طراحی مدلی مبتنی بر فناوری زنجیره بلوکی برای تقویت امنیت سایبری در صنعت بانکداری

حسین عموزاد خلیلی*
دانشگاه آزاد اسلامی، نوشهر، ایران
amoozad92@yahoo.com

ندا حقی**
دانشگاه آزاد اسلامی، تهران، ایران
nedahaghi.academic@gmail.com

رضا توکلی مقدم***
دانشگاه تهران، تهران، ایران
tavakoli@ut.ac.ir

تاریخ دریافت: ۱۴۰۰/۱۰/۰۵
تاریخ اصلاحات: ۱۴۰۱/۰۶/۲۷
تاریخ پذیرش: ۱۴۰۱/۰۷/۰۹

چکیده

مطالعه حاضر به دنبال تأمین این هدف است که مدلی مبتنی بر فناوری زنجیره بلوکی جهت تقویت امنیت سایبری در صنعت بانکداری براساس شبکه عصبی مصنوعی را مورد ارزیابی قرار دهد. این مدل براساس مدل مفهومی است که در یک شبیه‌سازی شبکه عصبی پرسپترون چند لایه که فرایندی مانند زنجیره بلوکی را شبیه‌سازی می‌کند به‌کار گرفته شده است. همچنین شبکه‌های عصبی ایجادشده در زنجیره بلوکی از پیوند قوی برخوردار هستند. علاوه بر این فناوری زنجیره بلوکی توانایی ایجاد امنیت سایبری را خواهد داشت. کارایی مرتبط با فناوری‌های زنجیره بلوکی پس از یادگیری به سطح ۷۷۰/۵۷ واحد رسیده و نشان‌دهنده آن است که روش پرسپترون چند لایه برای یادگیری روند فناوری زنجیره بلوکی می‌تواند به کارایی بیشتر برای امنیت سایبری منجر شود. مقدار واریانس برابر با ۲۷/۷۷ و همبستگی برابر با ۰/۹۹ شده است که قابلیت اطمینان بالا برای یک مدل مبتنی بر فناوری زنجیره بلوکی برای تقویت امنیت سایبری را نشان می‌دهد. در مجموع طراحی مدل مبتنی بر هزینه‌های عملیاتی، ارزیابی قابلیت اطمینان و اعتبار تجاری و خدمات مشتریان می‌تواند به تقویت امنیت سایبری در حوزه فناوری زنجیره بلوکی منجر شود.

واژگان کلیدی

زنجیره بلوکی؛ امنیت سایبری؛ بانکداری الکترونیک؛ اعتبار تجاری؛ شبکه عصبی مصنوعی.

۱- مقدمه

طراحی مدلی مبتنی بر فناوری زنجیره بلوکی جهت تقویت امنیت سایبری در صنعت بانکداری یکی از رویکردهای نوین در صنعت بانکداری می‌باشد که مبتنی بر زنجیره‌های بلوکی امن ایجاد می‌شود. صنعت بانکداری نیاز دارد تا همیشه فناوری‌های نوین را جهت حفاظت از داده‌ها بکار گیرد. فناوری زنجیره بلوکی یکی از روش‌های نوین است که در مرحله رمزنگاری داده‌های اولیه تا مقصد توانایی قدرتمندی را از خود نشان داده است. اما هنوز مدل‌های طراحی براساس متغیرها با قابلیت پشتیبانی آن در مراحل ابتدایی قرار دارد. این عملکرد می‌تواند به بهبود و کارایی بیشتر صنعت بانکداری منجر شود. چنین موضوعی در صنعت بانکداری به یک بایسته مبدل شده است، به‌طوریکه ارائه خدمات بانکی به جای مزیت رقابتی، یک الزام راهبردی است. اما مسأله مهم این است که چگونه می‌توان امنیت سایبری را با استفاده از زنجیره‌های بلوکی ایجاد کرد، به صورتیکه صنعت بانکداری در استفاده از آنها یک صنعت امن در نگهداری و انتقال داده‌های کاربران و مشتریان خود باشد. این موضوع سؤالی است که نیاز به مشخص‌سازی متغیرهایی جهت استفاده در فناوری بلاک‌چین دارد [۱]، دغدغه اصلی طراحی مدلی مبتنی بر فناوری زنجیره بلوکی جهت تقویت امنیت سایبری در صنعت بانکداری به اهمیت پایگاه داده‌ها در صنعت بانکداری اینترنتی باز می‌گردد [۲]. فناوری بلاک‌چین به‌عنوان یک پایگاه داده امن و قابل اعتماد و شفاف در سیستم‌های سازمانی می‌تواند علاوه بر افزایش امنیت در نگهداری اطلاعات، سازمان‌دهی بهتری داشته و همچنین درصد خطا در سیستم را به حداقل ممکن برساند [۹] اما باید مشخص گردد که چه متغیرهایی برای ساخت مدل طراحی‌شده فناوری بلاک‌چین در اولویت قرار گیرند. در این تحقیق درصدد ارزیابی قابلیت اطمینان، تبیین اعتبار تجاری، تبیین هزینه‌های عملیاتی و نیز تحلیل و بررسی خدمات مشتریان در زنجیره بلوکی جهت تقویت امنیت سایبری در صنعت بانکداری براساس شبکه عصبی مصنوعی هستیم.

* نویسنده مسئول- استادیار، گروه مهندسی صنایع، واحد ساری، دانشگاه آزاد اسلامی، ساری، ایران
** کارشناس ارشد، مدیریت فناوری اطلاعات، بانکدار بانک صادرات، تهران، ایران
*** استاد، دانشکده مهندسی صنایع، دانشکدگان فنی، دانشگاه تهران، تهران، ایران

ضرورت بررسی چنین موضوعی از این جهت است که گزینه‌های مرتبط با امنیت سایبری در صنعت بانکداری باید به صورت مداوم به‌روزرسانی شود و این موضوع درخصوص فناوری زنجیره بلوکی بیشتر مورد توجه می‌باشد، براین اساس مدلی مبتنی بر فناوری زنجیره بلوکی در صنعت بانکداری نیاز به ارایه بوده تا بتواند تقویت امنیت سایبری در این شبکه را نشان داده و آن را مورد ارزیابی قرار دهد. این مطالعه با سایر مطالعات همسو در این خصوص برخی تفاوت‌های اساسی دارد، یکی از این تفاوت‌ها به استفاده از رویکرد شبکه عصبی باز می‌گردد که در مطالعات مشابه فناوری زنجیره بلوکی برای امنیت سایبری دیده نشده است. نتایج حاصل از مدل پیشنهادی می‌تواند در سایر سازمان‌ها به صورت شبیه‌سازی مورد بهره‌برداری قرار گیرد، به عبارتی مؤسسات مالی اعتباری در سایر قلمروهای تحقیقاتی در این خصوص می‌توانند با بکارگیری روش و الگوی مدل‌سازی شده در این مطالعه به تقویت امنیت سایبری خود بپردازند. به عبارتی این مدل‌سازی می‌تواند به صورت مشابه و براساس متغیرهای به‌کار رفته در این مطالعه برای سایر سازمان‌ها نیز به‌کار برده شود. می‌توان بیان داشت پس از مدل‌سازی این مقاله می‌تواند یک قابلیت اطمینان برای سایر سازمان‌ها درخصوص مناسب‌بودن این رویکرد در تقویت امنیت سایبری ایجاد و آن‌ها را تشویق به استفاده از آن نماید. هدف اصلی این تحقیق ایجاد طراحی مدلی مبتنی بر فناوری زنجیره بلوکی برای تقویت امنیت سایبری در صنعت بانکداری می‌باشد. این مطالعه از دو منظر دارای جنبه‌های نوآوری می‌باشد. در گام اولیه مطالعات همسو موضوع امنیت شبکه‌های بانکداری را در قالب شبکه‌های عصبی مورد بررسی قرار نداده‌اند و این موضوع را مورد سنجش یا تعیین نتایج نهایی قرار نداده‌اند و از سوی دیگر موضوع به‌کارگیری فناوری زنجیره بلوکی برای تقویت امنیت سایبری در صنعت بانکداری مورد بررسی مطالعات پیش از این نبوده است و مطالعات خارجی و داخلی هر یک به بخشی از این موضوع اشاره کرده‌اند که این مورد از جنبه‌های نوآوری و جدیدبودن مطالعه حاضر در حوزه زنجیره بلوکی به‌شمار می‌رود.

۲- پیشینه تحقیق

اعتماد، شفافیت، آگاهی، امینت و حریم خصوصی از چالش‌های عصر دیجیتال است. فناوری بلاک‌چین با هدف مدیریت داده‌ها به صورت ایمن، شفاف و غیرمتمرکز ایجاد شده و می‌تواند راهکاری برای چنین چالش‌هایی باشد [۳]. در مقاله‌ای با توجه به توسعه و پیشرفت اینترنت‌اشیاء، پرداختن به امنیت توزیع‌شده برای آن، یک ضرورت دانسته شد [۴]. تحقیق دیگری بیانگر این موضوع است که اگرچه بلاک‌چین می‌تواند خود را به‌عنوان درمانی قطعی برای چالش‌های پیش روی حوزه امنیت و حفظ حریم خصوصی اینترنت‌اشیاء معرفی کند، اما تلاش‌های تحقیقاتی قابل توجهی باید به منظور انطباق الگوریتم‌های فشرده محاسباتی بلاک‌چین با محدودیت‌های سرسخت انرژی و پردازشی کامپیوترهای امروزی انجام شود [۱]. در مقاله‌ای بیان شد که بهبودهای مورد انتظار در ادغام اینترنت‌اشیاء در شهر هوشمند با بلاک‌چین عبارتند از؛ تمرکززدایی و مقیاس‌پذیری، مدیریت هویت، خودمختاری، قابلیت اطمینان، امنیت، بازار خدمات و ایمن‌سازی کدها [۵].

محققانی بررسی معماری‌های مبتنی بر بلاک‌چین و اینترنت‌اشیاء، مشکلات و موانع و روش‌های رفع آن مورد مطالعه قرار دادند. این مطالعه نشان داد که راه‌حل‌های اینترنت‌اشیاء مبتنی بر بلاک‌چین برای ساده‌سازی فرایندهای کسب و کار، بهبود تجربه مشتری و کاهش هزینه بسیار مناسب و قابل توجه هستند. لیکن علی‌رغم تمام مزایایی که بلاک‌چین دارد، این مدل بدون نقص نیست [۶]. این مطالعه نشان داد که فناوری بلاک‌چین در اینترنت‌اشیاء خصوصاً در جهت افزایش امنیت، هنوز در مرحله در حال ظهور است و با استفاده گسترده‌تر از پیشرفت‌های فناورانه، تحقیقاتی برای رسیدگی به خواسته‌های خاص، همراه با همکاری سازمان‌ها و دولت‌ها نیاز به پیشرفت دارد. در انتها به رویکرد حباب‌های اعتماد تأکید می‌شود که نشان‌دهنده توانایی آن در رفع نیازهای امنیتی مورد درخواست و همچنین تسریع در برابر حملات است [۷]. ۸ مؤلفه در ۵ سطح قرار گرفتند. الزامات قانونی و حقوقی از لحاظ خالص اثرگذاری (R-j) رتبه اول را دارد و الزامات تجاری رتبه آخر را دارد [۸]. مطالعه‌ای دیگر اثبات کرد که امنیت اینترنت‌اشیاء می‌تواند برای ساخت‌های بلاک‌چین در بانکداری مورد بهره‌برداری قرار گیرد [۲].

جدول ۱- متغیرهای نوآوری در مطالعات پیشین

ردیف	نام محقق	قابلیت اطمینان	هزینه‌های عملیاتی	اعتبار تجاری	هزینه‌های عملیاتی
۱	بازیار و همکاران (۱۳۹۹)	√			
۲	فقیه و همکاران (۱۳۹۹)	√	√		
۳	آهنی و همکاران (۱۳۹۹)				√
۴	زاهدی و همکاران (۱۳۹۸)			√	
۵	بختیاری و همکاران (۱۳۹۷)	√		√	
۶	نیک‌زاد و همکاران (۱۳۹۹)		√		
۷	صفویه و همکاران (۱۴۰۰)	√		√	

ردیف	نام محقق	قابلیت اطمینان	هزینه‌های عملیاتی	اعتبار تجاری	هزینه‌های عملیاتی
۸	گارپ[1] و همکاران (۲۰۲۱)	√			√
۹	وانگ و همکاران (۲۰۲۰)	√			
۱۰	عثمانی[2] و همکاران (۲۰۲۰)	√			
۱۱	ژو[3] و همکاران (۲۰۲۰)		√		
۱۲	نیک[4] و همکاران (۲۰۲۰)	√			
۱۳	انوار[5] و همکاران (۲۰۲۰)		√		
۱۴	مطالعه حاضر	√	√	√	√

تحقیقی نشان داد که بلاک‌چین در نهایت اعتبار تجاری در بانکداری را بهبود می‌دهد و در نهایت قابلیت کاربری بلاک‌چین برای سیستم بانکداری مفید خواهد بود [۱۰]. همچنین در مطالعه‌ای دیگر بلاک‌چین محافظت از داده‌های حریم خصوصی کاربران بانکی را بهبود می‌دهد و این موضوع سبب می‌شود که اعتبار تجاری بانک‌هایی که سیستم بلاک‌چین را به‌کار می‌گیرند بهبود یابد [۱۱]. نویسندگان اثبات کردند که بلاک‌چین سبب می‌شود که ارزیابی قابلیت اطمینان در سیستم بانکداری تجاری بهبود یابد [۱۲]. زمانی‌که سیستم بلاک‌چین مورد بهره‌برداری قرار می‌گرفت، ارزیابی مطالعه‌ای نشان داد که ماهیت غیرمتمرکز بلاک‌چین سبب می‌شود میزان نفوذ به یک زنجیره بلوکی غیرممکن گردد و این کار اشتراک‌گذاری داده‌های حساس بانکی را در بیرون ازشبکه حفاظت شده بانک ناممکن می‌سازد [۹]. همچنین بلاک‌چین می‌تواند خدمات مشتریان بانکی را تسهیل و همچنین حفاظت از حریم خصوصی داده‌های آن‌ها را افزایش دهد [۱۴]. هزینه‌های عملیاتی و هزینه‌های خدمات مشتریان زمانی که از یک شبکه بلاک‌چین استفاده می‌شد کاهش می‌یافت [۱۵]. با استفاده از بلاک‌چین در یک سیستم بانکداری باعث محافظت از داده‌های مالی کاربران می‌شود [۱۶].

یافته‌های مطالعه‌ای با عنوان "تأثیر بلاک‌چین در فرایندهای بانکی: مطالعه موردی Spunta بین بانکی" نشان داد که بلاک‌چین می‌تواند امنیت شبکه‌های بانکی را تأمین کند. همچنین بلاک‌چین می‌تواند از گزینه‌های مطرح درخصوص فرایندهای بانکی باشد. به عبارتی می‌توان در نظر گرفت که با استفاده از فناوری بلاک‌چین می‌توان امنیت سایبری در شبکه‌های بانکی را بهبود داد.

1. Garg
2. Osmani
3. XU
4. Niak
5. Anwar

۳- روش تحقیق

این تحقیق از نظر هدف کاربردی است. روش مورد استفاده به صورت شبکه عصبی مصنوعی می‌باشد. شبکه‌های عصبی مصنوعی[6] ابزارهایی مهم در میان مباحث هوش محاسباتی به حساب می‌آیند. برای این منظور از روش شبکه‌های عصبی پرسپترون[7] چند لایه استفاده خواهد شد. دسته‌ای از شبکه‌های عصبی مصنوعی پیشخور است. پرسپترون چند لایه یک کلاس از شبکه عصبی مصنوعی است. پرسپترون چند لایه‌ها به دلیل توانایی آنها در حل مشکلات تصادفی در تحقیقات مفید هستند، که اغلب راه‌حل‌های تقریبی را برای مشکلات بسیار پیچیده ارائه می‌دهند و می‌توانند حوزه‌های مختلف به طراحی یک مدل را پوشش دهند. در بخش اول پس از توصیف داده‌های تحقیق در بخش توصیف آماری داده‌ها اقدام به ارائه تجزیه و تحلیل ناشی از روش پرسپترون چند لایه می‌شود که در نرم‌افزار متلب صورت گرفت. در این بخش داده‌ها از دو دسته تشکیل می‌شوند، بخشی از داده‌ها مرتبط با پرسشنامه مطرح شده است که براساس طیف لیکرت اندازه‌گیری شده و براساس آن استخراج داده صورت گرفته و محاسبات پرسپترون چند لایه در یک شبکه عصبی مورد بررسی قرار گرفته است.

شبکه عصبی مصنوعی در واقع شبیه‌سازی دستگاه عصبی طبیعی است و شامل مجموعه‌ای از مهم‌ترین انواع شبکه‌های عصبی، شبکه‌های پرسپترون چند لایه (MLP) می‌باشد. این شبکه‌ها از چندین لایه تشکیل شده‌اند. در هر لایه تعدادی نرون در نظر گرفته می‌شود که به‌وسیله اتصالاتی به نرون‌های لایه‌های مجاور وصل می‌شوند. نرون‌های لایه اول، اطلاعات ورودی را گرفته و از طریق اتصالات مربوطه، به نرون‌های لایه مخفی منتقل می‌کنند. در این شبکه‌ها ورودی مؤثر هر نرون، حاصل ضرب خروجی نرون‌های لایه قبل در وزن‌های میان آن نرون‌ها می‌باشد (رابطه ۲).

$$Net_{pi} = \sum W_{ij} a_{pi} + b_i \qquad (۱)$$

در این رابطه، a_{pi}; مقدار خروجی لایه قبلی و w_{ij}; وزن‌های لایه مربوطه و میزان اریبی (Bias) می‌باشد. در واقع این رابطه یک رابطه خطی است. سپس مقدار F (netp) محاسبه می‌شود که F یک تابع محرک است. در لایه مخفی پس از محاسبه ورودی مؤثر در هر نرون، این ورودی از یک تابع محرک (Activation Function) گذرانده می‌شود. برای این کار، توابع محرک مختلفی ارائه شده است. گرایش بیشتر محققان به استفاده از توابع محرک کراندار می‌باشد.

برای یافتن شبکه عصبی با توپولوژی مناسب به کمک الگوریتم آموزشی و سنجش کارآیی مدل، معیارهای مختلفی وجود دارد که هدف همه آنها، کمینه‌شدن خطای مدل است. در این تحقیق از معیارهای ضریب تبیین و جذر میانگین مربعات خطا استفاده شده است.

6. Artificial Neural Network-ANN
7. Perceptron Neural Networks

$$R = \frac{\sum_{i=1}^{n}(obs - \overline{obs})(pre - \overline{pre})}{\sqrt{\sum_{i=1}^{n}(obs - \overline{obs})^2 \sum_{i=1}^{n}(pre - \overline{pre})^2}} \quad (۲)$$

$$RMSE = \sqrt{\sum_{i=1}^{n}(\frac{(obs - pre)}{n})} \quad (۳)$$

در این دو رابطه، تعداد داده‌های تحلیلی، $\overline{obs}$ و $\overline{pre}$ به ترتیب مقادیر مشاهده‌ای و پیش‌بینی‌شده، $\overline{obs}$ و pre به ترتیب میانگین مقادیر مشاهده‌ای و مقادیر پیش‌بینی شده در مدل و شبکه می‌باشد. در تحلیل مراحل مختلف برای مقایسه نتایج از این دو معیار استفاده شده است. همچنین جامعه آماری این تحقیق کلیه متخصصین و خبرگان در حوزه امنیت سایبری در فعالیت‌های بانکداری در بانک صادرات در شهر تهران می‌باشند که برابر با ۱۷۲ نفر بودند. برای تعیین نمونه آماری از روش نمونه‌گیری ساده تصادفی استفاده شد. نمونه آماری با توجه به فرمول کوکران برابر با ۱۱۹ نفر تعیین شده است.

روش تجزیه و تحلیل این مطالعه به صورت شبیه‌سازی شبکه عصبی است. علت انتخاب شبکه عصبی از این جهت است که این الگوریتم می‌تواند در فرایند بررسی داده‌های پژوهش قدرت یادگیری را به‌کار ببرد، یعنی این الگوریتم در هر دور محاسباتی که انجام می‌دهد سعی می‌کند سطوح مرتبط با خطای محاسباتی یا خطای آزمون را کاهش دهد و این موضوع یک برتری برای این الگوریتم نسبت به روش‌های مشابه ایجاد کرده است. از سوی دیگر شبکه عصبی در نهایت گزینه‌های قابل پیش‌بینی کنندگی را ارایه می‌دهد که این موضوع یک برتری نسبت به سایر روش‌ها در این حوزه می‌باشد.

۴- مدل شبیه‌سازی شده

مدل شبیه‌سازی در شبکه عصبی دارای سه بخش می‌باشد. یک بخش شامل متغیرهای پژوهش می‌باشد که به‌عنوان متغیرهای ورودی مورد تعریف قرار می‌گیرد. یک بخش شامل نرون‌های محاسباتی می‌باشد که براساس قواعد تعیین‌شده در فرایند محاسبات شبکه‌های عصبی تعداد نرون‌های واسط تولید می‌شوند و بخش نهایی شامل تابع متغیر هدف می‌باشد که براساس رسیدن به هدف نهایی که تقویت امنیت سایبری می‌باشد تعریف می‌شود. این موضوع در شکل (۱) نیز نشان داده شده است.

مدل شبیه‌سازی‌شده در این مقاله شامل ۴ متغیر می‌باشد. این مدل براساس متغیرهای پیشنهادشده به طراحی مدلی مبتنی بر فناوری زنجیره بلوکی برای تقویت امنیت سایبری در صنعت بانکداری پرداخت. این چهار متغیر شامل موارد زیر می‌باشد:

۱- ارزیابی قابلیت اطمینان.
۲- خدمات مشتریان.
۳- اعتبار تجاری.
۴- هزینه‌های عملیاتی.

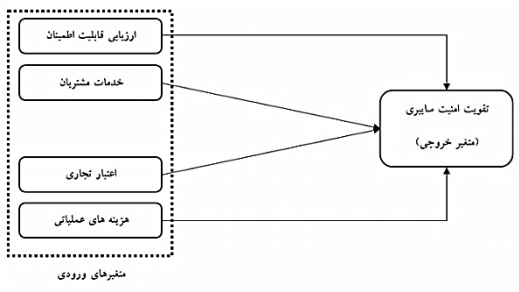
این مدل شبیه‌سازی براساس این چهار متغیر معرفی شده ساخته می‌شود و براساس آن شبکه عصبی پرسپترون به ساخت روابط ساختاری بین شبکه می‌پردازد. این مدل براساس ساخت شبکه عصبی ایجاد می‌شود. این مدل برگرفته از [۱۰،۱۲،۱۳،۹] می‌باشد. جدول (۲) نشان‌دهنده رفرنس و منبع مرتبط با هر یک از متغیرهای پژوهش می‌باشد.

جدول ۲- استناددهی متغیرهای پژوهش

ردیف	آماره‌های تخمینی	مطالعات استنادی
۱	ارزیابی قابلیت اطمینان	ژو و همکاران، ۲۰۲۰
۲	خدمات مشتریان	گارگ و همکاران، ۲۰۲۱
۳	اعتبار تجاری	عثمانی و همکاران، ۲۰۲۰
۴	هزینه‌های عملیاتی	رینک و بوشمن، ۲۰۲۰
۵	تقویت امنیت سایبری	رینک و بوشمن، ۲۰۲۰

علت انتخاب این متغیرها این بود که در مطالعات استنادی ارایه‌شده این مطالعات گزینه‌های مناسبی برای بررسی تقویت امنیت سایبری بود. به عبارتی مطالعات [۱۰،۱۲،۱۳،۹] نشان دادند که نتایج مرتبط با تقویت امنیت سایبری با متغیرهای ارایه‌شده در این مطالعه نتایج مناسب‌تری ارایه می‌دهد. به عبارتی این مطالعات استناد کردند که هزینه‌های عملیاتی، اعتبار تجاری، خدمات مشتریان و ارزیابی قابلیت اطمینان بهتر می‌توانند گزاره‌های مرتبط با تقویت امنیت سایبری را در یک شبیه‌سازی ارایه دهند. از منظر محاسباتی ارزیابی قابلیت اطمینان به تغییرات ایجادشده در تعداد خطاهای ناشی از تغییرات در پسماند داده‌ها نسبت به میانگین محاسباتی داده‌ها به‌دست می‌آید که مقادیری نزدیک به یک را در اکثر محاسبات ارایه می‌دهد. خدمات مشتریان نشان‌دهنده تغییرات در میزان کمیت و کیفیت ارایه‌شده خدمات از سوی مشتریان می‌باشد که به صورت نسبت خدمات ارایه‌شده در یک بازه زمانی مشخص نسبت به کل خدمات ارایه‌شده در یک سال مالی می‌باشد. اعتبار تجاری بیان می‌کند که به ازای هر تعداد مشخص از مشتریان چه نسبتی از رضایت‌مندی از برند شرکت ایجاد می‌شود و معمولاً مقادیری درصدی در محاسبات ضریب فنی را به خود اختصاص می‌دهد. هزینه‌های عملیاتی شامل همه هزینه‌های مرتبط با ایجاد محصول و فروش آن می‌باشد که شامل هزینه‌های بازاریابی، هزینه‌های تأمین مواد اولیه، هزینه‌های ارسال محصول و هزینه‌های انبارداری. تقویت امنیت سایبری شامل کلیه گزینه‌های مرتبط با امنیت می‌باشد. امنیت شامل کلیه کارکردهای مرتبط با دیواره‌های آتش و همچنین سرویسگرهای ابری می‌باشد که به صورت موازی به یکدیگر وصل می‌شوند و از ورود هر نوع داده اتفاقی با ماهیت حمله‌های هوشمند را جلوگیری می‌کند.

این مقالات نشان دادند که در یک مدل برای تقویت امنیت سایبری موضوع ارزیابی قابلیت اطمینان می‌تواند در طراحی مدل به‌کار گرفته شود. همچنین خدمات متشریان و اعتبار تجاری در این مطالعات برای یک مدل ساخته‌شده در جهت تقویت امنیت سایبری به‌کار گرفته شده است. علاوه بر این این مطالعات هزینه‌های عملیاتی نیز براساس طراحی مدل‌های مبتنی بر فناوری زنجیره بلوکی در ارتباط است و می‌توان در مدل به کار گرفته شود. مدل شبیه‌سازی شده در شبکه عصبی به صورت زیر می‌باشد:



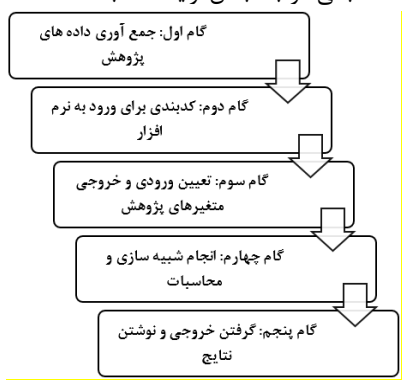
شکل ۱- مدل شبیه‌سازی شده شبکه عصبی ایجاد شده پرسپترون چند لایه برای زنجیره بلوکی

گام اولیه در شبیه‌سازی مدل پیشنهادی جمع‌آوری داده‌های پژوهش از قلمرو تحقیق بود. در این گام داده‌ها براساس پرسشنامه تنظیم‌شده براساس [۱۲،۹] تنظیم شده است. در این مرحله داده‌های مرتبط با متغیرهای پژوهش جمع‌آوری می‌شود و براساس متغیرهای ارایه‌شده در شکل (۱) جمع‌آوری گردید و در گام بعدی داده‌های گمشده و از دست رفته موجود در داده‌ها حذف شد.

در گام دوم: داده‌های مورد نیاز برای شبیه‌سازی به صورت کدبندی وارد نرم‌افزار می‌شود. در این مرحله برای هر یک از متغیرهای پژوهش داده‌های جمع‌آوری شده براساس پرسشنامه‌ها کدبندی و با طیف‌های ۱ تا ۵ در اختیار نرم‌افزار قرار می‌گیرد تا بتواند براساس آن داده‌های تحقیق را تقسیم‌بندی نمایند.

در گام سوم: با استفاده از داده‌های تحقیق متغیرهای مورد بررسی در پژوهش برای شبکه تعریف می‌شود و متغیرهای ورودی و هدف برای محاسبات شبکه عصبی ارایه شده است. این گام به صورت کلی شامل تعریف متغیرهای پژوهش به‌عنوان متغیرهای هدف و متغیرهای ورودی می‌باشد.

گام چهارم: در این گام براساس داده‌های ورودی تعیین‌شده محاسبات شبیه‌سازی در شبکه عصبی صورت می‌گیرد و خروجی ارایه می‌گردد. به عبارتی این مرحله شامل ارایه خروجی یک شبکه عصبی برای ارتباطات متغیرهای ارایه‌شده در گام‌های قبلی می‌باشد. در این مرحله که یک مرحله یادگیری و برآورد خطای محاسبات است به تعداد دورهای محاسباتی تعیین‌شده داده‌ها برای شبکه عصبی مورد تجزیه و تحلیل قرار می‌گیرد و در نهایت شبکه عصبی در حالتی ارایه می‌شود که کمترین سطح خطای محاسباتی مرتبط با آن ارایه شده باشد.



شکل ۲- فرایند انجام پژوهش

در شبیه‌سازی مدل ارایه‌شده از استنادات پژوهش استفاده شد. محققی استناد کرد که در مدل‌های تقویت امنیت سایبری برای مؤسسات مالی ارزیابی قابلیت اطمینان شبکه‌ای از اهمیت بالایی برخوردار است، یعنی انتظار بر این است که یک شبکه مناسب از منظر تقویت امنیت سایبری در مؤسسات مالی در صورتی بتواند کارکرد مناسبی را ارایه دهد که قابلیت اطمینان آن بالا باشد [۹]. پژوهشگرانی خدمات مشتریان را یک عامل مهم در تعیین سطح امنیت سایبری برای شبکه‌های رایانه‌ای دانستند که در مؤسسات مالی به‌کار برده می‌شوند. به عبارتی انتظار بر این است که با بهبود در سطح امنیت شبکه‌های امنیت سایبری سطح خدمات مشتریان را تقویت نمود [۱۲]. محققانی اعتبار تجاری را به‌عنوان یک ساختار مهم برای تقویت امنیت سایبری در نظر گرفتند. از منظر این محققین اعتبار تجاری براساس امنیت سایبری تعیین می‌شود و این امنیت سایبری است که تعیین می‌کند مشتریان بانک تا چه سطحی برای یک مؤسسه مالی یا بانک اعتبار تجاری قائل باشند [۱۳]. پژوهشگرانی هزینه‌های عملیاتی را موضوعی مهم برای ساخت یک شبکه ساختار امنیت سایبری برای شبیه‌سازی‌های شبکه عصبی می‌دانستند و آن را گزینه مهمی در این خصوص می‌دانستند. از منظر این محققین هزینه‌های عملیاتی یک گزینه مهم برای تعیین سطح امنیت سایبری در ساختار داده می‌باشند که می‌توانند به ساخت یک مدل شبیه‌سازی برای ارتقاء فناوری‌هایی مانند بلاک‌چین به‌کار گرفته شود [۱۰].

۵- یافته‌های تحقیق

در این مطالعه از پرسشنامه برگرفته از [۱۰،۱۲،۱۳،۹] استفاده شد این پرسشنامه شامل ۵ متغیر و ۳۰ گویه می‌باشد که برای هر یک از متغیرها تعداد ۶ سؤال در نظر گرفته شده بود و براساس کدبندی طیف لیکرت ۱ تا ۵ جمع‌آوری داده‌ها برای آن صورت می‌گیرد. پرسشنامه براساس نیازسنجی بانک‌ها برای امنیت سایبری و نقش فناوری بلاک‌چین در آن‌ها به گونه‌ای تنظیم شده است که بتواند نیازهای متخصصین را براساس گویه‌های ارایه‌شده مورد سنجش قرار دهد. این پرسشنامه در نهایت توانسته است داده‌های موردنیاز برای بررسی شبکه عصبی را ارایه دهد. در این مطالعه به دنبال پاسخ به این سؤال است که تقویت امنیت سایبری براساس فناوری‌های بلاک‌چین براساس معیارهای ارایه‌شده در مطالعه دارای قابلیت شبیه‌ساز می‌باشد؟ و همچنین به دنبال پاسخ به این سؤال می‌باشد که هر یک از متغیرهای ارایه‌شده در مدل شبیه‌سازی آیا گزینه مناسبی برای فناوری بلاک‌چین در قبال تقویت امنیت سایبری می‌باشد؟

در واقع این مطالعه به دنبال تأمین این هدف است که شبکه عصبی ارایه‌شده بتواند قابلیت‌های امنیت سایبری برای بانکداری را در یک فناوری شبکه بلاک‌چین مورد آزمایش و تعیین قرار دهد. همچنین به دنبال تأمین این هدف است که هر یک از متغیرها یا زیرفاکتورهای ارایه‌شده بتوانند در یک شبکه امنیت سایبری با فناوری بلاک‌چین دارای قابلیت اطمینان باشند. در شبیه‌سازی ارایه‌شده سعی می‌شود با

استفاده از محاسبات و ارایه قابلیت اطمینان و همچنین سطح خطای محاسباتی که به میانگین مربعات خطا معروف است به سؤالات پاسخ داده شود و اهداف تحقیق تأمین گردد.

مدل پرسپترون چند لایه براساس یک شبکه زنجیره عصبی که عملکردی مشابه با زنجیره بلوکی دارد مورد سنجش قرار گرفت. این مدل در مراحل محاسبات خود از چندین لایه تشکیل می‌شود و نورون‌های محاسباتی در فرایند تولید لایه‌ها اصول یادگیری را انجام می‌دهند که این نوع کارکرد مشابه کارکردهای مرتبط با زنجیره بلاکی می‌باشد. نتایج نشان‌دهنده دقت شبیه‌سازی پرسپترون چند لایه در شبکه زنجیره عصبی ارائه‌شده می‌باشد. دقت شبکه عصبی برابر با ۷۷/۶ درصد بود که معمولاً مقادیر بالای ۶۰ درصد را می‌توان مناسب برای شبیه‌سازی دانست. سطح دقت شبکه عصبی پرسپترون چند لایه در این حالت به پاسخ متخصصین بستگی دارد و براساس نمونه مورد بررسی ممکن است متفاوت باشد. همچنین تعداد نورون‌ها پنهان‌شده در لایه ۱ برابر ۹ نورون بود. هرچه تعداد نورون‌ها در لایه اول بیشتر باشد نشان می‌دهد که گزینه‌های انتقال داده پیام در مرحله یادگیری بیشتر می‌باشد و این به معنی پیچیده‌تر بودن فرایند انتقال داده در یک زنجیره بلوکی می‌باشد. تعداد نورون‌های پنهان به میزان نورون اولیه تعریف شده به‌عنوان ورودی داده بستگی دارد.

H0= نمی‌توان براساس شبکه عصبی مصنوعی امنیت سایبری را در صنعت بانکداری پیاده‌سازی کرد.

H1= می‌توان براساس شبکه عصبی مصنوعی امنیت سایبری را در صنعت بانکداری پیاده‌سازی کرد.

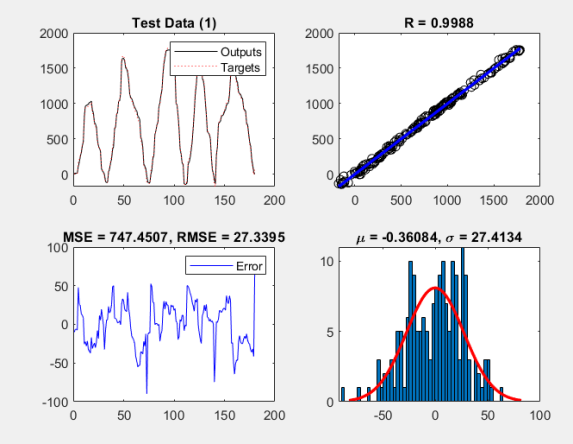
با توجه به یافته‌های پژوهش می‌توان گفت که توان مدلی مبتنی بر فناوری زنجیره بلوکی جهت تقویت امنیت سایبری در صنعت بانکداری براساس شبکه عصبی مصنوعی قابلیت پیاده‌سازی را خواهد داشت و این در این حالت دقت ارائه‌شده برای ساخت یک شبکه زنجیره بلوکی بیش از ۶۰ درصد بود. همچنین شبکه‌های عصبی ایجاد شده در زنجیره بلوکی از پیوند قوی برخوردار بودند و امکان شکستن آنها کم بود.

در گام بعد از شبیه‌سازی برای زنجیره بلوکی استفاده شد. معیار قضاوت در این حالت مقادیر خطای میانگین مربعات[1] بود، درصورتی‌که مقدار آن پس از انجام یادگیری بیش از مقدار اولی در کل داده‌ها بود نشان می‌دهد که زنجیره بلوکی تعریف شده براساس متغیر می‌تواند یک الگوی مناسب جهت بررسی زنجیره بلوکی باشد. در پاسخ به این سؤال می‌توان گفت با ایجاد یک شبکه شبیه‌سازی شده با پرسپترون چند لایه می‌توان یک مدل مبتنی بر فناوری زنجیره بلوکی را جهت تقویت امنیت سایبری در صنعت بانکداری ایجاد کرد، به شرط آنکه سطوح یادگیری ناشی از MLB برای امنیت سایبری مقادیر بالایی را گزارش نمایند.

H0= نمی‌توان یک مدل مبتنی بر فناوری زنجیره بلوکی را جهت تقویت امنیت سایبری در صنعت بانکداری ایجاد کرد.

H1= می‌توان یک مدل مبتنی بر فناوری زنجیره بلوکی را جهت تقویت امنیت سایبری در صنعت بانکداری ایجاد کرد.

شکل (۲) سطح رگرسیونی و همچنین نمودار توزیع نرمال داده‌ها برای اندازه‌گیری واریانس نشان داد. همچنین مقدار مجموع مجذور خطای محاسباتی[2] و کارایی خطای میانگین مربعات را نیز گزارش می‌کند. همچنین میزان همبستگی گزارش‌شده براساس شکل بالا برای داده‌های آزمون مشخص شده است.



شکل ۳- نتایج مرتبط با داده‌های آزمون

براساس شکل (۳) می‌توان جدول زیر را مرتبط با داده‌های مورد آزمون تنظیم کرد:

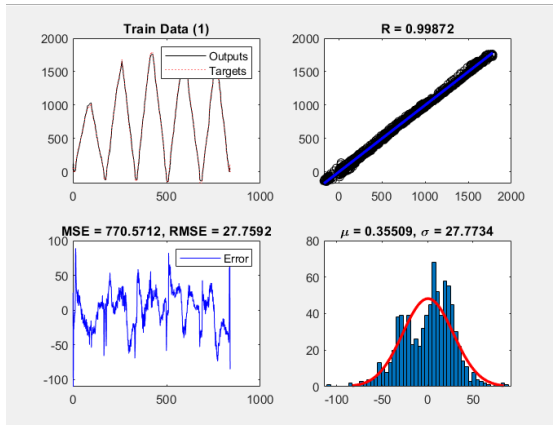
جدول ۳- نتایج مرتبط با آزمون داده‌های فناوری زنجیره بلوکی

ردیف	آماره‌های تخمینی	نماد متغیرها	مقدار عددی	P-Value
۱	همبستگی	R	۰/۹۹	۰/۰۰
۲	کارایی	MSE	۷۴۷/۴۵	
۳	مجموع مجذور خطای محاسباتی	RSME	۲۷/۳۳	
۴	واریانس	σ	۲۷/۴۱	
۵	میانگین مقادیر محاسباتی	μ	۰/۳۶	

براساس شکل (۳) می‌توان گفت که داده‌ها بعد از یادگیری به توزیع نرمال نزدیک‌تر شدند که این نشان می‌دهند فناوری زنجیره بلوکی توانایی ایجاد امنیت سایبری را خواهد داشت. همچنین سطح همبستگی و کارایی ارائه‌شده نیز گزارش شد. مهم‌ترین نکته در شکل (۳) می‌توان نزدیک‌شدن داده‌های تحقیق پس از یادگیری[3] داده به توزیع نرمال بود.

1. Mean Squared Error-MSE

2. Root-Mean-Square Error-RMSE
3. Train



شکل ۴- داده‌های یادگیری‌شده برای بررسی فناوری زنجیره بلوکی برای امنیت سایبری

براساس شکل (۳و۴) می‌توان جدول (۲) را تنظیم کرد. براساس جدول (۲) می‌توان گفت که کارایی مرتبط با فناوری‌های زنجیره بلوکی پس از یادگیری به سطح ۷۴۷/۴۵ واحد رسید، که نشان می‌دهد استفاده از روش پرسپترون چند لایه برای یادگیری روند فناوری زنجیره بلوکی می‌تواند به کارایی بیشتر برای امنیت سایبری منجر شود. همچنین مقدار واریانس برابر با ۲۷/۴۱ بود مقدار میانگین مقادیر محاسباتی برابر با ۰/۳۶ بود. همچنین همبستگی برابر با ۰/۹۹ بود. براساس شبیه‌سازی پرسپترون چند لایه می‌توان گفت که با ایجاد آزمون یادگیری در یک فناوری زنجیره بلوکی می‌توان انتظار داشت که سطح کارایی افزایش یابد.

H0= نمی‌توان قابلیت اطمینان در زنجیره بلوکی جهت تقویت امنیت سایبری در صنعت بانکداری در شبکه عصبی مصنوعی را به نتیجه قابل قبولی رساند.

H1= می‌توان قابلیت اطمینان در زنجیره بلوکی جهت تقویت امنیت سایبری در صنعت بانکداری در شبکه عصبی مصنوعی را به نتیجه قابل قبولی رساند.

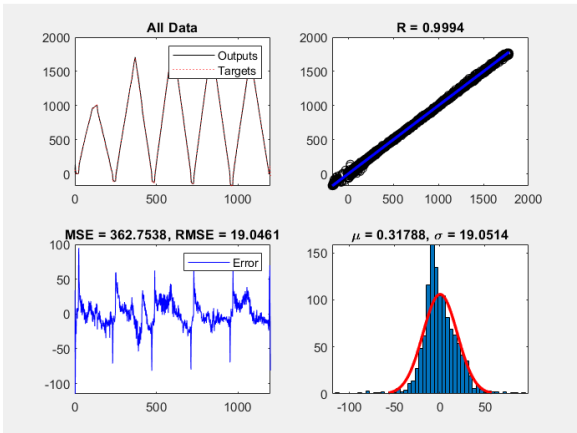
براساس جدول (۳) می‌توان دید که کارایی برابر با ۷۴۷ بود که پس از یادگیری توسط الگوریتم پرسپترون چند لایه این مقدار به ۷۷۰ رسید. به عبارتی می‌توان گفت که می‌توان مدلی مبتنی بر فناوری زنجیره بلوکی جهت تقویت امنیت سایبری در صنعت بانکداری براساس شبکه عصبی مصنوعی طراحی کرد، چرا که شبیه‌سازی در محیط نرم‌افزار متلب نشان داد که کارایی در فرایند یادگیری داده در یک شبکه پرسپترون چند لایه شبیه‌سازی شده با افزایش کارایی نسبت به داده‌های اولیه مواجه بوده است و همچنین داده‌ها به سطح داده‌های نرمال نزدیک شدند.

جدول ۴- نتایج مرتبط با آزمون داده‌های فناوری زنجیره بلوکی براساس الگوریتم یادگیری پرسپترون چند لایه

ردیف	نماد متغیرها	مقدار عددی	P-Value
۱	R	۰/۹۹	۰/۰۰
۲	MSE	۷۷۰/۵۷	
۳	RSME	۲۷/۷۵	
۴	σ	۲۷/۷۷	
۵	μ	۰/۳۵	

نتیجه تحلیل شبیه‌سازی پرسپترون چند لایه نشان می‌دهد که با استفاده از این شبیه‌سازها در یک زنجیره شبکه عصبی می‌توان قابلیت اطمینان در زنجیره بلوکی جهت تقویت امنیت سایبری در صنعت بانکداری در شبکه عصبی مصنوعی را به نتیجه قابل قبولی رساند، چرا که این شبکه در مسیر یادگیری سعی می‌کند در هر گام کارایی مرتبط با داده‌های به‌کار رفته را بهبود دهد و توانایی یادگیری خود از داده‌های مرتبط با یک زنجیره بلوکی را تقویت کند. براساس آنچه گفته شد.

براساس شکل (۵) می‌توان دید که داده‌ها در مرحله آغازین دارای همبستگی برابر با ۰/۹۹ برای قابلیت زنجیره بلوکی بودند. و همچنین میزان کارایی اولیه آنها برابر با ۳۶۲/۷۵ بود، به عبارتی کارایی این داده‌ها در گام اولیه در حد ۳۶۲/۷۵ بود. و واریانس آنها برابر با ۱۹/۰۵ بود. در گام بعد اعتبارسنجی[1] مرتبط با داده‌های تحقیق مورد بررسی قرار می‌گیرد. این اعتبار سنجی نشان می دهد که سطح کارایی[2] در چه سطحی خواهد بود. شکل (۵) نشان‌دهنده داده‌های پس از پایان یادگیری پرسپترون چند لایه و اعتبارسنجی بود. شکل (۴) نشان‌دهنده داده‌های به‌کار رفته در آزمون و وضعیت آماره‌های مرتبط با آن می‌باشد:



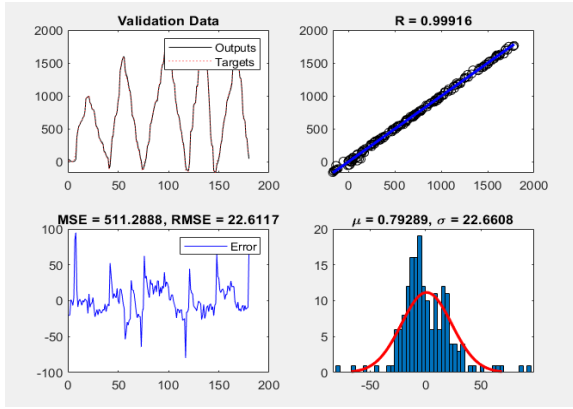
شکل ۵- وضعیت کل داده‌های بکار رفته در شروع شبیه‌سازی پرسپترون چند لایه برای بررسی قابلیت اطمینان در زنجیره بلوکی

H0= قابلیت اطمینان زنجیره بلوکی در یک فرایند تقویت امنیت سایبری در صنعت بانکداری در شبکه عصبی مصنوعی افزایش نمی‌یابد.

H1= قابلیت اطمینان زنجیره بلوکی در یک فرایند تقویت امنیت سایبری در صنعت بانکداری در شبکه عصبی مصنوعی افزایش می‌یابد.

براساس شکل (۶) می‌توان نشان داد که مقدار کارایی برابر با ۵۱۱/۲۸ و سطح واریانس برابر با ۲۲/۶۶ بود، همچنین همبستگی در اعتبارسنجی و پس از پایان یادگیری برابر با ۰/۹۹ بود. این موضوع نشان می‌دهد که با ایجاد یک زنجیره بلوکی در فرایند ایجاد امنیت سایبری می‌توان از آن برای صنعت بانکداری استفاده کرد.

1. Validation
2. MSE



شکل ۶- وضعیت کل داده‌های بکار رفته در شروع شبیه‌سازی پرسپترون چند لایه برای بررسی قابلیت اطمینان در زنجیره بلوکی

براساس جدول (۴) می‌توان دید که سطح کارایی در پایان شبیه‌سازی پرسپترون چند لایه برابر با ۵۱۱/۲۸ بود درحالیکه قبل از انجام شبیه‌سازی زنجیره بلوکی برابر با ۳۶۲/۷۵ بود. در تفسیر این موضوع می‌توان گفت که شبیه‌سازی با استفاده از پرسپترون چند لایه توانست قابلیت اطمینان زنجیره بلوکی در یک فرایند تقویت امنیت سایبری در صنعت بانکداری در شبکه عصبی مصنوعی افزایش دهد. برای بررسی این سؤال فرعی می‌توان داده‌های مرتبط با شبیه‌سازی پرسپترون چند لایه را مورد بررسی قرار داد که نشان می‌دهد اعتبار تجاری در یک زنجیره بلوکی جهت تقویت امنیت سایبری توانایی ایجاد جواب بهینه را دارد که براساس داده‌های اعتبارسنجی این موضوع روشن می‌شود.

H0= نمی‌توان وضعیت اعتبار تجاری در زنجیره بلوکی جهت تقویت امنیت سایبری را با استفاده از شبیه‌سازی پرسپترون چند لایه توان ایجاد کرد.

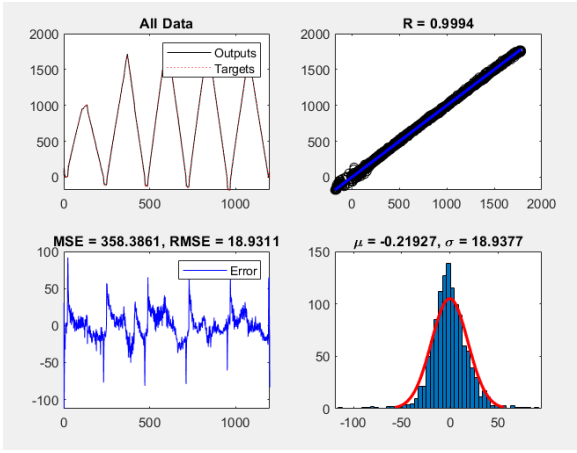
H1= می‌توان وضعیت اعتبار تجاری در زنجیره بلوکی جهت تقویت امنیت سایبری را با استفاده از شبیه‌سازی پرسپترون چند لایه توان ایجاد کرد.

شکل (۷) نشان‌دهنده کل داده‌های به‌کار رفته در آن می‌باشد. جدول (۶) همچنین نشان‌دهنده آماره‌های مرتبط با وضعیت کلی داده‌ها و همچنین وضعیت داده‌ها پس از اتمام شبیه‌سازی پرسپترون چند لایه بود.

جدول ۵- وضعیت قابلیت اطمینان زنجیره بلوکی

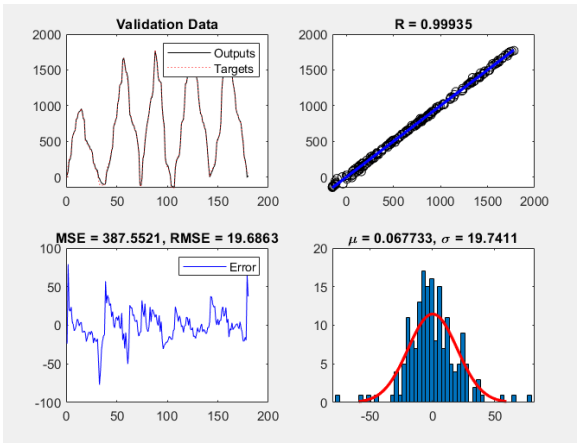
ردیف	نماد متغیرها	کل داده‌ها	اعتبارسنجی	P-Value
۱	R	۰/۹۹	۰/۹۹	۰/۰۰
۲	MSE	۳۶۲/۷۵	۵۱۱/۲۸	
۳	RSME	۱۹/۴	۲۲/۶۱	
۴	σ	۱۹/۰۵	۲۲/۶۶	
۵	μ	۰/۳۱	۰/۷۹	

براساس شکل (۶) می‌توان بیان داشت که اعتبار تجاری در زنجیره بلوکی جهت تقویت امنیت سایبری براساس کل داده‌ها دارای کارایی برابر با ۳۵۸/۳۸ بود و واریانس آن برابر با ۱۸/۹۳ بود. همچنین همبستگی کل داده‌ها ارائه‌شده برابر با ۰/۹۹ بود. شکل (۸) نشان‌دهنده وضعیت داده‌های اعتبارسنجی شده بود.



شکل ۷- اعتبار تجاری در زنجیره بلوکی جهت تقویت امنیت سایبری براساس کل داده

براساس شکل (۸) می‌توان بیان داشت که کارایی اعتبار تجاری در زنجیره بلوکی جهت تقویت امنیت سایبری بهبود یافته است و مقدار خطای میانگین مربعات به ۳۸۷/۵۵ رسیده است، همچنین سطح همبستگی برابر با ۰/۹۹ بود علاوه بر این مقدار واریانس برابر با ۱۹/۷۴ بود. در تفسیر شکل (۸) باید گفت که مقدار خطای میانگین مربعات پس از اعتبارسنجی داده‌های مرتبط با اعتبار تجاری در زنجیره بلوکی بهبود یافته است و این داده‌ها در سطح بهتری قرار دارند. به عبارتی با ایجاد یک شبیه‌سازی پرسپترون چند لایه برای بررسی اعتبار تجاری در زنجیره بلوکی جهت تقویت امنیت سایبری می‌توان این قابلیت اطمینان را ارائه داد که اعتبار تجاری در زنجیره بلوکی جهت تقویت امنیت سایبری برای بانکداری امکان‌پذیر است.



شکل ۸- اعتبار تجاری در زنجیره بلوکی جهت تقویت امنیت سایبری براساس داده‌های اعتبارسنجی شده

براساس جدول (۶) می‌توان بیان داشت که سطح خطای میانگین مربعات برابر با ۳۸۷/۵۵ بود، به عبارتی سطح کارایی نسبت به کل داده‌های تحقیق در سطح بالاتری قرار داشت و این نتایج نشان می‌دهد که شبیه‌سازی پرسپترون چند لایه توانایی بهبود وضعیت اعتبار تجاری در زنجیره بلوکی جهت تقویت امنیت سایبری را ایجاد خواهد کرد.

H0= سطح کارایی مرتبط با هزینه‌های عملیاتی در زنجیره بلوکی از سطح اولیه بیشتر نمی‌شود.

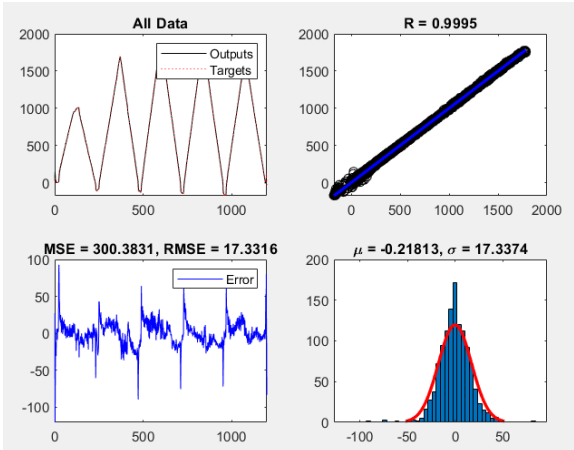
H1= سطح کارایی مرتبط با هزینه‌های عملیاتی در زنجیره بلوکی از سطح اولیه بیشتر می‌شود.

مطابق یافته‌های مقاله با استفاده از شبیه‌سازی پرسپترون چند لایه هزینه‌های عملیاتی در زنجیره بلوکی جهت تقویت امنیت سایبری در حوزه فعالیت بانکداری بهینه می‌شود. این حالت بهینگی براساس مقادیر مرتبط با خطای میانگین مربعات در محاسبات اعتبارسنجی ایجاد می‌شود و نشان می‌دهد با ایجاد فرایند یادگیری در یک شبکه پرسپترون چند لایه که منجر به بهبود زنجیره بلوکی می‌شود می‌توان بیان داشت که هزینه‌های عملیاتی در زنجیره بلوکی جهت تقویت امنیت سایبری در حوزه فعالیت بانکداری بهینه می‌شود. شکل (۹) دهنده کل داده‌های مرتبط با محاسبات پرسپترون چند لایه و شکل (۱۰) نشان‌دهنده اعتبارسنجی مرتبط با هزینه‌های عملیاتی است.

جدول ۶- وضعیت پارامترهای ارائه‌شده برای کل داده و داده‌های اعتبارسنجی‌شده

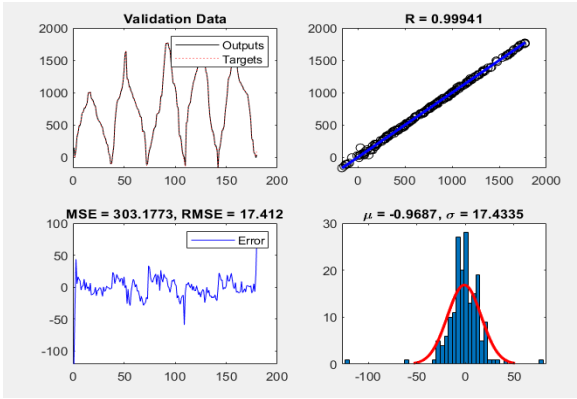
ردیف	نماد متغیرها	کل داده‌ها	اعتبارسنجی	P-Value
۱	R	۰/۹۹	۰/۹۹	۰.۰۰
۲	MSE	۳۵۸/۳۸	۳۸۷/۵۵	
۳	RSME	۱۸/۹۳	۱۹/۶۸	
۴	σ	۱۸/۹۳	۱۹/۷۴	
۵	μ	۰/۲۱	۰/۰۶	

براساس شکل (۹) می‌توان گفت که مقدار خطای میانگین مربعات برابر با ۳۰۰/۳۸ بود و سطح واریانس برابر با ۱۷/۳۳ بود. همچنین همبستگی در سطح ۰/۹۹ قرار داشت. علاوه بر این داده‌های مورد استفاده از ماهیت نرمالی برخوردار بودند و به شکل زنگوله‌ای نزدیک بودند و میانگین ارائه‌شده برابر با ۰/۲ بود. شکل (۹) نشان‌دهنده پارامترهای مرتبط با هزینه عملیاتی بعد از اعتبارسنجی داده‌های تحقیق بود.



شکل ۹- بررسی کل داده‌های هزینه‌های عملیاتی در زنجیره بلوکی

براساس شکل (۱۰) می‌توان نشان داد که مقدار خطای میانگین مربعات داده‌های اعتبارسنجی شده برابر با ۳۰۳/۱۷ بود و همچنین مقدار همبستگی برابر با ۰/۹۹ شد، علاوه بر این واریانس برابر با ۱۷/۴۳ بود. یافته‌های حاصل از شبیه‌سازی پرسپترون چند لایه در مسیر یادگیری در زنجیره بلوکی نشان داد که پس از انجام مراحل یادگیری مقدار خطای میانگین مربعات یا کارایی سیستم برای بررسی هزینه‌های عملیاتی افزایش یافته است و از عدد ۳۰۰/۳۸ به عدد ۳۰۳/۱۷ رسید. جدول (۶) نشان‌دهنده مقایسات بین پارامترهای کل داده‌ها و داده‌های اعتبارسنجی پس از یادگیری پرسپترون چند لایه در یک زنجیره بلوکی می‌باشد.



شکل ۱۰- داده‌های اعتبارسنجی‌شده مرتبط با هزینه‌های عملیاتی در زنجیره بلوکی

براساس جدول (۷) می‌توان دید که سطح کارایی مرتبط با هزینه‌های عملیاتی در زنجیره بلوکی پس از شبیه‌سازی و یادگیری در پرسپترون چند لایه بالاتر از سطح اولیه آن بود. با ایجاد یک شبکه زنجیره بلوکی براساس محاسبات پرسپترون چند لایه می‌توان هزینه‌های عملیاتی در زنجیره بلوکی را بهبود داد چرا که معیار مرتبط با کارایی خطای میانگین مربعات در مرحله اعتبارسنجی در سطح بیشتر از سطح اولیه قرار داشت. به عبارتی هزینه‌های عملیاتی در زنجیره بلوکی جهت تقویت امنیت سایبری در حوزه فعالیت بانکداری قابل استفاده است. همچنین برای آزمون از روش یادگیری الگو استفاده شد. در این روش داده‌های آزمون مورد بررسی قرار گرفتند.

جدول ۷- هزینه‌های عملیاتی در زنجیره بلوکی براساس پرسپترون چند لایه در کل داده‌ها و داده‌های اعتبارسنجی‌شده

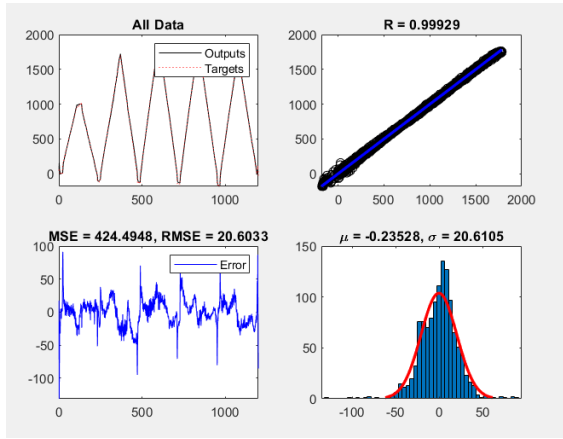
ردیف	نماد متغیرها	کل داده‌ها	اعتبارسنجی	P-Value
۱	R	۰/۹۹	۰/۹۹	۰/۰۰
۲	MSE	۳۰۰/۳۸	۳۰۳/۱۷	
۳	RSME	۱۷/۳۳	۱۷/۴۱	
۴	σ	۱۷/۳۳	۱۷/۴۳	
۵	μ	۰/۲۱	۰/۹۶	

H0= سطح کارایی مرتبط با خدمات مشتریان در زنجیره بلوکی پس از شبیه‌سازی افزایش نمی‌یابد.

H1= سطح کارایی مرتبط با خدمات مشتریان در زنجیره بلوکی پس از شبیه‌سازی افزایش می‌یابد.

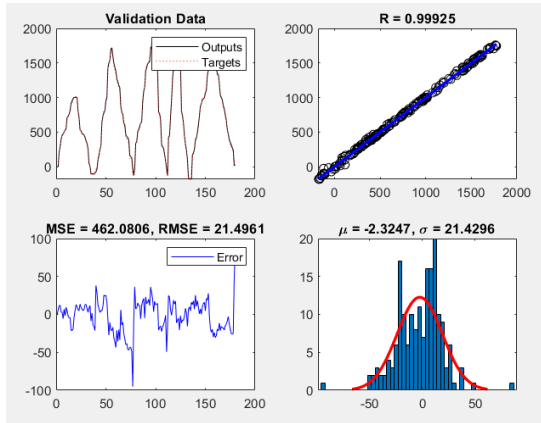
براساس شکل (۱۰) می‌توان نشان داد که مقدار کارایی محاسبه‌شده برای خدمات مشتریان در کل داده‌های تحقیق و پیش از شروع الگوریتم

یادگیری برابر با ۴۲۴ بود. مقدار واریانس برابر با ۲۰/۱۶ گزارش شده و میانگین برابر با ۰/۲۳ بود. در گام بعد پارامترهای حاصل از اعتبارسنجی داده‌ها در شبیه‌سازی روش یادگیری الگو[1] بررسی می‌شود. شکل (۱۰) نشان‌دهنده خدمات مشتریان در زنجیره بلوکی در کل داده‌های تحقیق در یک الگوی یادگیری پس از پایان یادگیری بود. شکل (۱۰) نشان‌دهنده وضعیت پارامترهای خدمات مشتریان در قبال کل داده‌های تحقیق است.



شکل ۱۱- خدمات مشتریان در زنجیره بلوکی در کل داده‌های تحقیق در یک الگوی یادگیری

براساس شکل (۱۱) می‌توان گفت که خدمات مشتریان در زنجیره بلوکی در اعتبارسنجی داده‌های تحقیق در یک الگوی یادگیری از کارایی کافی جهت تقویت امنیت سایبری در حوزه فعالیت بانکداری برخوردار است. علت این امر مقادیر مرتبط با خطای میانگین مربعات می‌باشد که در داده‌های اعتبارسنجی‌شده برابر با ۴۶۲/۰۸ بود، که نشان داد سطح داده‌های اعتبارسنجی مرتبط با خدمات مشتریان در زنجیره بلوکی از کارایی بیشتری پس از شبیه‌سازی روش یادگیری الگو برخوردار است. براساس این موضوع می‌توان جدول زیر را رسم کرد.



شکل ۱۲- خدمات مشتریان در زنجیره بلوکی در اعتبارسنجی داده‌های تحقیق در یک الگوی یادگیری

1. Learning Pattern Method-LPM

براساس جدول (۸) می‌توان دید که سطح کارایی مرتبط با خدمات مشتریان در زنجیره بلوکی پس از شبیه‌سازی و یادگیری در پرسپترون چند لایه بالاتر از سطح اولیه آن بود. در تفسیر این موضوع می‌توان گفت که با ایجاد یک شبکه زنجیره بلوکی براساس محاسبات پرسپترون چند لایه می‌توان خدمات مشتریان در زنجیره بلوکی را بهبود داد چرا که معیار مرتبط با کارایی خطای میانگین مربعات در مرحله اعتبارسنجی که پس از یادگیری قرار دارد در سطح بیشتر از سطح اولیه قرار داشت. به عبارتی خدمات مشتریان در زنجیره بلوکی جهت تقویت امنیت سایبری در حوزه فعالیت بانکداری قابل استفاده است، چرا که سطح کارایی مرتبط با خدمات مشتریان در پایان یادگیری پرسپترون چند لایه برابر با ۴۶۲/۰۸ بود که نسبت به مقدار اولیه آن برای کل داده‌ها از سطح بالاتری برخوردار بود.

جدول ۸- خدمات مشتریان در زنجیره بلوکی براساس پرسپترون چند لایه در کل داده‌ها و داده‌های اعتبارسنجی‌شده

ردیف	نماد متغیرها	کل داده‌ها	اعتبارسنجی	P-Value
۱	R	۰/۹۹	۰/۹۹	۰/۰۰
۲	MSE	۴۲۴/۴۹	۴۶۲/۰۸	
۳	RSME	۲۰/۶۰	۲۱/۴۹	
۴	σ	۲۰/۶۱	۲۱/۴۲	
۵	μ	۰/۲۳	۲/۳۲	

۶- نتیجه‌گیری

براساس مدل طراحی‌شده در شبکه عصبی می‌توان این یافته را بیان داشت که زنجیره بلوکی جهت تقویت امنیت سایبری در صنعت بانکداری براساس شبکه عصبی مصنوعی قابلیت بهره‌برداری دارد. برای این منظور شبکه امنیت سایبری باید از چهار عنصر تشکیل شود. این چهار عنصر عبارتند از ارزیابی قابلیت اطمینان شبکه، خدمات مشتریان، اعتبار تجاری و هزینه‌های عملیاتی. براین اساس یک ساختار فناوری بلاک‌چین جهت طراحی مدل با قابلیت اطمینان بالا که بتواند زنجیره بلاکی را تکمیل نماید باید براساس این مؤلفه‌ها تکمیل گردد. به عبارتی یک فناوری بلاک‌چین در شبکه بانکی می‌تواند براساس این چهار متغیر به یک امنیت سایبری با قابلیت اطمینان بالا منجر شود. این موضوع در یافته‌های این پژوهش مورد تأیید قرار گرفت. به عبارتی زمان ساخت شبکه‌های امنیت سایبری در بانکداری باید براساس مؤلفه‌های یادشده فناوری بلاک‌چین را برنامه‌ریزی کرد. این کار معمولاً با ایجاد واحدهای سخت‌افزاری مخصوص در فرایند ساخت شبکه‌های امنیتی ایجاد می‌گردد. این سخت‌افزارهای نصبی باید این قابلیت را داشته باشند که هزینه‌های عملیاتی را محاسبه نمایند، باید بتوانند قابلیت اطمینان سیستم را به صورت مداوم ارزیابی نمایند، باید بتوانند اعتبار تجاری ایجاد کنند و باید بتوانند هزینه‌های عملیاتی را اندازه‌گیری نمایند.

با استفاده از شبیه‌سازی پرسپترون چند لایه هزینه‌های عملیاتی در زنجیره بلوکی جهت تقویت امنیت سایبری در حوزه فعالیت بانکداری بهینه

می‌شود. مقدار خطای میانگین مربعات برابر با ۳۰۰/۳۸ بود و سطح واریانس برابر با ۱۷/۳۳ بود که این مقادیر نشان از سطح مناسب بهینگی امنیت سایبری می‌باشند. همچنین همبستگی در سطح ۰/۹۹ قرار داشت که نشان می‌دهد ارزیابی قابلیت اطمینان از موفقیت برخوردار بود. خدمات مشتریان در زنجیره بلوکی در اعتبارسنجی داده‌های تحقیق در یک الگوی یادگیری از کارایی کافی جهت تقویت امنیت سایبری در حوزه فعالیت بانکداری برخوردار است. علت این امر مقادیر مرتبط با خطای میانگین مربعات می‌باشد که در داده‌های اعتبارسنجی‌شده برابر با ۴۶۲/۰۸ بود، که نشان داد سطح داده‌های اعتبارسنجی مرتبط با خدمات مشتریان در زنجیره بلوکی از کارایی برخوردار است معمولاً مقادیر نزدیک به ۳ براساس [۱۱] برای این موضوع کفایت می‌کند که مقدار اعتبارسنجی در داده‌های این تحقیق بسیار بیشتر بود. سطح کارایی مرتبط با خدمات مشتریان در زنجیره بلوکی پس از شبیه‌سازی و یادگیری در پرسپترون چند لایه بالاتر از سطح اولیه آن بود. در تفسیر این موضوع می‌توان گفت که با ایجاد یک شبکه زنجیره بلوکی براساس محاسبات پرسپترون چند لایه می‌توان خدمات مشتریان در زنجیره بلوکی را بهبود داد چرا که معیار مرتبط با کارایی خطای میانگین مربعات در مرحله اعتبارسنجی که پس از یادگیری قرار دارد در سطح بیشتر از سطح اولیه قرار داشت. به عبارتی خدمات مشتریان در زنجیره بلوکی جهت تقویت امنیت سایبری در حوزه فعالیت بانکداری قابل استفاده است، چرا که سطح کارایی مرتبط با خدمات مشتریان در پایان یادگیری پرسپترون چند لایه برابر با ۴۶۲/۰۸ بود که نسبت به مقدار اولیه آن برای کل داده‌ها از سطح بالاتری برخوردار بود. براساس یافته‌های تحقیق می‌توان پیشنهاد کرد که سازمان‌های با عملکرد درخصوص امنیت سایبری در حوزه‌های مالی خدمات مشتریان را تحت دیواره‌های امنیتی بلاک‌چین مورد پوشش قرار دهند. همچنین پیشنهاد می‌شود که هزینه‌های عملیاتی مرتبط با کارکردهای ارایه خدمات به مشتریان براساس دیواره‌های آتش طراحی شده در فناوری بلاک‌چین به بهره‌برداری برسد. علاوه بر این برای تقویت امنیت شبکه‌های مالی در ساختار بانکی می‌تواند از گزاره‌های مرتبط با خطای سطح محاسباتی در زنجیره بلاک‌چین بهره برد و آن را به سایر شبکه‌های مالی در سازمان‌های بانکی نیز تعمیم داد. براساس یافته‌های پژوهش می‌توان برخی پیشنهادات برای پژوهش‌های آینده ارا ارایه داد می‌توان برای تحقیقات آتی این پیشنهاد را داد که بررسی تأمین امنیت برای بلاک‌چین در ساختارهای بانکداری آنلاین مورد بررسی قرار گیرد. همچنین می‌توان به محققین پیشنهاد داد که درخصوص اثرگذاری اینترنت‌اشیاء بر بهبود فناوری بلاک‌چین در ساختار امنیت بانکداری مورد بررسی قرار گیرد. علاوه بر این می‌توان اینترنت‌اشیاء و هوشمندسازی شبکه بانکی براساس فناوری بلاک‌چین مورد بررسی قرار گیرد.

۷- مراجع

۱- آهنی جان، سارا، صدوقی‌وش، مسعود. مطالعه و بررسی راهکارهای تأمین امنیت در فناوری بلاک‌چین، چهارمین کنفرانس ملی دانش و فناوری مهندسی برق کامپیوتر و مکانیک ایران، ۱۳۹۹.

۲- صفویه، الهام سادات و سیادتی، سامان، ارائه مدلی جهت بهبود امنیت اینترنت‌اشیاء با استفاده از زیرساخت بلاک‌چین (مطالعه موردی: در بانک ملت)، اولین کنفرانس بین‌المللی جهش علوم مدیریت، اقتصاد و حسابداری، ساری، ۱۴۰۰.

۳- بازیار، مصطفی. بررسی رابطه بین اکوسیستم کسب وکاری دیجیتال و فناوری بلاک‌چین (بررسی موردی بلاک‌چین مجوزدار هایپرلجر)، دومین کنفرانس بین‌المللی و ملی مطالعات مدیریت، حسابداری و حقوق، ۱۳۹۹.

۴- فقیه‌نیا، محمدعلی، رهسپارفرد، خیراله، فرجامی، یعقوب. امن‌سازی شبکه نامتمرکز اشیاء با بلاک‌چین (مطالعه موردی: خانه هوشمند)، سومین کنفرانس بین‌المللی فناوری‌های نوآورانه در زمینه علوم، مهندسی و تکنولوژی، ۱۳۹۹.

۵- قمری، فاطمه، شیدائیان، حامد. بکارگیری فناوری بلاک‌چین و اینترنت‌اشیاء در شهر هوشمند، چهارمین کنفرانس ملی دانش و فناوری مهندسی برق کامپیوتر و مکانیک ایران، ۱۳۹۹.

۶- زاهدی، فاطمه، ظروفی، محسن، ورمزیار، علی. بررسی معماری‌های مبتنی بر بلاک‌چین و اینترنت‌اشیاء / مشکلات و موانع و روش‌های رفع آن، نخستین کنفرانس بین‌المللی شهر هوشمند چالش‌ها و راهبردها، ۱۳۹۸.

۷- بختیاری، سعید، کشمیری، امیرحسین. بررسی فناوری بلاک‌چین در بهبود امنیت اینترنت‌اشیاء، ششمین کنگره بین‌المللی توسعه و ترویج علوم و فنون بنیادین در جامعه، ۱۳۹۷.

۸- نیک‌زاد خسمخی، بابک، پورنصیررودبنه، مریم، خدادادحسینی، سیدحمید. ارائه یک مدل برای تأمین امنیت مبتنی بر بلاک‌چین در بانکداری دیجیتالی (مطالعه موردی: بانک ملی ایران)، پنجمین کنفرانس ملی مهندسی کامپیوتر و بلاک‌چین ایران، ۱۳۹۹.

9- Xu, Z., Wang, Q., Wang, Z., Liu, D., Xiang, Y., & Wen, S. PPM: A Provenance-Provided Data Sharing Model for Open Banking via Blockchain. In Proceedings of the Australasian Computer Science Week Multiconference, 2020, (pp. 1-8).

10- Garg, P., Gupta, B., Chauhan, A. K., Sivarajah, U., Gupta, S., & Modgil, S. Measuring the perceived benefits of implementing blockchain technology in the banking sector. Technological Forecasting and Social Change, 120407. 2021.

11- Wang, H., Ma, S., Dai, H. N., & Imran, M. Blockchain-based data privacy management with nudge theory in open banking. Future Generation Computer Systems, 110, 2020, 812-823.

12- Osmani, M., El- Haddadeh, R., Hindi, N., Janssen, M., & Weerakkody, V. Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis. Journal of Enterprise Information Management. 2020.

13- Rajnak, V., & Puschmann, T. The impact of blockchain on business models in banking. Information Systems and e-Business Management, 2020. 1-53.

14- Naik, V., Pejawar, R., Singh, R., Aher, A., & Kanchan, S. Expeditious banking using Blockchain Technology. International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE), 2020, (pp. 1-6). IEEE.

15- Avasthi, A. A. Online Economy on the Move: The Future of Blockchain in the Modern Banking System. In International Conference on Innovative Computing and Communications, 2020, (pp. 129-145). Springer, Singapore

16- Anwar, S., & Yadav, A. Framework for Banking & Financial Sector Through Artificial Intelligence and Blockchain Technology. (In respect to Middle East). Solid State Technology, 63(6), 2020, 6321-6328.

17- Cucari, N., Lagasio, V., Lia, G., & Torriero, C. (2022). The impact of blockchain in banking processes: the Interbank Spunta case study. Technology Analysis & Strategic Management, 34(2), 138-150.