مطالعات علوم کاربردی در مهندسی

دوره ۱۰، شماره ۴، زمستان ۱۴۰۳

صفحات ۱۴۵-۱۲۸

Online ISSN: ۲۴۷۶-۴۵۰۷

Print ISSN: ۲۵۳۸-۲۰۵۵

www.irijournals.com

نقش هوش مصنوعی درتوسعه ی امنیت داده های شبکه بانکی کشور

حمیدغفاری[۱]، سعیدروحی شالمایی[۲]

[۱] دانشجوی دکتری علم اطلاعات ومدیریت دانش، پردیس بین المللی کیش، دانشگاه تهران، تهران، ایران

[۲] دکتری علم اطلاعات ومدیریت دانش، پردیس بین المللی کیش، دانشگاه تهران، تهران، ایران

چکیده

هدف از پژوهش حاضر بررسی نقش هوش مصنوعی درتوسعه ی امنیت داده های شبکه بانکی کشور بود. روش پژوهش حاضر توصیفی- تحلیلی بوده و دارای ماهیت کاربردی می باشد. جامعه آماری پژوهش حاضر را کارشناسان و خبرگان بانک‌های استان تهران تشکیل دادند. حجم نمونه اشباع نظری صورت گرفت. جهت گردآوری اطلاعات از روش میدانی و ابزار مصاحبه استفاده گردید. داده های بدست آمده به روش کیفی در محیط نرم افزاری مکس‌کیودا مورد تجزیه و تحلیل قرار گرفتند. یافته ها نشان داد که ۲۰ مضمون در قالب ۱۰ عامل به عنوان نقش هوش مصنوعی در توسعه ی امنیت داده های شبکه بانکی کشور شناسایی شدند که عبارت بودند از: (تحلیل داده‌های بزرگ، تشخیص تقلب، پیش‌بینی تهدیدات، بهبود فرآیندهای احراز هویت، مدیریت ریسک، پاسخگویی به تهدیدات، آموزش و فرهنگ‌سازی، تحلیل رفتارمشتری، مدیریت و نظارت بر سیستم‌ها، توسعه فناوری‌های نوین). بر این اساس می توان نتیجه گرفت با در نظرگرفتن مولفه های فوق به بهبود امنیت داده‌های شبکه بانکی کشور کمک کرد و به کاهش خطرات امنیتی و افزایش اعتماد مشتریان کمک نمود.

کلمات کلیدی: هوش مصنوعی، امنیت داده، شبکه بانکی

- مقدمه

در دنیای امروز، فناوری اطلاعات و ارتباطات به یکی از ارکان اساسی در تمامی حوزه‌ها، به ویژه در بخش مالی و بانکی تبدیل شده است. امنیت داده‌ها، به‌خصوص در شبکه‌های بانکی، به دلیل ماهیت حساس اطلاعات مالی و خصوصی مشتریان، از اهمیت بالایی برخوردار است. در این میان، هوش مصنوعی به‌عنوان یک ابزار نوآورانه در شناسایی و مقابله با تهدیدات امنیتی، به‌ویژه در بانک‌ها و مؤسسات مالی، عملکردی حیاتی دارد (براینیولفسون و مکافی[1]، ۲۰۱۴).

هوش مصنوعی با توانایی پردازش حجم بالای داده‌ها، شناسایی الگوها و رفتارهای مشکوک، و ارائه تحلیل‌های پیش‌بینی‌کننده، می‌تواند به مدیریت ریسک و بهبود استراتژی‌های امنیتی کمک شایانی نماید. سیستم‌های مبتنی بر هوش مصنوعی قادرند به‌سرعت به تهدیدات جدید واکنش نشان دهند و با یادگیری ماشینی، به‌طور مستمر بهبود یابند (هلینگ[2]، ۲۰۱۹).

با توجه به رشد روزافزون جرایم سایبری و حملات هکری، استفاده از تکنیک‌های هوش مصنوعی می‌تواند به بانک‌ها در تشخیص زودهنگام تهدیدات و به حداقل رساندن خسارات ناشی از آن‌ها کمک کند. علاوه بر این، هوش مصنوعی می‌تواند به تحلیل رفتار مشتریان و شناسایی فعالیت‌های غیرعادی بپردازد که به شناسایی کلاهبرداری و سوءاستفاده‌های مالی کمک می‌کند (بلانچ[3] و همکاران، ۲۰۱۹).

در این پژوهش، به بررسی نقش هوش مصنوعی در توسعه امنیت داده‌های شبکه بانکی کشور پرداخته خواهد شد. هدف این است که نشان دهیم چگونه این فناوری می‌تواند به‌عنوان یک راه‌حل موثر در افزایش امنیت داده‌های بانکی عمل نماید و چالش‌ها و فرصت‌های آن را مورد تحلیل قرار دهیم. باتوجه به اهمیت این موضوع درعصردیجیتال، نتایج این پژوهش می‌تواندبه بهبود استراتژی‌های امنیتی در بانک‌ها و افزایش اعتماد مشتریان به خدمات مالی کمک نماید.

- مرور ادبیات تحقیق

استفاده از هوش مصنوعی در بخش بانکی

هوش مصنوعی یک اصطلاح جامع است که شامل مجموعه‌ای از تکنیک‌ها و روش‌ها می‌شود که هدف آن‌ها بازتولید قابلیت‌های پیچیده‌ای مانند تصمیم‌گیری خودکار و استفاده از زبان است. یادگیری ماشین یک زیرمجموعه از هوش مصنوعی است که به کشف الگوها در داده‌ها و اتخاذ تصمیمات مناسب می‌پردازد. یادگیری ماشین به دو دسته یادگیری تحت نظارت و یادگیری بدون نظارت تقسیم می‌شود، بسته به این که آیا سیستم به‌طور صریح پاسخ‌های صحیح را دریافت می‌کند یا نه. یادگیری عمیق از شبکه‌های عصبی برای پردازش اطلاعات بسیار پیچیده استفاده می‌کند. هوش مصنوعی امکان استفاده از ابزارهای تحلیلی پیشرفته و راه‌حل‌های نوآورانه کسب‌وکار را در بخش بانکی فراهم می‌کند. سیستم‌های مبتنی بر هوش مصنوعی این امکان را برای بانک‌ها فراهم می‌کنند که دسترسی چندکاناله به مشتریان را توسعه دهند، به ترجیحات مشتریان پی ببرند و خدمات را به نیازهای مشتریان تطبیق دهند (سانی[4] و همکاران، ۲۰۲۰).

بخش مالی با ظهور شرکت‌های فین‌تک رقابتی‌تر شده است. انتظار می‌رود بانک‌ها راه‌حل‌های نوآورانه و اقدامات امنیتی مناسب برای حفظ حریم خصوصی اطلاعات مشتریان و برآورده کردن نیازهای آن‌ها را پیاده‌سازی کنند. با این حال، بانک‌های موجود در مقایسه با شرکت‌های فین‌تک جدید در استفاده از فناوری‌های نوین در موقعیت نامساعدی قرار دارند. بانک‌ها ممکن

[1] Brynjolfsson & McAfee
[2] Helbing
[3] Belanche
[4] Sanny

است در سازگاری با فناوری‌های جدید دچار مشکل شوند، زیرا رویه‌های موجود مانع از اجرای این فناوری‌ها می‌شوند. این ممکن است خطرات امنیتی اضافی ایجاد کند، زیرا سیستم‌های نرم‌افزاری مالی و امنیتی قدیمی با راه‌حل‌های نوآورانه سازگار نیستند (ارن[5]، ۲۰۲۱).

یکی از مسائل اصلی پیرامون استفاده از هوش مصنوعی در بخش بانکی، حریم خصوصی داده‌ها است. با توجه به اینکه چارچوب‌های نظارتی مربوطه هنوز در حال توسعه هستند، ممکن است مشخص نباشد که آیا بانک باید به ارائه‌دهندگان خدمات ثالث برای حفظ حریم خصوصی داده‌ها اعتماد کند یا خیر. استفاده از ابزارهای مبتنی بر هوش مصنوعی، مانند پردازش زبان طبیعی (NLP) برای تحلیل ارتباطات کارکنان و مشتریان یا چت‌بات‌ها برای ارتباط با مشتریان، ممکن است به حریم خصوصی افراد آسیب برساند. محیط نظارتی همچنان در حال تغییر است و این عدم قطعیت ممکن است توانایی بانک‌ها را در مقابله با تهدیدات سایبری مختل کند (تریویدی[6]، ۲۰۱۹).

درحالی که بسیاری از ابزارهای مبتنی بر هوش مصنوعی که توسط بانک‌ها استفاده می‌شوند، مرتبط با سیستم‌های پشتیبان هستند، برخی از قابلیت‌های هوش مصنوعی به‌طور صریح به کاربران نهایی ارائه می‌شوند. در زمینه امنیت سایبری، این به این معنی است که تدابیر امنیتی اتخاذ شده توسط بانک‌ها باید با آشنایی مشتریان با فناوری در نظر گرفته شوند. این موضوع به مدل پذیرش فناوری مرتبط است که توضیح می‌دهد چرا کاربران ممکن است فناوری‌های جدید را بپذیرند. این مدل دو عامل اصلی پذیرش فناوری را مفید بودن و سهولت استفاده می‌داند. بنابراین، امنیت سایبری سیستم‌های مبتنی بر هوش مصنوعی باید رفتار کاربران و آسیب‌پذیری‌های امنیتی ناشی از این رفتار را در نظر بگیرد. به‌ویژه، کاربران خدمات بانکداری اینترنتی ممکن است ناخواسته اطلاعات ورود خود را با دیگران به اشتراک بگذارند که می‌تواند منجر به نقض امنیت شود (اکبرالسادات و اسماعیل پور، ۱۴۰۱).

هوش مصنوعی و جرایم سایبری

هوش مصنوعی می‌تواند ابزارهای قدرتمندی برای بانک‌ها در مبارزه با تهدیدات جرایم سایبری ارائه دهد. روش‌هایی مانند شبکه‌های عصبی مصنوعی، سیستم‌های ایمنی مصنوعی، منطق فازی و الگوریتم‌های ژنتیکی به‌طور موفقیت‌آمیزی برای پیشگیری و شناسایی جرایم سایبری استفاده شده‌اند. به‌ویژه، شبکه‌های عصبی مصنوعی می‌توانند برای پردازش اطلاعات توزیع‌شده به‌منظور شناسایی ناهنجاری‌ها و پیشنهاد اقدامات مقابله‌ای استفاده شوند. شبکه‌های عصبی مصنوعی به نویز مقاوم هستند و به اندازه کافی انعطاف‌پذیرند تا پدیده‌های پیچیده و پویا را مدیریت کنند. به‌طور کلی، هوش مصنوعی توسط کسب‌وکارها برای شناسایی تهدیدات و متوقف کردن حملات، تحلیل نقاط پایانی موبایل و تقویت تحلیل انسانی استفاده شده است. در بخش بانکی، هوش مصنوعی می‌تواند درسه سطح، یعنی حفاظت، شناسایی و پاسخ‌دهی به‌کارگرفته شود (محمدی و شمس اللهی، ۱۴۰۲).

زیان‌های ناشی از حملات سایبری به بانک‌ها را می‌توان به دو گروه تقسیم کرد: زیان‌های مستقیم و زیان‌های غیرمستقیم. زیان‌های مستقیم به سرقت واقعی پول و نقض داده‌ها مربوط می‌شود. زیان‌های غیرمستقیم شامل روابط عمومی ضعیف و افزایش نارضایتی مشتریان است. تحلیل میزان جرایم سایبری در صنعت بانکداری کشورهای در حال توسعه نشان می‌دهد که جرایم سایبری به‌طور منفی بر یکپارچگی، کارایی و شهرت بانک‌ها تأثیر می‌گذارد. نتایج مشابهی در مورد امنیت سایبری در

[5] Eren
[6] Trivedi

خدمات بانکداری اینترنتی عربستان سعودی، هند و پاکستان گزارش شده است. به‌ویژه، محققان دریافتند که صفحه ورود به سیستم تعداد قابل توجهی از بانک‌ها هیچ اطلاعاتی درباره خطرات امنیتی مانند فیشینگ، مهندسی اجتماعی، شبکه‌های عمومی، SSL و سیاست رمز عبور نداشتند (عبداللهی کیا و شایان، ۱۴۰۲).

یادگیری ماشین خصمانه یک حوزه از یادگیری ماشین است که به‌دنبال تأثیرگذاری بر خروجی یک سیستم آموزش‌دیده با ارائه ورودی‌های خاص است. با توجه به تعداد سیستم‌های مبتنی بر هوش مصنوعی که در صنعت بانکداری به‌کار گرفته می‌شوند، یادگیری ماشین خصمانه می‌تواند یک تهدید عمده باشد. شبکه‌های مولد خصمانه (GAN) یک پیکربندی یادگیری ماشین هستند که در آن یک سیستم یادگیری ماشین برای شناسایی نقص‌ها در خروجی تولیدشده توسط سیستم یادگیری ماشین دیگری آموزش می‌بینند. توسعه GANها توانایی‌های هوش مصنوعی را برای تولید محتوای مصنوعی متقاعدکننده، یا "دیپ فیک" بهبود بخشیده است. یک روش یادگیری ماشین مرتبط با اختلال خصمانه به‌دنبال بهره‌برداری از مرزهای تصمیم‌گیری سیستم‌های موجود است. این امکان را می‌دهد که سیستم موجود را مجبور به تولید خروجی نادرست با تغییرات جزئی در ورودی‌ها کنیم (چنگیزی، ۱۴۰۳).

وجود یادگیری ماشین خصمانه نشان می‌دهد که سیستم‌های مبتنی بر هوش مصنوعی دارای آسیب‌پذیری‌های ذاتی هستند که باید هنگام استفاده از این سیستم‌ها در امنیت سایبری به آن‌ها توجه شود. بنابراین، جرایم سایبری مبتنی بر هوش مصنوعی را می‌توان به دو دسته تقسیم کرد. اول، هوش مصنوعی می‌تواند به‌عنوان ابزاری برای تسهیل جرم استفاده شود. به‌عنوان مثال، هکرها ممکن است از الگوریتم‌های هوش مصنوعی برای کشف آسیب‌پذیری‌ها در سیستم‌های امنیتی بانک‌ها استفاده کنند. دوم، یک سیستم هوش مصنوعی می‌تواند خود هدف یک جرم باشد. این مربوط به یادگیری ماشین خصمانه است و ممکن است شامل هکرهایی باشد که سیستم‌های امنیتی بانک‌ها را به گونه‌ای غیرقابل پیش‌بینی رفتار می‌دهند تا آسیب وارد کنند (آکدمیر و بلوت[7]، ۲۰۲۴).

جرایم مبتنی بر هوش مصنوعی شامل جعل صوتی و تصویری، فیشینگ هدفمند، اختلال در سیستم‌های کنترل‌شده توسط هوش مصنوعی، اخاذی‌های بزرگ‌مقیاس و مسمومیت داده‌ها است. جعل صوتی و تصویری می‌تواند توسط هکرها برای درخواست دسترسی به سیستم‌های امن یک بانک استفاده شود. فیشینگ یک تهدید عمده در مهندسی اجتماعی برای مشتریان و کارکنان در صنعت بانکداری است. فیشینگ هدفمند می‌تواند از سیستم‌های مبتنی بر هوش مصنوعی برای بهره‌برداری از داده‌های شبکه‌های اجتماعی به‌منظور بهبود نرخ موفقیت حمله استفاده کند. هکرها همچنین ممکن است از هوش مصنوعی برای اختلال در سیستم‌های امنیتی مبتنی بر هوش مصنوعی بانک‌ها استفاده کنند. هوش مصنوعی ممکن است حملات وب‌محور بزرگ‌مقیاس را تسهیل کند که می‌تواند بانک‌ها را در معرض اخاذی قرار دهد. با توجه به اینکه زیان‌های اقتصادی جهانی سالانه به دلیل جرایم سایبری حدود ۴۰۰ میلیارد دلار برآورد می‌شود، بررسی اختلال هوش مصنوعی در امنیت سایبری در صنعت بانکداری به‌ویژه اهمیت دارد (دمیرل و توپکو[8]، ۲۰۲۴).

-روش پژوهش

این پژوهش دارای رویکرد کیفی است و از نظریه داده بنیاد به‌عنوان روش پژوهش استفاده کرده است. در تحقیق کیفی حاضر، ابتدا محققان با الهام از ادبیات و مبانی نظری مرور شده به انتخاب چند محور جهت شروع مصاحبه و دریافت تجربیات

[7] Akdemir & Bulut
[8] Demirel & Topcu

مصاحبه‌شوندگان پرداخته و این محورها در قالب مقولات اصلی و فرعی تنظیم و با مصاحبه‌شوندگان در میان گذاشته شد. سپس از آن‌ها خواسته شد تجربیات خود را در این زمینه بازگو نمایند. نحوه ساماندهی جلسات مصاحبه به‌این‌ترتیب بود که از طریق تلفن یا پست الکترونیک با مصاحبه‌شونده هماهنگی اولیه صورت گرفت. در مرحله بعد متن کامل گفتگوها ضبط و سپس پیاده‌سازی شد. بعد از استخراج جملات کلیدی برحسب فراوانی تکرار آن‌ها و با استفاده از یک نظام مقوله‌بندی و عنوان دهی، با الهام از ادبیات پژوهش، هر مجموعه از جملات کلیدی بر اساس نزدیکی مفهومی و بیان یک مفهوم مشترک تحت عنوان یک مقوله مشخص عنوان‌بندی شد. لازم به ذکر است که مقوله‌بندی جملات کلیدی در ۲۰ مقوله صورت گرفته است. جامعه آماری پژوهش حاضر را کارشناسان و خبرگان بانک‌های استان تهران تشکیل دادند. حجم نمونه مشتمل بر ۲۰ نفرشامل بودند، که با رویکرد گلوله برفی انتخاب شدند. مصاحبه‌های عمیقی تا نیل به نقطه اشباع نظری صورت گرفت. با توجه به آن‌که تحقیق موردنظر درصدد بود با استفاده از راهبرد پژوهشی نظریه داده بنیاد به تصویر روشنی از چگونگی نقش هوش مصنوعی درتوسعه ی امنیت داده های شبکه بانکی کشور در قالب یک مدل بپردازد، از سؤال‌های مطابق جدول (۱) استفاده شده است.

جدول (۱) پرسش‌های پروتکل مصاحبه " نقش هوش مصنوعی درتوسعه ی امنیت داده های شبکه بانکی کشور"

پرسش‌های مصاحبه
[۱] به نظر شما هوش مصنوعی چه تعریفی دارد و چگونه می‌تواند در امنیت داده‌های شبکه بانکی به کار گرفته شود؟
[۲] چه کاربردهایی از هوش مصنوعی را در زمینه امنیت داده‌ها در بانک‌ها مشاهده کرده‌اید؟
[۳] به نظر شما مزایای استفاده از هوش مصنوعی در بهبود امنیت داده‌های بانکی چیست؟
[۴] چه چالش‌هایی در پیاده‌سازی هوش مصنوعی برای امنیت داده‌های شبکه بانکی وجود دارد؟
[۵] چگونه هوش مصنوعی می‌تواند در شناسایی و تحلیل تهدیدات سایبری در شبکه‌های بانکی کمک کند؟
[۶] آیا نمونه‌های موفقی از استفاده هوش مصنوعی در امنیت داده‌های بانکی در کشور یا سایر کشورها وجود دارد؟ لطفاً توضیح دهید.
[۷] به نظر شما آینده هوش مصنوعی در صنعت بانکداری و امنیت داده‌ها چگونه خواهد بود؟
[۸] چه اقداماتی باید در زمینه آموزش و فرهنگ‌سازی برای کارکنان بانک‌ها در زمینه استفاده از هوش مصنوعی انجام شود؟
[۹] چگونه می‌توان تعادل بین استفاده از هوش مصنوعی و حفظ حریم خصوصی مشتریان را برقرار کرد؟
[۱۰] به نظر شما فناوری‌های نوینی مانند بلاک‌چین و اینترنت اشیا چه تأثیری بر امنیت داده‌های بانکی و نقش هوش مصنوعی دارند؟

پس ازدریافت جواب سؤال‌ها، متن مصاحبه‌ها به‌دقت مکتوب شد و درکنار متن این مصاحبه‌ها، ازاسنادو مدارک دست دوبرای تبیین بهترنظریه استفاده گردید.دراین پژوهش، به‌منظور تجزیه‌وتحلیل داده‌ها پس از مکتوب کردن مصاحبه‌ها، داده‌های جمع‌آوری‌شده از طریق کدگذاری واکاوی شدو طی سه مرحله کدگذاری باز، محوری و انتخابی طبقه‌بندی گردید(کوهن[9] و همکاران، ۲۰۱۷).

[9] Cohen

برای بررسی روایی و پایایی، بنا به معیارهای ارائه‌شده توسط"کرسول و میلر[10] (۲۰۰۰)" به‌منظور حصول اطمینان از روایی پژوهش یا به عبارتی دقیق بودن یافته‌هاازمنظر پژوهشگر، مشارکت‌کنندگان یا خوانندگان گزارش پژوهش اقدامات زیر انجام شد:

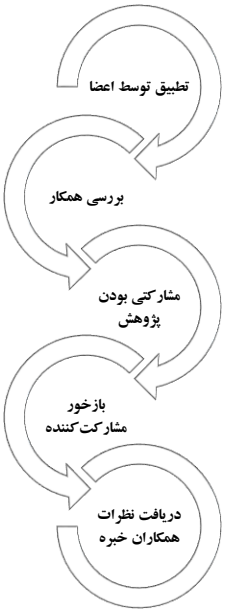
۱) تطبیق توسط اعضا:مشارکت‌کنندگان گزارش نهایی پژوهش، فرایندتحلیل و مقوله‌های به‌دست‌آمده را بازبینی و نظر خود را در ارتباط با آن‌ها ابراز کردند.

۲) بررسی همکار: چند نفر از دانشجویان دکتری و اعضای هیئت‌علمی دانشگاه که در مصاحبه‌ها مورد مشارکت قرار نگرفته بودند، به بررسی یافته‌ها و اظهارنظر درباره آن‌ها پرداختند.

۳) مشارکتی بودن پژوهش: به‌طور هم‌زمان از مشارکت‌کنندگان درتحلیل و تفسیر داده‌ها استفاده شد.

۴) بازخورمشارکت‌کننده: تفسیرها و نتایج به مشارکت‌کنندگان ارائه و موارد بد درک شده تعیین و اصلاح شدند.

۵) دریافت نظرات همکاران خبره:تبیین‌ها و نتایج توسط همکاران و خبرگان مورد بازبینی قرار گرفت و نظرات اصلاحی آن‌ها اعمال گردید.



نمودار ۱- حصول اطمینان از روایی پژوهش

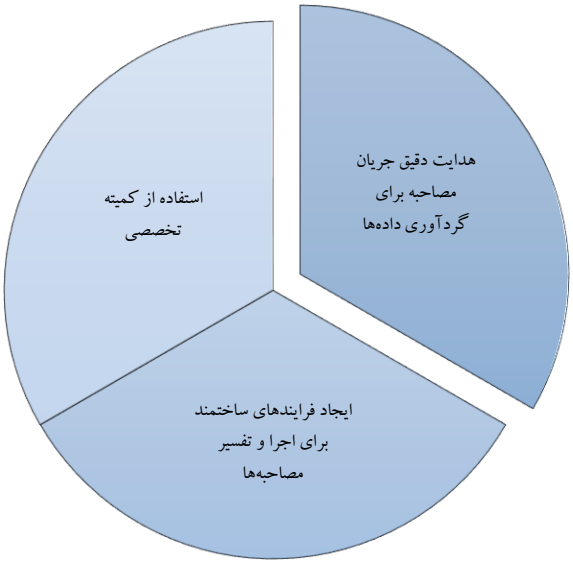
همچنین، استراتژی‌های بهبود پایایی در این پژوهش به‌صورت زیر بوده است:

۱) هدایت دقیق جریان مصاحبه برای گردآوری داده‌ها: در پژوهش حاضرمطابق با استانداردهای پژوهش‌های کیفی، راهنمای مصاحبه طراحی و مصاحبه‌ها با رعایت اصول علمی و اخلاقی برگزار گردید. به‌منظور اطمینان از پایایی نتایج مصاحبه‌ها، پس از کدگذاری اولیه، در فاصله زمانی کوتاهی کدگذاری‌ها بازبینی شد و نظرات تکمیلی آنان دریافت شد.

۲) ایجاد فرایندهای ساختمند برای اجرا و تفسیر مصاحبه‌ها: در فرایند مصاحبه‌ها، هر مصاحبه به‌طور جداگانه ثبت و سپس، پیاده‌سازی شد تا اطمینان حاصل شود که چیزی نادیده گرفته نمی‌شود. مصاحبه‌ها در محیط‌های آرام برگزار و پس از جمع‌آوری، داده‌ها با استفاده از روش‌های کدگذاری با رویکرد نظریه داده بنیاد تحلیل و تفسیر شدند.

۳) استفاده ازکمیته تخصصی:کلیه فرایندهای این پژوهش با نظارت اساتید مدیریت صنعتی و مدیریت فناوری اطلاعات انجام گردید.

[10] Creswell & Miller



نمودار ۲- استراتژی‌های بهبود پایایی

در ادامه پاسخ چهار مصاحبه شونده پژوهش آورده شده است:

"به نظر من، هوش مصنوعی به مجموعه‌ای از فناوری‌ها و الگوریتم‌ها اطلاق می‌شود که به سیستم‌ها این امکان را می‌دهد تا از طریق یادگیری و تحلیل داده‌ها، تصمیم‌گیری کنند. در امنیت داده‌های شبکه بانکی، هوش مصنوعی می‌تواند برای شناسایی الگوهای غیرعادی، پیش‌بینی تهدیدات و بهبود فرآیندهای احراز هویت مورد استفاده قرار گیرد. در بانک‌ها، هوش مصنوعی در تشخیص تقلب، تحلیل رفتار مشتریان و مدیریت ریسک به کارگرفته می‌شود. به عنوان مثال، سیستم‌های مبتنی بر هوش مصنوعی می‌توانند تراکنش‌های مشکوک را شناسایی کرده و آن‌ها را برای بررسی بیشتر علامت‌گذاری کنند. مزایای استفاده از هوش مصنوعی شامل افزایش دقت در شناسایی تهدیدات، کاهش زمان پاسخ به حملات و بهبود تجربه مشتری است. همچنین، هوش مصنوعی می‌تواند به بانک‌ها کمک کند تا هزینه‌های مربوط به امنیت را کاهش دهند. چالش‌های پیاده‌سازی شامل موانع فنی مانند عدم وجود داده‌های کافی برای آموزش الگوریتم‌ها، هزینه‌های بالا و موانع فرهنگی در پذیرش فناوری‌های جدید است. همچنین، نیاز به تخصص‌های فنی در این زمینه نیز یک چالش مهم محسوب می‌شود...(مصاحبه شونده شماره ۵)."

"هوش مصنوعی می‌تواند با تحلیل داده‌های بزرگ و شناسایی الگوهای غیرعادی، در شناسایی و تحلیل تهدیدات سایبری مؤثر باشد. به عنوان مثال، الگوریتم‌های یادگیری ماشین می‌توانند رفتارهای مشکوک را شناسایی کرده و به تیم‌های امنیتی هشدار دهند. در کشورهایی مانند ایالات متحده و انگلستان، بانک‌ها از هوش مصنوعی برای تشخیص تقلب و مدیریت ریسک استفاده کرده‌اند. به عنوان نمونه، برخی از بانک‌ها از سیستم‌های مبتنی بر هوش مصنوعی برای تحلیل رفتار مشتریان و شناسایی الگوهای مشکوک بهره‌برداری کرده‌اند... (مصاحبه‌شونده شماره ۹). "

"آینده هوش مصنوعی در صنعت بانکداری بسیار روشن به نظر می‌رسد. با پیشرفت فناوری، انتظار می‌رود که بانک‌ها به سمت استفاده بیشتر از هوش مصنوعی برای تحلیل پیشرفته و پیش‌بینی تهدیدات حرکت کنند.همچنین، هوش مصنوعی می‌تواند به بهبود خدمات مشتری و ارائه پیشنهادات شخصی‌سازی‌شده کمک کند. برای آموزش و فرهنگ‌سازی در زمینه استفاده از هوش

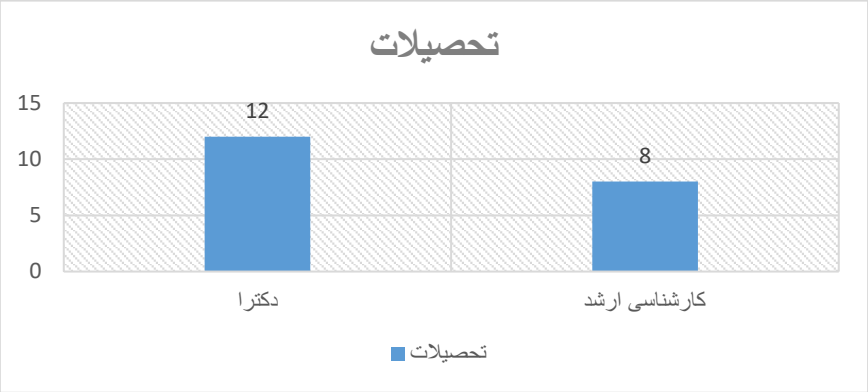
مصنوعی، بانک‌ها باید برنامه‌های آموزشی منظم و کارگاه‌های عملی برگزارکنند. این برنامه‌ها باید شامل آشنایی با فناوری‌های جدید و نحوه استفاده مؤثر از آن‌ها باشد... (مصاحبه‌شونده شماره ۱). "

"برای حفظ حریم خصوصی مشتریان، بانک‌ها باید مقررات و سیاست‌های مشخصی را در مورد استفاده از داده‌ها تدوین کنند. همچنین، استفاده از تکنیک‌های ناشناس‌سازی داده‌ها می‌تواند به ایجاد تعادل بین استفاده از هوش مصنوعی و حفظ حریم خصوصی کمک کند. فناوری‌های نوینی مانند بلاک‌چین و اینترنت اشیا می‌توانند به بهبود امنیت داده‌های بانکی کمک کنند. بلاک‌چین می‌تواند امنیت تراکنش‌ها را افزایش دهد و اینترنت اشیا می‌تواند داده‌های بیشتری را برای تحلیل در اختیار هوش مصنوعی قرار دهد. این فناوری‌ها در کنار هوش مصنوعی می‌توانند به ایجاد سیستم‌های امنیتی کارآمدتر کمک کنند... (مصاحبه‌شونده شماره ۱۳). "

در ادامه در جدول (۲)، خلاصه‌ای از اطلاعات مصاحبه‌شوندگان آورده شده است.

جدول (۲) خلاصه‌ای از اطلاعات مصاحبه‌شوندگان

ردیف	جنسیت	تحصیلات
۱	مرد	دکترا
۲	مرد	دکترا
۳	مرد	دکترا
۴	زن	دکترا
۵	مرد	دکترا
۶	زن	دکترا
۷	مرد	دکترا
۸	مرد	دکترا
۹	مرد	دکترا
۱۰	مرد	کارشناس ارشد
۱۱	مرد	کارشناس ارشد
۱۲	مرد	کارشناس ارشد
۱۳	مرد	کارشناس ارشد
۱۴	مرد	کارشناس ارشد
۱۵	زن	کارشناس ارشد
۱۶	مرد	کارشناس ارشد
۱۷	مرد	دکترا
۱۸	مرد	دکترا
۱۹	مرد	دکترا
۲۰	مرد	کارشناس ارشد



نمودار ۳- اطلاعات مصاحبه شوندگان

-یافته‌های پژوهش

با توجه به نظریه داده بنیادبه تحلیل داده‌هادرقالب کدگذاری باز، محوری و انتخابی پرداخته‌شده است.

الف) کدگذاری باز:

کدگذاری باز اشاره به بخشی از تحلیل دارد که با عنوان گذاری و مقوله‌بندی پدیده، آن‌طور که داده‌ها نشان داده‌اندسروکاردارد‌ونیازمندپرسیدن هستند، " مفاهیم" سؤالات و انجام مقایسه‌هاست. محصول عنوان گذاری و مقوله‌بندی که رکن اصلی در نظریه‌پردازی داده بنیاد تلقی می‌شوند. کدگذاری باز شامل تحلیل و کدگذاری داده‌ها، مشخص کردن طبقات و تفسیرآن‌ها بر اساس ویژگی‌های هر طبقه است. همچنین کدگذاری بازداده‌ها، به بخش‌های مجزا خردشده که برای به دست آوردن شباهت‌ها و تفاوت‌ها موردبررسی قرار می‌گیرند. منظور از خرد کردن و مفهوم‌پردازی این است که به هرکدام از حوادث، رخدادها و ایده‌هایی که در داده‌ها موجود است برچسبی بدهیم. این نام برچسب یا نشانه‌ای است که به‌جای حادثه، رخداد یا ایده می‌نشیند. در مرحله بعد، خود مفاهیم بر اساس شباهت‌هایشان طبقه‌بندی می‌شوند که به این کار مقوله پردازی گفته می‌شود. عنوانی که به مقوله‌ها (ابعاد) اختصاص داده می‌شود، انتزاعی‌تر از مفاهیمی (اجزایی) است که مجموعاً آن مقوله را تشکیل می‌دهند. مقولات دارای قدرت مفهومی بالایی هستند؛ زیرا می‌توانند مفاهیم و خرده مقولات را بر محور خود جمع کنند. عنوان یا نامی که برای مقولات انتخاب می‌شوند باید بیشترین ارتباط را با داده‌هایی که مقوله نمایانگر آن است، داشته و آن‌قدر با آن همخوان باشد که بتوان آنچه بیان می‌کند را به‌سرعت به یاد آورد و درباره‌اش فکر کرد. مضامین نیز ازکنار هم قرارگرفته مقولات مرتبط ایجادمی‌شوند.نمونه‌ای ازنتایج فراگردکدگذاری دراین تحقیق، درقالب مقوله‌های استخراج‌شده از مفاهیم در جدول (۳) ذکرشده‌اند. به‌منظور جلوگیری از طولانی شدن حجم مقاله از ارائه موارد تکراری و تعاریف تفصیلی مقولات ذکرشده خودداری شد؛ و نمونه‌ای از مصادیق مرتبط جهت آشنایی مخاطبان گرامی ارائه‌شده است.

ب) کدگذاری محوری:

هدف این مرحله، برقراری رابطه بین ابعاد (مقولات) تولیدشده در مرحله کدگذاری باز است. این کار بر اساس یک الگو و سرمشق جامع و کلی موسوم به مدل پارادایم انجام می‌شود و به نظریه‌پرداز کمک می‌کند تا تئوری فرایند اجتماعی موردمطالعه را راحت‌تر توسعه دهد. اساس فرایند ارتباط دهی درکدگذاری محوری برتمرکز و تعیین یک مقوله به‌عنوان مقوله

محوری یا اصلی قرار داشته و سپس سایر مقولات، به‌عنوان مقولات فرعی، ذیل عناوین مختلف مدل پارادایم بـه مقولـه اصـلی ارتباط داده می‌شوند (استراوس و کوربین[11]، ۱۹۹۸).

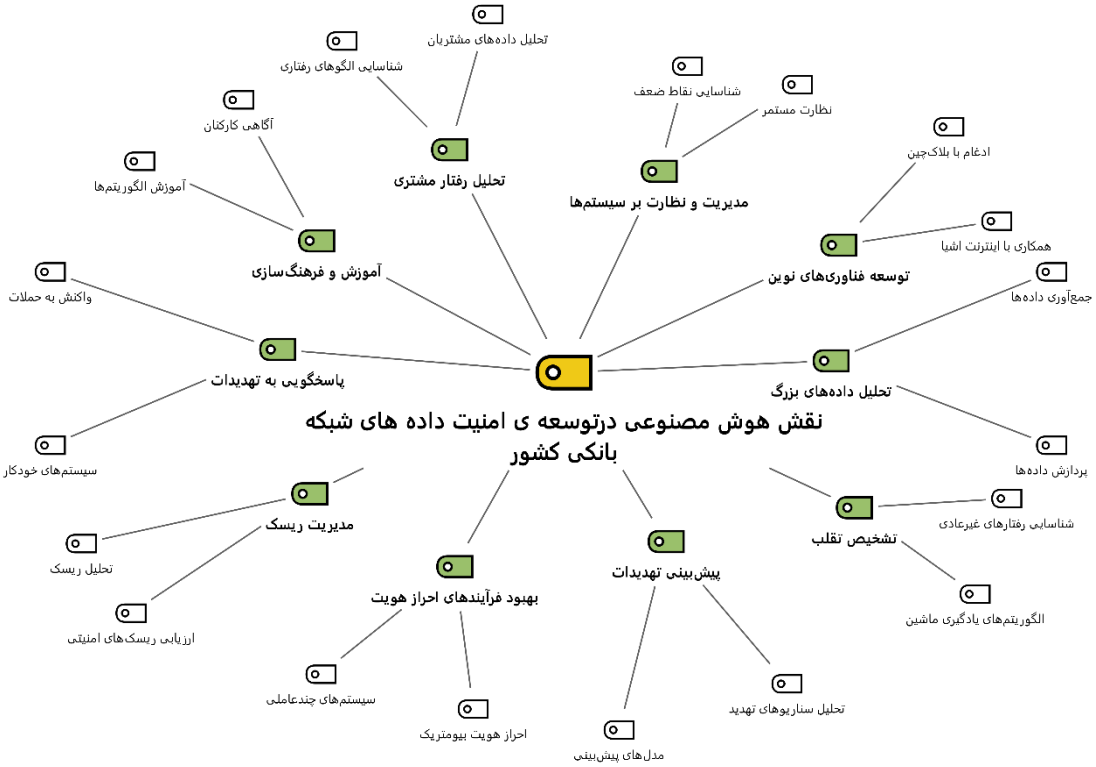
جدول (۳) نتایج کدگذاری

کدگذاری انتخابی	کدگذاری محوری	کدگذاری باز
تحلیل داده‌های بزرگ	جمع‌آوری داده‌ها پردازش داده‌ها	هوش مصنوعی می‌تواند حجم زیادی از داده‌های تراکنش‌ها و رفتار مشتریان را تجزیه و تحلیل کند تا الگوهای مشکوک را شناسایی کند.
تشخیص تقلب	الگوریتم‌های یادگیری ماشین شناسایی رفتارهای غیرعادی	این الگوریتم‌ها می‌توانند به طور خودکار تقلب‌ها را شناسایی کنند و به تیم‌های امنیتی هشدار دهند. آن‌ها می‌توانند رفتارهای غیرعادی رادرزمان واقعی شناسایی کنند.
پیش‌بینی تهدیدات	مدل‌های پیش‌بینی تحلیل سناریوهای تهدید	استفاده ازمدل‌های پیش‌بینی می‌تواندبه بانک‌ها کمک کندتا تهدیدات آینده راشناسایی کرده و اقدامات پیشگیرانه انجام دهند.
بهبود فرآیندهای احراز هویت	احراز هویت بیومتریک سیستم‌های چندعاملی	هوش مصنوعی می‌تواند درسیستم‌های احرازهویت بیومتریک مانندتشخیص چهره واثرانگشت به کارگرفته شودتاامنیت دسترسی به حساب‌ها را افزایش دهد.
مدیریت ریسک	تحلیل ریسک ارزیابی ریسک‌های امنیتی	هوش مصنوعی می‌تواند درشناسایی و ارزیابی ریسک‌های مربوط به امنیت داده‌ها و تراکنش‌ها کمک کند و بانک‌ها را در اتخاذ تصمیمات بهینه یاری دهد.
پاسخگویی به تهدیدات	سیستم‌های خودکار واکنش به حملات	هوش مصنوعی می‌تواند به سیستم‌های خودکار برای پاسخ به تهدیدات سایبری کمک کند، به طوری که در صورت شناسایی یک حمله، اقدامات لازم به سرعت انجام شود.
آموزش و فرهنگ‌سازی	آموزش الگوریتم‌ها آگاهی کارکنان	هوش مصنوعی می‌تواند به بانک‌ها کمک کند تا کارکنان خود را در زمینه شناسایی تهدیدات و بهترین شیوه‌های امنیتی آموزش دهند.
تحلیل رفتار مشتری	شناسایی الگوهای رفتاری تحلیل داده‌های مشتریان	با تحلیل رفتار مشتری، بانک‌ها می‌توانند الگوهای مشکوک را شناسایی کرده و به سرعت به آن‌ها واکنش نشان دهند.
مدیریت و نظارت بر سیستم‌ها	نظارت مستمر شناسایی نقاط ضعف	هوش مصنوعی می‌تواندبه نظارت مستمربر سیستم‌های بانکی کمک کند و به شناسایی نقاط ضعف امنیتی بپردازد.
توسعه فناوری‌های نوین	ادغام با بلاک‌چین همکاری با اینترنت اشیا	هوش مصنوعی می‌تواند با فناوری‌های جدید مانند بلاک‌چین و اینترنت اشیا ادغام شود تا امنیت داده‌ها را افزایش دهد.

[11] Strauss & Corbin

ج) کدگذاری انتخابی:

در این مرحله می‌توان مطابق با شکل(۱) مدل ترسیمی ارائه‌شده برای پاسخ به سؤال پژوهش (چگونه هوش مصنوعی درتوسعه ی امنیت داده های شبکه بانکی کشور موثر است؟) است.



شکل (۱) کدگذاری انتخابی و مدل نهایی برای نقش هوش مصنوعی درتوسعه ی امنیت داده های شبکه بانکی کشور

-نتیجه‌گیری و پیشنهادها

هوش مصنوعی قادر است الگوهای عادی تراکنش‌ها را شناسایی کندوهرگونه رفتار غیرمعمول را به سرعت شناسایی کند. این کار به شناسایی تقلب و تهدیدات امنیتی کمک می‌کند. با استفاده از الگوریتم‌های یادگیری ماشین، بانک‌ها می‌توانند تهدیدات احتمالی را پیش‌بینی کرده و اقدامات پیشگیرانه انجام دهند. این پیش‌بینی‌ها می‌تواند شامل شناسایی الگوهای حملات سایبری باشد. تحلیل داده‌های بزرگ به بانک‌ها این امکان را می‌دهد که در زمان واقعی به تهدیدات پاسخ دهند. این امر به کاهش زمان واکنش و جلوگیری از خسارات مالی کمک می‌کند. با تجزیه و تحلیل داده‌های بزرگ، بانک‌ها می‌توانند تصمیمات بهتری در زمینه امنیت اتخاذ کنند. این تصمیمات می‌تواند شامل تغییرات در سیاست‌های امنیتی و به‌روزرسانی سیستم‌ها باشد. تحلیل داده‌های بزرگ می‌تواند به شناسایی و ارزیابی ریسک‌های مختلف کمک کند و به بانک‌ها اجازه دهد که استراتژی‌های بهتری برای مدیریت ریسک‌های امنیتی ایجاد کنند. با تحلیل داده‌های بزرگ، بانک‌ها می‌توانند رفتار مشتریان را درک کرده و هرگونه رفتار مشکوک را شناسایی کنند. این کار به کاهش تقلب و افزایش امنیت کمک می‌کند. هوش مصنوعی می‌تواند فرآیندهای امنیتی را خودکار کند و به کاهش بار کاری تیم‌های امنیتی کمک کند. این امر باعث می‌شود که آن‌ها بتوانند بر روی مسائل پیچیده‌تر تمرکزکنند. با تحلیل مداوم داده‌های بزرگ، بانک‌ها می‌توانند از تهدیدات جدید آگاه

شوند و استراتژی‌های امنیتی خود را به‌روز کنند. تحلیل داده‌های بزرگ با هوش مصنوعی نه تنها به شناسایی و پیشگیری از تهدیدات کمک می‌کند، بلکه به بهبود کلی امنیت داده‌های شبکه بانکی و اعتماد مشتریان نیز منجر می‌شود. این ترکیب می‌تواند به عنوان یک ابزار قوی در حفاظت از اطلاعات حساس و جلوگیری از تقلب و حملات سایبری عمل کند.

هوش مصنوعی می‌تواند به شناسایی الگوهای عادی تراکنش‌ها کمک کند و هرگونه رفتار غیرمعمول را شناسایی کند. این شناسایی به سرعت می‌تواند به کشف تقلب‌ها منجر شود. با تحلیل داده‌ها در زمان واقعی، امکان شناسایی و جلوگیری از تقلب‌های در حال انجام فراهم می‌شود. این امر به کاهش خسارات مالی و حفظ اعتبار بانک کمک می‌کند. استفاده از هوش مصنوعی در تشخیص تقلب می‌تواند به کاهش خطاهای انسانی کمک کند. سیستم‌های خودکار می‌توانند با دقت بیشتری رفتارهای مشکوک را شناسایی کنند. الگوریتم‌های یادگیری ماشین می‌توانند به پیش‌بینی تقلب‌ها بر اساس داده‌های تاریخی و الگوهای رفتاری مشتریان کمک کنند. این پیش‌بینی‌ها می‌تواند به بانک‌ها در اتخاذ تصمیمات پیشگیرانه کمک کند. هوش مصنوعی می‌تواند داده‌های مختلف از منابع گوناگون (مانند تاریخچه تراکنش‌ها، اطلاعات مشتریان و رفتار آنلاین) را تجزیه و تحلیل کند تا الگوهای تقلب را شناسایی کند. با استفاده از سیستم‌های هوش مصنوعی، بانک‌ها می‌توانند هزینه‌های مربوط به امنیت را کاهش دهند و در عوض بر روی توسعه و بهبود سیستم‌های امنیتی سرمایه‌گذاری کنند. سیستم‌های هوش مصنوعی می‌توانند با یادگیری از داده‌های جدید، دقت تشخیص تقلب را افزایش دهند و تعداد مثبت‌های کاذب را کاهش دهند، که می‌تواند به بهبود تجربه مشتری کمک کند. با تحلیل رفتار مشتریان و شناسایی الگوهای غیرعادی، بانک‌ها می‌توانند به صورت مؤثری تقلب‌ها را شناسایی کنند و ازآن‌ها جلوگیری کنند. تشخیص تقلب با هوش مصنوعی نه تنها به شناسایی و پیشگیری از تقلب‌ها کمک می‌کند، بلکه به بهبود کلی امنیت داده‌های شبکه بانکی و افزایش اعتماد مشتریان نیز منجر می‌شود. این ابزار می‌تواند به عنوان یک راهکار مؤثر در حفاظت از اطلاعات حساس و جلوگیری از خسارات مالی عمل کند.

هوش مصنوعی می‌تواند الگوهای تهدیدات گذشته را شناسایی کند و این الگوها را برای پیش‌بینی تهدیدات آینده استفاده کند.این امر به بانک‌ها کمک می‌کند تا به موقع اقدامات پیشگیرانه انجام دهند. با استفاده از الگوریتم‌های یادگیری ماشین، بانک‌ها می‌توانند رفتارهای مخرب را شبیه‌سازی و پیش‌بینی کنند. این پیش‌بینی‌ها می‌تواند شامل شناسایی حملات سایبری و تقلب‌های مالی باشد. پیش‌بینی تهدیدات در زمان واقعی به بانک‌ها این امکان را می‌دهد که به سرعت به تهدیدات پاسخ دهند و از وقوع آن‌ها جلوگیری کنند. این امر به کاهش خسارات مالی و افزایش امنیت کمک می‌کند. با پیش‌بینی تهدیدات، بانک‌ها می‌توانند ریسک‌های مختلف را شناسایی و ارزیابی کنند و استراتژی‌های مناسبی برای مدیریت آن‌ها ایجاد کنند. پیش‌بینی تهدیدات با هوش مصنوعی به بانک‌ها این امکان را می‌دهد که تصمیمات بهتری در زمینه امنیت اتخاذ کنند. این تصمیمات می‌تواند شامل تغییرات در سیاست‌های امنیتی و به‌روزرسانی سیستم‌ها باشد. با پیش‌بینی تهدیدات، بانک‌ها می‌توانند منابع خود را به طور مؤثرتری تخصیص دهند و بر روی نقاط ضعف تمرکز کنند. با پیش‌بینی مداوم تهدیدات، بانک‌ها می‌توانند از تهدیدات جدید آگاه شوند و استراتژی‌های امنیتی خود را به‌روز کنند. پیش‌بینی تهدیدات می‌تواند به شناسایی رفتارهای غیرعادی مشتریان کمک کند و به بانک‌ها این امکان را بدهد که اقدامات لازم را انجام دهند. پیش‌بینی تهدیدات با هوش مصنوعی نه تنها به شناسایی و پیشگیری از تهدیدات کمک می‌کند، بلکه به بهبود کلی امنیت داده‌های شبکه بانکی و افزایش اعتماد مشتریان نیز منجر می‌شود. این ابزار می‌تواند به عنوان یک راهکار مؤثر در حفاظت از اطلاعات حساس و جلوگیری از خسارات مالی عمل کند.

هوش مصنوعی می‌تواند الگوهای رفتاری کاربران را شناسایی کند و به این ترتیب، دقت احراز هویت را افزایش دهد. این امر به شناسایی هویت واقعی کاربران کمک می‌کند. با تحلیل داده‌ها، هوش مصنوعی می‌تواند هرگونه رفتار غیرعادی را شناسایی کند

و در صورت نیاز، دسترسی را مسدود کند. این امر به کاهش تقلب و دسترسی غیرمجاز کمک می‌کند. هوش مصنوعی می‌تواند به بهبود فرآیندهای احراز هویت چندعاملی کمک کند، به‌طوری‌که از ترکیب روش‌های مختلف (مانند بیومتریک، رمزعبوروتأیید دومرحله‌ای) استفاده شود. با استفاده از هوش مصنوعی، فرآیندهای احراز هویت می‌توانند در زمان واقعی تحلیل و ارزیابی شوند، که به سرعت به تهدیدات پاسخ می‌دهد و امنیت را افزایش می‌دهد. هوش مصنوعی می‌تواند به خودکارسازی فرآیندهای احراز هویت کمک کند و به این ترتیب، خطاهای انسانی را کاهش دهد. این خودکارسازی دقت و کارایی را افزایش می‌دهد. با استفاده از الگوریتم‌های یادگیری ماشین، سیستم‌های احراز هویت می‌توانند تهدیدات احتمالی را پیش‌بینی و شناسایی کنند و از آن‌ها جلوگیری کنند. با استفاده از هوش مصنوعی، فرآیندهای احراز هویت می‌توانند به گونه‌ای طراحی شوند که تجربه کاربری بهتری ارائه دهند و کاربران را از مراحل پیچیده و زمان‌بر رها کنند. هوش مصنوعی می‌تواند به تحلیل و گزارش‌گیری از الگوهای احراز هویت کمک کند و بانک‌ها را در بهبود سیاست‌های امنیتی یاری کند. بهبود فرآیندهای احراز هویت با هوش مصنوعی نه تنها به افزایش امنیت داده‌های شبکه بانکی کمک می‌کند، بلکه به بهبود تجربه کاربری و کاهش تقلب نیز منجر می‌شود. این ابزار می‌تواند به عنوان یک راهکار مؤثر درحفاظت از اطلاعات حساس و جلوگیری از خسارات مالی عمل کند.

هوش مصنوعی می‌تواند به تحلیل و ارزیابی حجم زیادی از داده‌ها کمک کند و ریسک‌های مختلف را شناسایی کند. این شناسایی به بانک‌ها این امکان را می‌دهد که نقاط ضعف خود را شناسایی کنند. با استفاده از الگوریتم‌های یادگیری ماشین، سیستم‌های هوش مصنوعی می‌توانند تهدیدات آینده را پیش‌بینی کنند. این پیش‌بینی‌ها به بانک‌ها کمک می‌کند تا اقدامات پیشگیرانه انجام دهند. هوش مصنوعی می‌تواند به تحلیل داده‌ها در زمان واقعی کمک کند، که به بانک‌ها این امکان را می‌دهد که به سرعت به تهدیدات پاسخ دهند و از وقوع آن‌ها جلوگیری کنند. با استفاده از هوش مصنوعی، بانک‌ها می‌توانند ریسک‌های مالی را شناسایی و ارزیابی کنند و استراتژی‌های مناسبی برای مدیریت آن‌ها ایجاد کنند. هوش مصنوعی می‌تواند به خودکارسازی فرآیندهای مدیریت ریسک کمک کند و به این ترتیب، خطاهای انسانی را کاهش دهد. این امر به دقت و کارایی در مدیریت ریسک کمک می‌کند. هوش مصنوعی می‌تواند به تحلیل رفتار مشتریان کمک کند و الگوهای مشکوکی را شناسایی کند که ممکن است به تقلب یا تخلفات مالی منجر شود. با استفاده از هوش مصنوعی، بانک‌ها می‌توانند تصمیمات بهتری در زمینه مدیریت ریسک اتخاذ کنند. این تصمیمات می‌تواند شامل تغییرات درسیاست‌های امنیتی و به‌روزرسانی سیستم‌ها باشد. با شناسایی و مدیریت ریسک‌ها، بانک‌ها می‌توانند منابع خود را به طور مؤثرتری تخصیص دهند و بر روی نقاط ضعف تمرکز کنند. مدیریت ریسک با هوش مصنوعی نه تنها به شناسایی و پیشگیری از تهدیدات کمک می‌کند، بلکه به بهبود کلی امنیت داده‌های شبکه بانکی و افزایش اعتماد مشتریان نیز منجر می‌شود. این ابزار می‌تواند به عنوان یک راهکار مؤثر درحفاظت از اطلاعات حساس و جلوگیری از خسارات مالی عمل کند.

هوش مصنوعی می‌تواند حجم زیادی از داده‌ها را به سرعت تحلیل کند و تهدیدات را شناسایی کند. این تحلیل به بانک‌ها کمک می‌کند تا به موقع واکنش نشان دهند. الگوریتم‌های یادگیری ماشین می‌توانند الگوهای حملات سایبری را شناسایی کنند و به این ترتیب، بانک‌ها می‌توانند به پیش‌بینی و شناسایی حملات مشابه در آینده بپردازند. با استفاده از هوش مصنوعی، فرآیندهای پاسخ به تهدیدات می‌توانند به صورت خودکار انجام شوند. این امر به کاهش زمان پاسخ و افزایش کارایی کمک می‌کند. هوش مصنوعی می‌تواند به تحلیل داده‌ها در زمان واقعی کمک کند و به سرعت به تهدیدات پاسخ دهد، که این امر به جلوگیری از خسارات بیشتر کمک می‌کند. با استفاده از هوش مصنوعی، امکان کاهش خطاهای انسانی در فرآیندهای پاسخ به تهدیدات وجود دارد. این امر به بهبود دقت و کارایی سیستم‌ها کمک می‌کند. سیستم‌های هوش مصنوعی می‌توانند از

تجربیات گذشته یاد بگیرند و به بهبود فرآیندهای پاسخ به تهدیدات کمک کنند. این یادگیری به بانک‌ها امکان می‌دهد تا استراتژی‌های بهتری برای مقابله با تهدیدات ایجاد کنند. با تحلیل داده‌ها و شناسایی الگوهای مشکوک، هوش مصنوعی می‌تواند تهدیدات را قبل از وقوع شناسایی کند و به این ترتیب، بانک‌ها می‌توانند اقدامات پیشگیرانه انجام دهند. با پاسخگویی سریع به تهدیدات، بانک‌ها می‌توانند از اختلالات در خدمات خود جلوگیری کنند و تجربه کاربری بهتری ارائه دهند.

پاسخگویی به تهدیدات با هوش مصنوعی نه تنها به افزایش امنیت داده‌های شبکه بانکی کمک می‌کند، بلکه به بهبود کارایی و کاهش خسارات مالی نیز منجر می‌شود. این ابزار می‌تواند به عنوان یک راهکار مؤثر در حفاظت از اطلاعات حساس و ایجاد اعتماد در مشتریان عمل کند.

هوش مصنوعی می‌تواند به تحلیل نیازهای آموزشی کارکنان کمک کند و برنامه‌های آموزشی متناسب با نیازهای آن‌ها ارائه دهد.این امر به افزایش آگاهی و دانش کارکنان درباره تهدیدات امنیتی کمک می‌کند. با استفاده از هوش مصنوعی، می‌توان رفتارهای مشکوک را شناسایی کرد و در صورت نیاز، آموزش‌های لازم به کارکنان ارائه داد. این شناسایی به جلوگیری از وقوع حملات داخلی کمک می‌کند. هوش مصنوعی می‌تواند به شبیه‌سازی سناریوهای حمله کمک کند تا کارکنان بتوانند در شرایط واقعی‌تر آموزش ببینند و آمادگی بیشتری برای مقابله با تهدیدات پیدا کنند.باتحلیل داده‌های مربوط به هرفرد، هوش مصنوعی می‌تواندمحتوای آموزشی شخصی‌سازی‌شده‌ای ارائه دهد که به نیازها و سطح دانش هر کارمند پاسخ دهد. آموزش‌های مستمر و فرهنگ‌سازی می‌تواند به ایجاد یک فرهنگ امنیتی قوی در سازمان کمک کند، به‌طوری‌که همه کارکنان به اهمیت امنیت داده‌ها توجه داشته باشند. هوش مصنوعی می‌تواند با استفاده از فناوری‌های نوین مانند یادگیری تعاملی و واقعیت مجازی، فرآیند یادگیری را تسهیل کند و تجربه آموزشی بهتری ایجاد کند. استفاده از چت‌بات‌ها و سیستم‌های هوش مصنوعی می‌تواند به کارکنان کمک کند تا به سؤالات و مشکلات خود در زمینه امنیت داده‌ها پاسخ دهند و در صورت نیاز، راهنمایی‌های لازم را دریافت کنند. هوش مصنوعی می‌تواند به ارزیابی اثربخشی برنامه‌های آموزشی کمک کند و نقاط ضعف و قوت آن‌ها را شناسایی کند. این ارزیابی به بهبود مستمر فرآیندهای آموزشی کمک می‌کند. آموزش و فرهنگ‌سازی با هوش مصنوعی نه تنها به افزایش آگاهی و دانش کارکنان درباره امنیت داده‌ها کمک می‌کند، بلکه به ایجاد یک فرهنگ امنیتی قوی و پاسخگویی مؤثر به تهدیدات نیز منجر می‌شود. این امر به حفاظت از اطلاعات حساس و افزایش اعتماد مشتریان در شبکه بانکی کمک می‌کند.

هوش مصنوعی می‌تواند الگوهای عادی رفتار مشتریان را شناسایی کند و در صورت وقوع رفتارهای غیرمعمول، هشدارهای لازم راصادر کند. این امر به شناسایی و جلوگیری از کلاهبرداری‌ها کمک می‌کند. با تحلیل داده‌های تاریخی رفتار مشتریان، هوش مصنوعی می‌تواند تهدیدات احتمالی را پیش‌بینی کند و به بانک‌ها اجازه می‌دهد تا اقدامات پیشگیرانه انجام دهند. با استفاده از هوش مصنوعی، بانک‌ها می‌توانند نیازها و ترجیحات مشتریان را شناسایی کرده و خدمات متناسب با آن‌ها ارائه دهند. این شخصی‌سازی باعث افزایش رضایت مشتریان و کاهش احتمال رفتارهای مشکوک می‌شود. هوش مصنوعی می‌تواند تراکنش‌های مشتریان را در زمان واقعی تحلیل کند و در صورت شناسایی تراکنش‌های مشکوک، اقدامات لازم را انجام دهد. این امر به کاهش کلاهبرداری و تقلب در تراکنش‌ها کمک می‌کند. تحلیل رفتار مشتری با هوش مصنوعی می‌تواند به کاهش خطاهای انسانی در شناسایی تهدیدات کمک کند و دقت و سرعت پاسخ به تهدیدات را افزایش دهد. هوش مصنوعی قادر است حجم زیادی از داده‌های مشتریان را تحلیل کند و الگوهای مهم را استخراج کند که به شناسایی تهدیدات کمک می‌کند. با استفاده از تحلیل رفتار مشتری و شناسایی تهدیدات، بانک‌ها می‌توانند از داده‌های حساس مشتریان محافظت کنند و اعتماد آن‌ها را جلب کنند. هوش مصنوعی می‌تواند به تحلیل داده‌ها در زمان واقعی کمک کند و به سرعت به تهدیدات پاسخ دهد،

که این امر به جلوگیری از خسارات بیشتر کمک می‌کند. تحلیل رفتار مشتری با هوش مصنوعی نه تنها به افزایش امنیت داده‌های شبکه بانکی کمک می‌کند، بلکه به بهبود تجربه کاربری و افزایش اعتماد مشتریان نیز منجر می‌شود. این ابزار می‌تواند به عنوان یک راهکارمؤثردرحفاظت از اطلاعات حساس و کاهش کلاهبرداری‌ها عمل کند.

هوش مصنوعی می‌تواند به طورمداوم سیستم‌ها را نظارت کند و به شناسایی تهدیدات و فعالیت‌های مشکوک در زمان واقعی کمک کند. این نظارت مستمر به جلوگیری از حملات سایبری کمک می‌کند. با استفاده از الگوریتم‌های هوش مصنوعی، بانک‌ها می‌توانند حجم زیادی از داده‌ها را تحلیل کنند و الگوهای ناهنجاری را شناسایی کنند که ممکن است به تهدیدات امنیتی اشاره داشته باشند. هوش مصنوعی می‌تواند به شناسایی الگوهای غیرمعمول در فعالیت‌های سیستم‌ها کمک کند. این شناسایی به بانک‌ها اجازه می‌دهد تا به سرعت به تهدیدات پاسخ دهند. هوش مصنوعی می‌تواند با استفاده ازداده‌های تاریخی، حملات احتمالی را پیش‌بینی کندو به بانک‌ها امکان می‌دهد تا اقدامات پیشگیرانه انجام دهند. با استفاده از هوش مصنوعی، بسیاری ازفرآیندهای نظارتی و مدیریتی می‌توانند به صورت خودکار انجام شوند، که این امر به کاهش بار کاری کارکنان و افزایش کارایی کمک می‌کند. هوش مصنوعی می‌تواند به تحلیل داده‌ها در زمان واقعی کمک کند و در صورت شناسایی تهدیدات، به سرعت اقداماتی را انجام دهد.هوش مصنوعی می‌تواندبه شناسایی و ارزیابی ریسک‌های امنیتی کمک کند و به بانک‌ها اجازه دهد تا استراتژی‌های مدیریت ریسک مؤثرتری را پیاده‌سازی کنند.سیستم‌های مبتنی برهوش مصنوعی می‌توانند به صورت خودکار گزارش‌های دقیقی از وضعیت امنیتی سیستم‌ها تولید کنند و به مدیران کمک کنند تا تصمیمات بهتری اتخاذ کنند. مدیریت و نظارت برسیستم‌ها با هوش مصنوعی نه تنها به بهبود امنیت داده‌های شبکه بانکی کمک می‌کند، بلکه به افزایش کارایی و کاهش خطاهای انسانی نیز منجر می‌شود. این امر به حفاظت از اطلاعات حساس و کاهش خطرات امنیتی در بانک‌ها کمک می‌کند.

هوش مصنوعی می‌تواند به بهبود زیرساخت‌های امنیتی کمک کند و فناوری‌های جدیدی مانند تشخیص نفوذ، رمزنگاری پیشرفته واحرازهویت چندعاملی را به کار گیرد. با استفاده از الگوریتم‌های هوش مصنوعی، می‌توان به شناسایی تهدیدات جدید و الگوهای حمله نوین پرداخت. این شناسایی به بانک‌ها کمک می‌کند تا به سرعت به تهدیدات واکنش نشان دهند. هوش مصنوعی می‌تواند به شبیه‌سازی سناریوهای حمله و پیش‌بینی رفتارهای مهاجمان کمک کند، که این امر به بانک‌ها اجازه می‌دهد تا اقدامات پیشگیرانه انجام دهند. با استفاده از هوش مصنوعی، بسیاری از فرآیندهای امنیتی می‌توانند به صورت خودکار انجام شوند، که این امر به کاهش خطاهای انسانی و افزایش دقت کمک می‌کند. هوش مصنوعی می‌تواند به تحلیل داده‌ها در زمان واقعی کمک کند و در صورت شناسایی تهدیدات، به سرعت اقداماتی را انجام دهد. هوش مصنوعی می‌تواند به شناسایی و ارزیابی ریسک‌های امنیتی کمک کند و به بانک‌ها اجازه دهد تا استراتژی‌های مدیریت ریسک مؤثرتری را پیاده‌سازی کنند. با استفاده از هوش مصنوعی، بانک‌ها می‌توانند خدمات خود را بر اساس نیازها و رفتارمشتریان شخصی‌سازی کنند، که این امربه افزایش رضایت مشتریان و کاهش رفتارهای مشکوک منجرمی‌شود.سیستم‌های مبتنی برهوش مصنوعی می‌توانند به صورت خودکار گزارش‌های دقیقی از وضعیت امنیتی تولید کنند و به مدیران کمک کنند تا تصمیمات بهتری اتخاذ کنند. توسعه فناوری‌های نوین با هوش مصنوعی نه تنها به بهبود امنیت داده‌های شبکه بانکی کمک می‌کند، بلکه به افزایش کارایی، کاهش هزینه‌ها و بهبود تجربه کاربری نیز منجر می‌شود. این امر به حفاظت از اطلاعات حساس و کاهش خطرات امنیتی در بانک‌ها کمک می‌کند.

باتوجه به آنچه که بدست آمد پیشنهاد می شود: توسعه سیستم‌های هوش مصنوعی که می‌توانند رفتارهای غیرمعمول مشتریان را شناسایی و هشدارهای لازم راصادرکنند. ایجاد سیستم‌های تشخیص نفوذ که با استفاده از هوش مصنوعی،

تهدیدات سایبری را در زمان واقعی شناسایی کنند. استفاده از الگوریتم‌های هوش مصنوعی برای بهبود فرآیند احراز هویت، شامل تشخیص چهره، اثر انگشت و سایرروش‌های بیومتریک. بهره‌گیری از تکنیک‌های تحلیل داده‌های بزرگ برای پیش‌بینی و شناسایی تهدیدات امنیتی قبل از وقوع آن‌ها. توسعه سیستم‌های خودکار برای مدیریت و نظارت بر امنیت داده‌ها که به کاهش خطای انسانی کمک کند. استفاده از هوش مصنوعی برای تحلیل رفتار مشتریان و شناسایی الگوهای کلاهبرداری و فعالیت‌های مشکوک.توسعه سیستم‌های هوش مصنوعی که به شناسایی و ارزیابی ریسک‌های امنیتی کمک کنند و استراتژی‌های مدیریت ریسک بهینه را پیشنهاد دهند. به‌روزرسانی و آموزش مداوم مدل‌های هوش مصنوعی با داده‌های جدید برای افزایش دقت و کارایی آن‌ها. پیاده‌سازی سیستم‌های هوش مصنوعی که به طور خودکار گزارش‌های امنیتی دقیق تولید کنند و به مدیران کمک کنند تا تصمیمات بهتری اتخاذ کنند. ایجاد برنامه‌های آموزشی مبتنی بر هوش مصنوعی برای آموزش کارکنان در زمینه امنیت سایبری و استفاده از فناوری‌های نوین؛ اجرای این پیشنهادات می‌تواند به بهبود امنیت داده‌های شبکه بانکی کشورکمک کند و به کاهش خطرات امنیتی و افزایش اعتماد مشتریان منجر شود.

منابع

– اکبرالسادات، مجید.، اسماعیل پور، بابک. (۱۴۰۱). مروری بر روش های کشف تقلب بانکی با استفاده از هوش مصنوعی. اکتشاف و پردازش هوشمند دانش، ۲ (۳)، ۴۱-۲۰.

– چنگیزی ماسوله، علی.(۱۴۰۳).بررسی تاثیرهوش مصنوعی بربهینه سازی تجربه کاربری بانقش میانجی بهبودتعاملات مشتری درپلتفرم های تجارت الکترونیک، بیست و چهارمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات، بابل.

– عبداللهی کیا، محمدرضا.، شایان، علی.(۱۴۰۲).تاثیررویکردهای نوین دراستفاده ازهوش مصنوعی درصنعت بانکداری ایران: با تمرکز بر بانک ملی ایران، هفتمین همایش ملی افق های نوین در مدیریت، اقتصاد و کامپیوتر، تهران.

– محمدی، حمیدرضا.، شمس اللهی، ژامک. (۱۴۰۲). تاثیر هوش مصنوعی در صنعت بانکداری، هفتمین همایش ملی افق های نوین در مدیریت، اقتصاد و کامپیوتر، تهران.

– مرتضائی دکاهی، قادر. (۱۴۰۲). چت بات ها فرصتی نوین در خدمات بانکداری الکترونیک، ششمین همایش ملی فناوریهای نوین در مهندسی برق، کامپیوتر و مکانیک ایران، تهران .

– مظهرپور، دیار.، سیدکلان، سیدمحمد.(۱۴۰۳).سنتزپژوهی کاربردچت بات ها (نرم افزار هوش مصنوعی) در آموزش زبان انگلیسی.

– Akdemir, D. M., & Bulut, Z. A. (2024). Business and Customer-Based Chatbot Activities: The Role of Customer Satisfaction in Online Purchase Intention and Intention to Reuse Chatbots. Journal of Theoretical and Applied Electronic Commerce Research, 19(4), 2961-2979.

– Alnaser, F. M., Rahi, S., Alghizzawi, M., & Ngah, A. H. (2023). Does artificial intelligence (AI) boost digital banking user satisfaction? Integration of expectation confirmation model and antecedents of artificial intelligence enabled digital banking. Heliyon, 9(8).

– Belanche, D., Casaló, L. V., & Flavián, C. (2019). Artificial Intelligence in FinTech: understanding robo-advisors adoption among customers. Industrial Management & Data Systems, 119(7), 1411-1430.

– Brynjolfsson, E., & McAfee, A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. WW Norton & company.

– Demirel, S., & Topcu, M. (2024). The Impact of Artificial Intelligence Applications on Digital Banking in Turkish Banking Industry. Advances in Human-Computer Interaction, 2024(1), 9921363.

– Eren, B. A. (2021). Determinants of customer satisfaction in chatbot use: evidence from a banking application in Turkey. International Journal of Bank Marketing, 39(2), 294-311.

– Helbing, D. (2019). Societal, economic, ethical and legal challenges of the digital revolution: from big data to deep learning, artificial intelligence, and manipulative technologies (pp. 47-72). Springer International Publishing.

– Oracle. (2017). Data-driven tech trends shaping customer experience and you’re your business can quickly adapt.

– Sanny, L., Susastra, A., Roberts, C., & Yusramdaleni, R. (2020). The analysis of customer satisfaction factors which influence chatbot acceptance in Indonesia. Management Science Letters, 10(6), 1225-1232.

– Shaikh, I. A. K., Khan, S., & Faisal, S. (2023). Determinants affecting customer intention to use chatbots in the banking sector. Innovative Marketing, 19(4), 257-268.

– Trivedi, J. (2019). Examining the customer experience of using banking chatbots and its impact on brand love: The moderating role of perceived risk. Journal of internet Commerce, 18(1), 91-111.