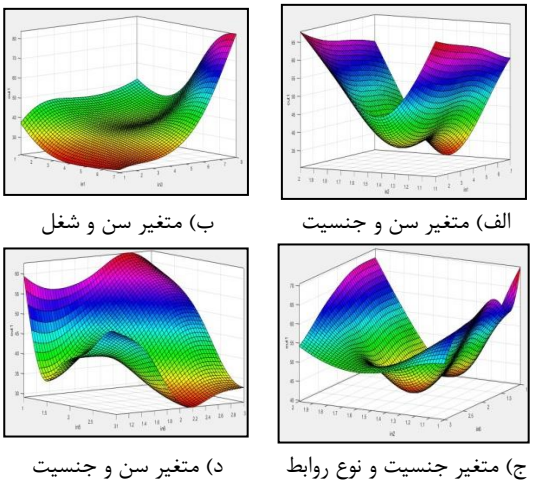
بعد از ارائه مدل و ورودی‌های الگوریتم، ساختار شبکه ترسیم شده و فایل خامی از شبکه در دسترس خواهد بود. در ادامه، شبکه مورداستفاده در این الگوریتم، در شکل (۶) ارائه شده است.

بعد از مشخص شدن ساختار شبکه، یک حالت n بعدی از متغیرها تشکیل‌شده که هر نقطه‌ای در این فضا مصادف با یک مقدار از اعتماد خواهد بود. اما متأسفانه به دلیل عدم توانایی ترسیم نرم‌افزارها در فضایی بیش از ۳ بعد، باید برای هر متغیر، این فضا را به‌صورت دوبه‌دو ترسیم نمود که حاصل کار به‌عنوان نمونه در شکل (۷) نشان داده‌شده است.

در ادامه به بررسی برخی فضای تغییرات اعتماد در مدل پژوهش بر اساس نقش‌ها و توابع عضویت آموزش داده شده، پرداخته شده است.



شکل ۶- مدل اصلی الگوریتم پژوهش

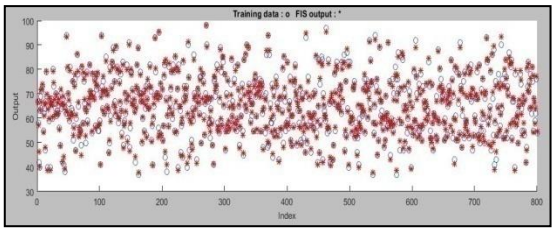


الف) متغیر سن و جنسیت — ب) متغیر سن و شغل

ج) متغیر جنسیت و نوع روابط — د) متغیر سن و جنسیت

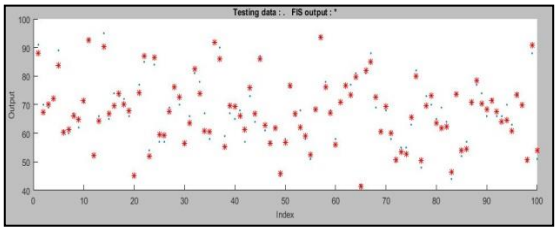
شکل ۷- نمایش سه‌بعدی تغییرات اعتماد بر اساس تغییرات دو متغیر ورودی

با توجه به اینکه ۶ متغیر در این پژوهش وجود داشته ۱۵ زوج مختلف از متغیرها نیز به دست خواهد آمد. پس برای تشخص باید ۱۵ مرتبه متغیرهایی که در هر بار انتخاب نشده باشند را به‌صورت ثابت در نظر گرفت و برای دو متغیر در حال تحلیل میزان اعتماد دوطرفه محاسبه شود. برای سنجش اعتماد در فضای مجازی با الگوریتم حاضر با ثابت ماندن ۴ متغیر و تغییرات دو متغیر دیگر، به‌راحتی از این نمودارها می‌توان میزان اعتماد را محاسبه نمود. اما با بیشتر شدن تعداد متغیرها به دلیل محاسبات بسیار زیاد، باید الگوریتم این محاسبات را سرعت بخشد. در نمودارهای ارائه شده می‌توان مشاهده نمود که روابط میان زوج متغیرها نیز گاهی بسیار پیچیده بوده است و نمی‌توان روند خاصی برای زوج متغیرها نیز در نظر گرفت و این به دلیل تعداد زیاد نمونه‌ها و نیز آموزش دقیق الگوریتم و یافتن ضرایب تغییر، بسیار مناسب برای تشخیص اعتماد می‌باشد. در ادامه نمودارهای آموزش الگوریتم برای پیش‌بینی دقیق‌تر ارائه شده است.



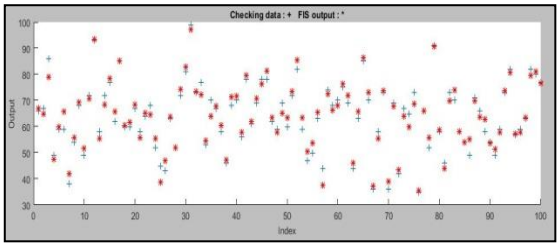
شکل ۸- مقایسه داده‌های واقعی و داده‌های آموزش داده‌شده بعد از یادگیری الگوریتم

در شکل (۸) می‌توان مشاهده نمود که مقادیر تا حد بسیار زیادی بر روی یکدیگر منطبق بوده است. هر چه این نقاط بیشتر بر روی یکدیگر مطبق گردند نشان از آموزش بهتر الگوریتم دارد. نکته‌ی دیگر است که به دلیل اینکه الگوریتم با همین داده‌ها آموزش دیده است، بهتر است از داده‌های جانبی که آموزش ندیده و برایش جدید می‌باشند و پاسخ اعتماد نیز برای آن مشخص است، بررسی صورت پذیرد. سپس بعد از این کار، مجدداً الگوریتم یادگیری خود را تقویت می‌نماید. در ادامه داده‌های تست را می‌توان مشاهده نمود که ۱۰۰ نمونه برای این کار در نظر گرفته شده است.



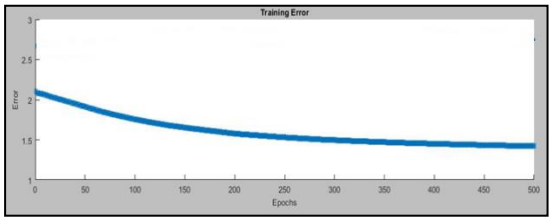
شکل ۹- مقایسه داده‌های واقعی و داده‌های تست توسط الگوریتم آموزش دیده

در تصویر شکل (۹) می‌توان مشاهده نمود که اختلاف میان تشخیص‌ها برای داده‌هایی که تاکنون با آن‌ها مواجه نشده بود، اندکی ضعیف‌تر بوده است که طبیعی نیز خواهد بود. اما با این وجود همچنان نتایج نشان داده است که تمامی پاسخ‌ها و شرایط را تا حدود بسیار زیادی نزدیک به مقدار واقعی بیان نموده است و در تشخیص خود کاملاً موفق بوده است. در ادامه بررسی داده‌های چک (بررسی) صورت گرفته است.



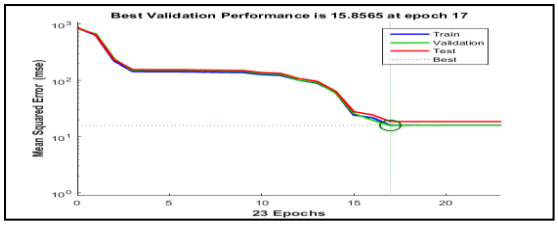
شکل ۱۰- مقایسه داده‌های واقعی و داده‌های بررسی توسط الگوریتم آموزش دیده و تست‌شده

همان‌طور که در شکل (۱۰) مشخص است، الگوریتم ارائه شده به درستی آموزش دیده و توانسته است برخی از موارد را کاملاً درست حدس زده و میزان اعتماد بیان‌شده از طرف کاربران را دقیقاً و با دقت بسیار بالایی به دست آورد. از طرف دیگر فاصله مشاهده شده در بخش تست، در این بخش مشاهده نشده است و این اختلاف پاسخ تا حد بسیار مطلوبی کاهش یافته است. این نکته نشان از این است که این پژوهش توسط دیتاست و نوع برخورد و آموزش مدل خود، توانسته به‌خوبی توسط مشخصات فردی قابل‌اندازه‌گیری افراد، به درستی و بسیار نزدیک به نظر افراد، میزان اعتمادشان به سایرین در فضای مجازی را پیش‌بینی نماید. در ادامه، بررسی میزان خطای این آموزش در طول ۵۰۰ چرخه آموزش در نظر گرفته شده برای مدل فازی-عصبی تطبیقی ارائه شده صورت پذیرفته شده است که نتیجه آن در شکل (۱۱) نشان داده‌شده است.



شکل ۱۱- نمودار تغییرات خطای آموزش در طول آموزش شبکه

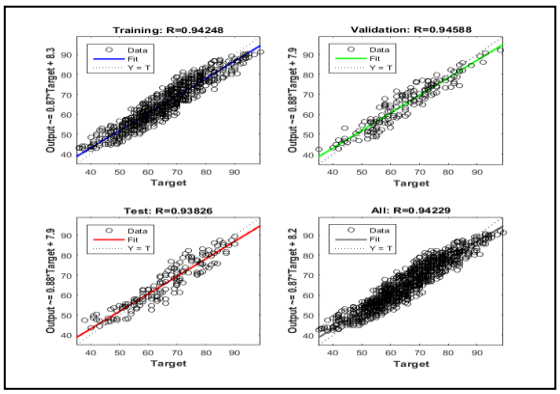
مشاهده می‌شود. الگوریتم پیاده‌سازی شده درنهایت دارای ۹۸.۵ درصد دقت در پیش‌بینی است و در ادامه بر اساس دیتاست جمع‌آوری‌شده پیش‌بینی به روش شبکه عصبی پیش‌خور نیز صورت گرفته شده و نتایج آن در شکل (۱۲) ارائه شده است.



شکل ۱۲- روند همگرایی آموزش با شبکه عصبی پیش‌خور

در شکل ارائه شده مشاهده شد که پیش‌بینی با خطای تقریباً ۱۶ درصدی (دقت ۸۴ درصدی) صورت گرفته شده است. مقایسه شکل‌های (۱۱) و (۱۲) نشان از دقت بالای الگوریتم فازی عصبی ارائه شده نسبت به شبکه عصبی عادی برای تشخیص سطح اعتماد در شبکه‌های مجازی دارد. شبکه‌های عصبی عادی به دلیل داشتن رویکرد خطی

در تحلیل‌ها، میزان دقت کمتری در قیاس با سایر روش‌های تحلیل غیرخطی خواهند داشت، زیرا در تحلیل خطی فضای محتمل کمتری برای جستجوی پاسخ بهینه وجود خواهد داشت، به همین دلیل ورود تحلیل فازی عصبی سبب شد تا دقت تحلیل به‌مراتب بهبود یابد. همچنین برای تعیین قدرت تشخیص تغییرات در نمونه¬ها توسط الگوریتم ارائه شده، با استفاده از مدل رگرسیونی این مقدار تعیین شده است و نتایج در شکل (۱۳) نشان داده‌شده است.



شکل ۱۳- خروجی رگرسیونی پیش‌بینی اعتماد بر اساس معیارهای ورود

با استفاده از مدل رگرسیون تعیین شده است که برای متغیرها در نظر گرفته شده حدوداً تا ۹۵ درصد تغییرات نمونه¬ها قابل تشخص خواهند بود. البته باید بیان نمود که این درصد بیان‌شده تنها برای تغییرات واریانس اعتماد بوده است که با درصد دقت بیان‌شده برای مقایسه با شبکه فازی عصبی متفاوت است.

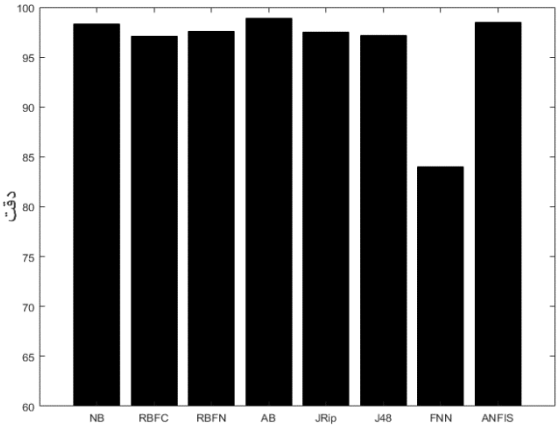
در آخرین آزمایش، دقت روش پیشنهادی با سایر روش‌های متنوعی که تاکنون به‌منظور پیش‌بینی و تشخیص اعتماد در تحقیقات گذشته ارائه‌شده‌اند، مقایسه شده است. جدول ۲ مقادیر دقت مربوط به این روش‌ها را نشان می‌دهد.

جدول ۲- مقایسه دقت روش پیشنهادی با سایر روش‌ها

روش تشخیص اعتماد دقت

روش تشخیص اعتماد	دقت
Naive Bayes(NB)	۹۸.۳
Radial Basis Function Classifier (RBFC)	۹۷.۱
Radial Basis Function Network (RBFN)	۹۷.۶
AdaBoost(AB)	۹۸.۹
Decision tree algorithm JRip	۹۷.۵
Decision tree algorithms J48	۹۷.۲
Feed Forward Network (FFN)	۸۴
ANFIS(proposed)	۹۸.۵

شکل (۱۴) نیز نمودار ستونی دقت روش‌های مختلف را نشان می‌دهد. در این شکل محور افقی، عنوان هر روش و محور عمودی، درصد دقت آن را نشان می‌دهد.



شکل ۱۴- نمودار ستونی مقایسه دقت روش پیشنهادی با سایر روش‌ها

مشاهده می‌شود که روش پیشنهادی نسبت به اغلب روش‌های گذشته تشخیص اعتماد، عملکرد بهتری داشته است. تنها روش AdaBoost نسبت به روش پیشنهادی اندکی بهتر عمل می‌کند که البته این روش جزء یادگیری‌های گروهی محسوب می‌شود که از چندین مدل به‌جای یک مدل استفاده می‌کنند. ازآنجایی‌که مدل پیشنهادی، شبکه‌های عصبی و مفاهیم منطق فازی را باهم در قالب یک مدل فازی-عصبی تطبیقی به کار می‌برد، از امکانات هر دو در قالب یک سیستم بهره می‌برد و قادر است میزان اعتماد را به‌خوبی و با درصد خطای کم محاسبه کند.

۵-نتیجه‌گیری

اولین نتیجه‌ای که از این پژوهش می‌توان حاصل نمود این است که ویژگی‌های شخصی به دلیل ذاتی و منحصر به فرد بودن برای هر فرد، بهترین عامل برای مشخص نمودن رفتار افراد از جمله اعتماد است. در همین راستا پژوهش‌های زیادی صورت گرفته است که بر روی رابطه قوی میان اعتماد و ویژگی‌های شخصیتی افراد تأکید دارند [۳۱، ۳۲ و ۳۳]. همچنین نتایج به‌دست‌آمده از این پژوهش نیز این مهم را در بررسی دیتاست موجود کاملاً تائید نموده است، زیرا در بخش بررسی و ارزشیابی الگوریتم فازی عصبی، داده‌هایی که در بخش آموزش شرکت داده نشده بودند به درستی تشخیص و میزان اعتماد آن‌ها با درصد خطای کم محاسبه شد. این اتفاق ناشی از مناسب بودن دیتاست و نیز الگوریتم پیشنهادی تحلیلی است. ترکیب شبکه عصبی با تحلیل‌های فازی باعث بهبود در نتایج خواهد شد که این

نکته به دلیل استفاده پیوسته و در نظر گرفتن بازه‌های احتمالاتی بسیار وسیع‌تر در بخش آموزش و نیز تخصیص اوزان برای تشخیص می‌باشد. عامل در نظر گرفتن احتمالات، باعث بهبود در قدرت تشخیص حتی تا درصدهای بسیار بالا شده است. البته لازم به ذکر است که نوع دیتاست نیز در این دقت اثرگذار است و با توجه به اینکه در این پژوهش هدف یافتن میزان اعتماد بر اساس ویژگی های شخصیتی و نیز شرایط استفاده از اینترنت بود و در این زمینه دیتاست مناسبی نیز وجود نداشت، با مشارکت بخش‌های مختلف اصناف و دانشگاهی اقدام به گردآوری داده‌های افراد شد. با توجه به اینکه مشخصات ثبتی افراد دارای اهمیت بود، این ویژگی‌ها قابلیت تغییر کمی را خواهند داشت و به‌عنوان دیتاست تائید شده قابلیت استفاده دارد. با در نظر گرفتن روش خوشه‌بندی کاهشی برای توابع عضویت می‌توان تا حد زیادی روابط در شبکه و مدل ارائه شده را کاهش داد که در نتیجه حجم عظیمی از محاسبات را کاهش می‌دهد و زمان اجرای برنامه به‌شدت کاهش می‌یابد. همچنین به دلیل در نظر گرفتن فضای پیوسته و تحت کنترل بیشتر در توابع عضویت، می‌توانند نتایج بسیار مطلوبی ارائه دهند که در پژوهش حاضر نیز این قدرت کاملاً مشهود بوده است. لازم به ذکر است که با توجه به بررسی و مقایسه‌های صورت گرفته بر اساس شبکه عصبی پیش‌خور و سایر روش‌های مشابه مشخص گردید که میزان دقت الگوریتم فازی عصبی ارائه شده، بالاتر از مدل‌های مشابه بوده است.

مراجع

[1] Yevseiev, Serhii, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, and Iryna Manzhul. "Modeling the protection of personal data from trust and the amount of information on social networks." EUREKA: Physics and Engineering,(1) (2021): 24-31.

[2] Laptiev, Oleksandr, Vitalii Savchenko, Andrii Kotenko, Volodimir Akhramovych, Vladimir Samosyuk, German Shuklin, and Anatjliy Biehun. "Method of determining trust and protection of personal data in social networks." International Journal of Communication Networks and Information Security 13, no. 1 (2021): 15-21.

[3] Xue, Kaijing, Shili Guo, Yi Liu, Shaoquan Liu, and Dingde Xu. "Social networks, trust, and disaster-risk perceptions of rural residents in a multi-disaster environment: evidence from Sichuan, China." International journal of environmental research and public health 18, no. 4 (2021): 2106.

[4] Pérez-Escoda, Ana, Luis Miguel Pedrero-Esteban, Juana Rubio-Romero, and Carlos Jiménez-Narros. "Fake news reaching young people on social networks: Distrust challenging media literacy." Publications 9, no. 2 (2021): 24.

[5] Adali, Sibel, Robert Escriva, Mark K. Goldberg, Mykola Hayvanovych, Malik Magdon-Ismail, Boleslaw K. Szymanski, William A. Wallace, and Gregory Williams. "Measuring behavioral trust in social networks." In 2010 IEEE international conference on intelligence and security informatics, pp. 150-152. IEEE, 2010.

[6] Sherchan, Wanita, Surya Nepal, and Cecile Paris. "A survey of trust in social networks." ACM Computing Surveys (CSUR) 45, no. 4 (2013): 1-33.

[7] Golbeck, Jennifer. "Generating predictive movie recommendations from trust in social networks." In International Conference on Trust Management, pp. 93-104. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006.

[8] Walter, Frank E., Stefano Battiston, and Frank Schweitzer. "Personalised and dynamic trust in social networks." In Proceedings of the third ACM conference on Recommender systems, pp. 197-204. 2009.

[9] Golbeck, Jennifer. "Combining provenance with trust in social networks for semantic web content filtering." In Provenance and Annotation of Data: International Provenance and Annotation Workshop, IPAW 2006, Chicago, IL, USA, May 3-5, 2006, Revised Selected Papers, pp. 101-108. Springer Berlin Heidelberg, 2006.

[10] Hamdi, Sana, Alda Lopes Gancarski, Amel Bouzeghoub, and Sadok Ben Yahia. "Tison: Trust inference in trust-oriented social networks." ACM Transactions on Information Systems (TOIS) 34, no. 3 (2016): 1-32.

[11] Gong, Zaiwu, Hui Wang, Weiwei Guo, Zejun Gong, and Guo Wei. "Measuring trust in social networks based on linear uncertainty theory." Information Sciences 508 (2020): 154-172.

[12] Laifa, Meriem, Samir Akrouf, and Ramdane Mammeri. "Forgiveness and trust dynamics on social networks." Adaptive Behavior 26, no. 2 (2018): 65-83.

[13] Massa, Paolo. "A survey of trust use and modeling in real online systems." In Trust in E-services:

Technologies, Practices and Challenges, pp. 51-83. IGI Global, 2007.

[14] Ruohomaa, Sini, and Lea Kutvonen. "Trust management survey." In International Conference on Trust Management, pp. 77-92. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005.

[15] Hoffman, Kevin, David Zage, and Cristina Nita-Rotaru. "A survey of attack and defense techniques for reputation systems." ACM Computing Surveys (CSUR) 42, no. 1 (2009): 1-31.

[16] Ruan, Yefeng, and Arjan Durresi. "A survey of trust management systems for online social communities–trust modeling, trust inference and attacks." Knowledge-Based Systems 106 (2016): 150-163.

[17] Abdul-Rahman, Alfarez, and Stephen Hailes. "Supporting trust in virtual communities." In Proceedings of the 33rd annual Hawaii international conference on system sciences, pp. 9-pp. IEEE, 2000.

[18] Wu, Nannan, Yejun Xu, Xia Liu, Huimin Wang, and Enrique Herrera-Viedma. "Water–Energy–Food nexus evaluation with a social network group decision making approach based on hesitant fuzzy preference relations." Applied Soft Computing 93 (2020): 106363.

[19] Zheng, Ye-Fu, and Jun Xu. "A trust transitivity model for group decision making in social network with intuitionistic fuzzy information." Filomat 32, no. 5 (2018): 1937-1945.

[20] Porcel, Carlos, Alberto Ching-López, Gastón Lefranc, Vincenzo Loia, and Enrique Herrera-Viedma. "Sharing notes: An academic social network based on a personalized fuzzy linguistic recommender system." Engineering Applications of Artificial Intelligence 75 (2018): 1-10.

[21] Wu, Jian, Sha Wang, Francisco Chiclana, and Enrique Herrera-Viedma. "Two-fold personalized feedback mechanism for social network consensus by uninorm interval trust propagation." IEEE Transactions on Cybernetics 52, no. 10 (2021): 11081-11092.

[22] Pei, Feng, Yu-Wei He, An Yan, Mi Zhou, Yu-Wang Chen, and Jian Wu. "A consensus model for intuitionistic fuzzy group decision-making problems based on the construction and propagation of trust/distrust relationships in social networks." International Journal of Fuzzy Systems 22 (2020): 2664-2679.

[۲۳] حسینی، سیاوش، سعید ستایشی، غلامحسین روشنی، عبدالحمید زاهدی، و فرزین شماع، "افزایش کارآیی جریان‌سنج دوفازی با استفاده از روشهای استخراج ویژگی حوزه ی فرکانسو شبکه عصبی در طیف خروجی آشکارساز"، نشریه مدل‌سازی در مهندسی ۱۹، ۶۷ (۱۴۰۰): ۴۷-۵۷.

[۲۴] قنادزاده، حسین، الهیار داغبندان، محمد اکبری زاده، و میثم آزادیان، " مدل‌سازی سیستمهای تعادلی بخار-مایع و مایع-مایع با استفاده از مدلهای ترمودینامیکی، ساختارهای فازی و شبکههای عصبی نوع GMDH "، نشریه مدل‌سازی در مهندسی ۱۶، ۵۵، (۱۳۹۷):۱۹-۳۳.

[۲۵] میراخورلو، فرزانه، و ابراهیم نجفی کانی، "بررسی و پیش‌بینی خواص فیزیکی و مکانیکی کامپوزیت کاه و گچ به کمک مدل شبکه استنتاج عصبی فازی تطبیقی"، نشریه مدل‌سازی در مهندسی ۱۷، ۵۸ (۱۳۹۸): ۲۶۷-۲۷۸.

[26] Hallowell, Nina, Shirlene Badger, Aurelia Sauerbrei, Christoffer Nellåker, and Angeliki Kerasidou. "“I don’t think people are ready to trust these algorithms at face value”: trust and the use of machine learning algorithms in the diagnosis of rare disease." BMC medical ethics 23, no. 1 (2022): 112.

[27] Rechkemmer, Amy, and Ming Yin. "When confidence meets accuracy: Exploring the effects of multiple performance indicators on trust in machine learning models." In Proceedings of the 2022 chi conference on human factors in computing systems, pp. 1-14. 2022.

[28] Nakashima, Heitor Hoffman, Daielly Mantovani, and Celso Machado Junior. "Users’ trust in black-box machine learning algorithms." Revista de Gestão (2022).

[29] Shetty, Nisha P., Balachandra Muniyal, Pratyay Prakhar, Angad Singh, Gunveen Batra, Akshita Puri, Divya Bhanu Manjunath, and Vidit Vinay Jain. "Trust Based Resolving of Conflicts for Collaborative Data Sharing in Online Social Networks." In Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2022, Volume 2, pp. 35-48. Singapore: Springer Nature Singapore, 2022.

[30] Almuzaini, Fatimah, Sarah Alromaih, Alhanoof Althnian, and Heba Kurdi. "WhatsTrust: A trust management system for WhatsApp." Electronics 9, no. 12 (2020): 2190.

[31] Bansal, Gaurav, Fatemeh Mariam Zahedi, and David Gefen. "Do context and personality matter? Trust and privacy concerns in disclosing private information online." Information & Management 53, no. 1 (2016): 1-21.

[32] Salem, Maha, Gabriella Lakatos, Farshid Amirabdollahian, and Kerstin Dautenhahn. "Would you trust a (faulty) robot? Effects of error, task type and personality on human-robot cooperation and trust." In Proceedings of the tenth annual ACM/IEEE international conference on human-robot interaction, pp. 141-148. 2015.

[33] Fonagy, Peter, Patrick Luyten, Elizabeth Allison, and Chloe Campbell. "What we have changed our minds about: Part 1. Borderline personality disorder as a limitation of resilience." Borderline personality disorder and emotion dysregulation 4 (2017): 1-11.

[34] Abbasimehr, Hossein, and MohammadJafar Tarokh. "Trust prediction in online communities employing neurofuzzy approach." Applied Artificial Intelligence 29, no. 7 (2015): 733-751.

[35] Khammar, Gholamali, Behnam Mohammadi, Vahid Dehbashi, and Hadi Esmaeilpour Moghadam. "Evaluation of Trust Indices to E-City Network Using Adaptive Network-Based Fuzzy Inference System (ANFIS) and RBF Network (Case Study of Ghir City)." Social Welfare Quarterly 17, no. 64 (2017): 199-235.

[36] Nuñez-Gonzalez, J. David, Manuel Graña, and Bruno Apolloni. "Reputation features for trust prediction in social networks." Neurocomputing 166 (2015): 1-7.