فصلنامهٔ پدافند غیرعامل و امنیت (پژوهشی)
سال چهاردهم: شمارهٔ ۵۰- بهار ۱۴۰۴
صص: ۱۱۵ - ۱۵۵
تاریخ دریافت:۱۴۰۴/۰۷/۰۴ تاریخ پذیرش:۱۴۰۴/۱۰/۱۵

Quarterly of Passive Defense & Security
Vol.14, No.50,Spring 2025
P-P: 115 - 155

ارائه مدل امنیت سایبری در بانکداری الکترونیک با رویکرد آمیخته

حسین بابایی[۱]
منصوره علیقلی[۲]
داریوش غلام زاده[۳]
محمدرضا رادفر[۴]

چکیده

این پژوهش به‌صورت آمیخته (کیفی-کمی) انجام شد. روش تحقیق در بخش کیفی برمبنای هدف، بنیادی بود. تحلیل داده‌ها در بخش کیفی با استفاده از رویکرد گرندد‌تئوری انجام شد. جامعه آماری، شامل ۱۵ نفر از خبرگان حوزه بانکداری الکترونیک و امنیت سایبری بودند. روش نمونه‌گیری از نوع هدفمند بود. ابزار گردآوری داده، مصاحبه‌های نیمه‌ساختاریافته با پرسش‌های نیمه‌باز پاسخ بود. روش تحقیق در بخش کمی از نظر هدف، کاربردی (در بانک ملت) بود و از منظر اجرا از نوع توصیفی پیمایشی بود. برای تحلیل داده‌ها از روش معادلات ساختاری استفاده شد. جامعه آماری، شامل کلیه کاربران استفاده‌کننده از بانکداری الکترونیک بانک ملت بود. جهت تعیین حجم نمونه از فرمول کوکران در جوامع نامحدود استفاده شد که برابر با ۳۸۴ نفر بودند. روش نمونه‌گیری از نوع تصادفی بود و از پرسشنامه محقق‌ساخته استفاده گردید. در این تحقیق، نتایج داده‌های کیفی به نتایج داده‌های کمی در توسعه و آزمون الگو کمک کرد. بررسی مطالعات نشان‌داد که شکاف نوظهوری بین اقدامات بانک‌ها و انتظارات کاربران وجود دارد و در تحقیقات موجود تأثیر برخی از فنّاوری‌های جدید در بانکداری الکترونیک بر امنیت سایبری بررسی نشده است. این پژوهش، با شناسایی عوامل و شرایط مؤثر و تعیین

۱. گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
hossein.babaee@iau.ac.ir
۲. گروه مدیریت بازرگانی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران (نویسنده مسئول)
man.aligholi@iau.ac.ir
۳. گروه مدیریت دولتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایرانd.gholam@iau.ac.ir
۴. گروه مدیریت مالی و حسابداری، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایرانradfar@iau.ac.ir

متغیرهای مهم امنیت سایبری، این شکاف را برای اقدامات بانک‌ها در کاهش خطرهای امنیت سایبری برای کاربران، پر کرد و درنهایت یک الگوی امنیت سایبری جامع، کارآمد و بومی را برای بانکداری الکترونیک ارائه کرد که ضمن پوشش ابعاد فنی، مدیریتی و انسانی بتواند اعتماد مشتریان را افزایش داده و هزینه‌ها را کاهش دهد. نتایج نشان‌داد که استفاده از فنّاوری‌های نوین مانند بلاک‌چین و یادگیری ماشین، به همراه شناسایی رفتارهای کاربران و فرهنگ سازمانی، می‌تواند به بهبود امنیت و افزایش اعتماد مشتریان به خدمات بانکداری الکترونیک کمک کند.

کلیدواژگان: بانکداری الکترونیک، امنیت سایبری، تهدیدهای سایبری، فنّاوری‌های نوین، الگوی پارادایمی.

۱- مقدمه

بانک‌های سنتی مملو از مکانیسم‌های مالی متعارف هستند که برای به حداقل رساندن هزینه‌ها به روشی پایدار، تحت‌فشار زیادی قرار می‌گیرند (نجف و همکاران[1]، ۲۰۲۰). در دهه گذشته، نوآوری‌های مبتنی بر فنّاوری در امور مالی، دسترسی مصرف‌کننده به بسیاری از خدمات مالی را افزایش داده است (کیم و همکاران[2]، ۲۰۱۵). بانک‌های سنتی پس از همکاری با شرکت‌های فین‌تک در برابر نفوذهای سایبری آسیب‌پذیرتر می‌شوند (کرآدو و همکاران[3]، ۲۰۲۰).

با آنلاین شدن بیشتر سرویس‌ها و فراگیرشدن داده‌ها، امنیت داده‌ها یک چالش بزرگ برای بانک‌ها است (الدحیدآوری و همکاران[4]، ۲۰۲۰). تحول دیجیتال رو به رشد بخش بانکداری، باعث افزایش سطح حمله احتمالی به این صنعت شده است. این تحول بانک‌ها را در معرض افزایش سطح فعالیت‌های تهدید سایبری قرارداده است (کرائوس و همکاران[5]، ۲۰۲۱). حملات سایبری به مؤسسات مالی در سال‌های اخیر افزایش یافته است. اگرچه آن‌ها از اواخر دهه ۲۰۰۰ وجود داشته‌اند، اما این حملات سایبری از سال ۲۰۱۷

1. Najaf, K., Schinckus, C., Mostafiz, M. I., & Najaf, R.
2. Kim, Y., Park, Y. J., Choi, J., & Yeon, J.
3. Creado, Y., & Ramteke, V.
4. Aldahidhavi, H. M. K., Abdulreza, J. Z. S., Sebai, M., & Harjan, S. A.
5. Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N.

در حال افزایش است (سادلاکوسکی و همکاران[1]، ۲۰۱۷). بخش بزرگی از حملات سایبری تأثیر محدودی دارد و تنها بر یک یا چند نفر تأثیر می‌گذارد؛ اما در دهه گذشته، چند حمله سایبری در مقیاس بزرگ در بخش مالی شناسایی شده است که تأثیرات قابل‌توجهی در کوتاه‌مدت و بلندمدت داشته است (پارلور و همکاران[2]، ۲۰۱۸).

استفاده گسترده از فنّاوری‌های دیجیتال، نفوذ و مقیاس حملات سایبری را افزایش داده است که تهدیدی قابل‌توجه برای امنیت و حریم خصوصی داده‌های مشتریان در کانال‌های دیجیتال است (وورهیس و همکاران[3]، ۲۰۲۴). علاوه براین، هزینه تأمین امنیت داده‌های مشتریان در کانال‌های مالی دیجیتال می‌تواند از هزینه ارائه خدمات مالی دیجیتال بیشتر باشد و می‌تواند پیامدهای جدی برای کارایی و سودآوری ارائه‌دهندگان مالی دیجیتال داشته باشد (ویدودو و همکاران[4]، ۲۰۲۰). همچنین، اصلاحات مالی و بانکی می‌تواند به ارائه بهتر، ایمن و نوآورانه مالی دیجیتال به کاربران کمک کند (شیخ و همکاران[5]، ۲۰۲۳). به همین دلیل داشتن برنامه‌های مؤثر امنیت سایبری در بانکداری مهم‌تر از گذشته شده است (لیم و همکاران[6]، ۲۰۲۱).

علی‌رغم پژوهش‌های بسیار پیرامون مسئلهٔ امنیت سایبری در بانکداری الکترونیک، با توجه به‌سرعت بالای تغییرات و به‌روز پدیده‌های جدید و همچنین بر اساس مشاهدات تجربی در خصوص امنیت سایبری در بانکداری الکترونیک در شرایط عدم اطمینان موجود شکاف مطالعاتی وجود دارد. لذا با توجه به اهمیت موضوع پژوهش، محقق کوشیده است تا الگوی امنیت سایبری در بانکداری الکترونیک را مورد واکاوی قرار دهد.

۲- بیان مسئله و ضرورت

پژوهش‌ها نشان‌داده‌اند که امنیت سایبری، عامل کلیدی موفقیت بانکداری الکترونیک محسوب می‌شود و از سوی دیگر، گذرگاهی برای دست‌یابی به ارتقای اثربخشی سازمانی و تعالی آینده بانک‌ها فراهم می‌آورد. حال‌آنکه علی‌رغم پژوهش‌های

1. Sadlakowski, D., & Sobieraj, A.
2. Parlour, Richard & Bouyon, Sylvain & Krause, Simon
3. Van Voorhis, C., Hatcher, W., Kalat, T., Wang, Y., & Hammad, E.
4. Widodo, D. P., Syah, T. Y. R., & Negoro, D. A.
5. Shaikh, A. A., Glavee-Geo, R., Karjaluoto, H., & Hinson, R. E.
6. Tristan Lim, Patrick Thang

فـراوان در خصوص در بانکداری الکترونیک، هنوز فقدان بررسـی تأثیر برخی از پدیده‌های جدید سـازمانی براین رویکرد مشـهود اسـت. همچنین پدیده امنیت سایبری و نقش آن در توسعه این رویکرد نیز ازجمله عواملی است که کمتر موردتوجه قرار گرفته است.

بانکـداری الکترونیـک به‌دلیـل حجـم بـالای تراکنش‌هـای مالـی و اطلاعـات محرمانه مشـتریان، یکـی از پرخطرتریـن و حسـاس‌ترین حوزه‌هـا در بحـث امنیـت سـایبری اسـت. افزایـش حملات سـایبری به صنعت بانکـداری الکترونیک، نه‌تنها موجب خسـارت مالی می‌شـود بلکـه باعث کاهـش اعتماد مشـتریان می‌شـود. همچنین ضعف در پیاده‌سـازی راهبردهای امنیتی باعث آسـیب‌پذیر شـدن سامانه‌های بانکی در برابر تهدیدات سایبری می‌شـوند. توسـعه بانکداری الکترونیک با اسـتفاده از فنّاوری‌های نوین، سـطح تهدیدات سایبری را افزایش می‌دهد که نیازمند طراحی و توسعه الگوی امنیتی نوین و بومی است.

حملات سایبری به برخی از بانک‌های ایرانی باعث از دسترس خارج‌شدن حساب‌ها و افشـای اطلاعـات مشـتریان شـد کـه حفـظ امنیـت داده‌هـا و تراکنش‌هـای مالـی بـرای بانک‌های ایرانی به چالشی بزرگ تبدیل کرده است. از طرفی افزایش وابستگی به بانکداری الکترونیک در ایران که جرائم سـایبری را شـدت بخشیده اسـت و تهدید قابل‌توجهی برای حفظ اطلاعات خصوصی مشتریان در ایران به وجود آورده است.

چالـش پیـش‌رو در تحقیـق حاضر، بـا توجه به آسـیب‌پذیری چارچوب‌هـای داده‌های دیجیتالی، ازجمله خطر حمله، سرقت و کلاه‌برداری از سوی هکرها (و سایر فعالیت‌های مجرمانه سایبری) نقش برجستهٔ امنیت سایبری در بانکداری الکترونیک است. نتایج این پژوهـش می‌توانـد نقـش مؤثـری در ادبیات پژوهش مربـوط به امنیت سـایبری در بانکداری الکترونیـک داشـته باشـد و از سـوی دیگـر، مسـیری جدیـد درزمینـهٔ بحـث و بررسـی در موضوعـات فرایند ارزیابی امنیت سـایبری در بانکـداری الکترونیک فراهم آورد. همان‌گونه کـه مـرور ادبیات نشـان‌داد، تاکنـون پژوهش‌های بسـیاری به‌صـورت مسـتقل در خصوص توسـعهٔ امنیـت سـایبری در بانکـداری الکترونیک انجام شـده اسـت، اما به نظر می‌رسـد، تاکنون پژوهشـی که به‌صورت مسـتقیم با موضوع پژوهش حاضر مرتبط باشـد، انجام نشده اسـت؛ بنابرایـن شـکاف نظـری در تحقیقـات، وجود یـک الگو اسـت که بتوانـد بانکداری الکترونیک را از منظر امنیت سایبری مورد ارزیابی قرار دهد.

با توجه به مباحث مطرح شده، مسئله اصلی این پژوهش این است که: چگونه می‌توان یک الگوی امنیت سایبری جامع، کارآمد و بومی را برای بانکداری الکترونیک توسعه داد که ضمن پوشش ابعاد فنی، مدیریتی و انسانی بتواند اعتماد مشتریان را افزایش داده و هزینه‌ها را کاهش دهد؟

۳- سؤالات پژوهش

۱- متغیرهای امنیت سایبری در حوزه بانکداری الکترونیک کدامند؟

۲- میزان تأثیر متغیرهای شناسایی شده در الگوی امنیت سایبری چقدر است؟

۳- آیا الگوی امنیت سایبری در بانکداری الکترونیک از اعتبار برخوردار است؟

۴- مبانی نظری

بانکداری الکترونیک به ارائه خدمات بانکداری از طریق اینترنت به‌وسیله رایانه شخصی یا سایر تجهیزات با قابلیت دسترسی به اینترنت اشاره دارد. درواقع بانکداری الکترونیک یکپارچه‌سازی بهینه همه فعالیت‌های یک بانک از طریق به‌کارگیری فنّاوری اطلاعات است که امکان ارائه کلیه خدمات موردنیاز مشتریان را بدون حضور فیزیکی فراهم می‌کند (شاکیل و همکاران[1]، ۲۰۲۰).

مشتریان تلاش می‌کنند عادت‌ها، رفتارها و نحوهٔ ارتباط خود با ارائهٔ خدمات بانکداری اینترنتی را تغییر دهند؛ بنابراین کیفیت خدمات در صنعت بانکداری اینترنتی مهم است. در بستر اینترنت، کیفیت خدمات الکترونیکی به‌منزلهٔ ارزیابی و تصمیم‌گیری کلی مصرف‌کننده در مورد کیفیت خدمات ارائه‌شده از طریق اینترنت تعریف می‌شود. کاربران در صورتی سامانه‌های بانکداری الکترونیک را می‌پذیرند و به آن اعتماد می‌کنند تنها اگر مشاهده نمایند که سامانه امن است، ازاین‌رو امنیت نقش مهمی در احساس امنیت آن‌ها بازی می‌کند. (کنی و همکاران[2]، ۲۰۰۵)

امنیت ادراک‌شده از خدمات الکترونیک، به امنیت و قابلیت اعتماد معاملات و تبادلات الکترونیکی اشاره دارد. بسیاری از پژوهشگران متغیر امنیت ادراکی را به‌عنوان یکی از عوامل بااهمیت در پذیرش فنّاوری شناسایی کرده‌اند. (باطنی و همکاران، ۱۳۹۰)

1. Shakeel, waria et al.
2. Kenney, Martin & Patton, Donald

امنیت سایبری مجموعه ابزارها، سیاست‌ها، مفاهیم امنیتی، اعمال امنیتی، رویکردهای مدیریت بحران، آموزش و فنّاوری‌هایی است که در راستای دردسترس‌بودن، مورداطمینان بودن و صحت اطلاعات است که به‌منظور حفاظت از فضای سایبری و دارایی کاربران و سازمان‌ها به کار می‌رود. (عسکری و همکاران، ۱۳۹۹)

در این تحقیق به مروری بر سرعت افزایش شدت جرائم سایبری در بانک و رایج‌ترین تهدیدات سایبری که بر بانکداری الکترونیک تأثیر می‌گذارد، پرداخته شد و سپس میزان تأثیر متغیرهای امنیت سایبری در بانکداری الکترونیک اندازه‌گیری شد و درنهایت الگوی نهایی ارائه گردید. لذا با ارائهٔ الگوی بر اساس نظرات خبرگان این صنعت، برای استفاده بانک از فنّاوری اطلاعات و ارتباطات برای ارائه خدمات الکترونیک به مشتریان، می‌توان سرمایه‌گذاری در این حوزه را هدفمند نموده و منجر به کاهش حملات سایبری، جذب مشتریان بیشتر، کاهش هزینه‌ها، افزایش درآمدها و افزایش سودآوری بانک‌ها گردد.

۵- پیشینه پژوهش

سله و کوِندا[1] (۲۰۲۵) در پژوهشی با عنوان آیا تهدیدها و خطرهای امنیت سایبری بر پذیرش بانکداری دیجیتال تأثیر دارند؟ یک مرور نظام‌مند ادبیات» با هدف شناسایی تهدیدهای امنیت سایبری که مانع پذیرش بانکداری دیجیتال می‌شوند و ارائه راهبردهای پایدار برای مقابله با این تهدیدها در صنعت بانکداری انجام دادند. یافته‌ها نشان‌دادند که ارتقای دانش امنیتی، به‌روزرسانی فنّاوری‌های حفاظتی و به‌کارگیری راهکارهای آموزشی از مؤثرترین عوامل در توسعه امنیت سایبری در بانکداری الکترونیک هستند و می‌توانند زمینه‌ساز پذیرش گسترده‌تر خدمات دیجیتال در نظام بانکی باشند.

آیینادیس و همکاران[2] (۲۰۲۵) در پژوهشی با عنوان بررسی عوامل مؤثر بر پذیرش بانکداری الکترونیکی در اتیوپی از دیدگاه مشتریان با هدف تحلیل متغیرهایی که بر پذیرش و استفاده از خدمات بانکداری الکترونیکی اثر می‌گذارند، مطالعه‌ای پیمایشی انجام دادند. تحلیل نظری پژوهش بر پایه الگوی پذیرش فنّاوری و چارچوب فنّاوری-سازمان-محیط انجام شد که در آن تأکید بر نقش زیرساخت‌های فنّاورانه، حمایت‌های

1. Cele, N. N., & Kwenda, S
2. Ayinaddis, S. G., Mirete, T. G., & Getahun, B. W

سازمانی و محیطی و نگرش فردی نسبت به فنّاوری است. یافته‌های پژوهش حاکی از آن بود که ارتقای امنیت سایبری در بانکداری الکترونیک به‌طور غیرمستقیم از طریق بهبود سهولت استفاده، افزایش سازگاری سامانه‌ها با نیازهای کاربران، توسعه دسترسی پایدار به خدمات و تقویت سودمندی ادراک‌شده محقق می‌شود، زیرا این عوامل اعتماد مشتریان را نسبت به سامانه‌های الکترونیکی افزایش داده و آسیب‌پذیری ناشی از خطاهای انسانی و تهدیدهای سایبری را کاهش می‌دهند.

الخواجه و ابوروب[1] (۲۰۲۵) در پژوهشی با عنوان زنجیره بلوکی برای ایمن‌سازی ذخیره‌سازی داده‌ها در خدمات بانکداری دیجیتال به بررسی کارکرد فنّاوری زنجیره بلوکی به‌عنوان راهکاری نوین برای ارتقای امنیت داده‌ها در بانکداری الکترونیک پرداختند. بر اساس تحلیل نتایج، عوامل مؤثر بر توسعه امنیت سایبری در بانکداری الکترونیک شامل به‌کارگیری معماری غیرمتمرکز برای حذف نقاط آسیب‌پذیر، استفاده از الگوریتم‌های رمزنگاری پیشرفته برای تضمین تمامیت داده‌ها، پایبندی به استانداردهای بین‌المللی حریم خصوصی و ایجاد چارچوب‌های اجرایی برای پیاده‌سازی عملی زنجیره بلوکی در محیط بانکی است. این عوامل به شکل هم‌افزا موجب افزایش تاب‌آوری نظام بانکی در برابر تهدیدات سایبری، ارتقای شفافیت در مدیریت داده‌ها و شکل‌گیری الگوهای نوین و پایدار امنیت سایبری در بانکداری الکترونیک می‌شوند.

بیشاکو و همکاران[2] (۲۰۲۵) در پژوهشی با عنوان چالش‌ها، نگرانی‌های امنیتی و راهبردهای کاهش خطر در بانکداری الکترونیکی با هدف بررسی ابعاد مختلف تهدیدهای امنیتی ناشی از دیجیتالی‌شدن خدمات بانکی و ارائه راهکارهای مدیریتی و فنّاورانه برای کاهش این تهدیدها به مطالعه پرداختند. در تحلیل نهایی، توسعهٔ امنیت سایبری در بانکداری الکترونیک در گرو چند عامل کلیدی دانسته شده است که شامل ایجاد زیرساخت‌های فنی پایدار، استقرار نظام‌های احراز هویت چندلایه، آموزش و آگاهی‌بخشی مستمر به مشتریان، تدوین چارچوب‌های نظارتی دقیق و همکاری میان نهادهای مالی و نهادهای تنظیم‌گر است. این عوامل با تقویت فرهنگ امنیت اطلاعات و

1. Al-khawaja, H. A., & Aburub, F. A
2. Bixhaku, S., Polo, A., Zyberi, I., & Caca, E

ارتقای اعتماد کاربران، نقش تعیین‌کننده‌ای در افزایش تاب‌آوری سایبری و پایداری نظام بانکداری الکترونیکی دارند.

ییو تینگ یان آزورا و همکاران[1] (۲۰۲۵) در پژوهشی با عنوان یک چارچوب مدیریت خطر امنیت سایبری یکپارچه برای سامانه‌های بانکداری آنلاین، چارچوبی ارائه دادند که شامل یک الگوی تهدید، یک الگوی خطر، یک روش‌شناسی جامع مدیریت خطر و وظایف از پیش تعریف‌شده برای مقابله است. این چارچوب در طول مراحل شناسایی تهدید و تحلیل آسیب‌پذیری، سناریوهای حمله بالقوه و تأثیرات احتمالی آن‌ها با استفاده از رویه‌های از پیش تعریف‌شده و با درنظرگرفتن زمینه ارزیابی می‌کند و فرایند ارزیابی، خطرات امنیت سایبری را کمّی می‌کند و استراتژی‌های کاهش مناسب را برای رسیدگی به تهدیدها و خطرات شناسایی شده تسهیل می‌کند.

آدِدوییِن و همکاران[2] (۲۰۲۴) در یک تحقیق با عنوان خطرات امنیت سایبری در بانکداری آنلاین، کاربرد استراتژی‌های پیشگیرانه را موردبررسی قراردادند. در تحقیق مذکور به بررسی ابعاد مختلف امنیت سایبری در صنعت بانکداری پرداخته است. با توجه به افزایش استفاده از بانکداری آنلاین و هم‌زمان با آن افزایش جرائم سایبری، این تحقیق به‌دنبال روشن‌کردن چشم‌انداز فعلی امنیت سایبری، ارزیابی کارآمدی چارچوب‌های موجود و پیشنهاد تقویت‌های استراتژیک برای تقویت دفاع‌های دیجیتال بوده است.

موهونا[3] (۲۰۲۴) در تحقیقی با عنوان تهدیدات نوظهور امنیت سایبری در بخش بانکداری؛ نقاط ضعف و راه‌حل‌ها را از منظر قانون موردبررسی قراردادند. تحقیق مذکور به بررسی تهدیدات جدید امنیت سایبری در صنعت بانکداری پرداخته و نقاط ضعف موجود در این بخش را شناسایی کرد. هدف این تحقیق، ارتقاء آگاهی در مورد چالش‌های موجود و ارائه پیشنهادهایی برای بهبود قوانین و مقررات امنیت سایبری در بانکداری بود.

سلواراج[4] (۲۰۲۱) به بررسی نقش امنیت سایبری با کمک هوش مصنوعی (AI) در پیشگیری و کشف کلاه‌برداری مالی پرداخت. نکته برجسته تحقیق او درک امنیت سایبری، شامل ابزارها، برنامه‌ها، چالش‌ها و شرایط نظارتی آن است که بر عملکرد آن تأثیر می‌گذارد.

1. Yiu Ting Yan Azura, Muhammad Ajmal Azad & Yussuf Ahmed
2. Adedoyin Tolulope Oyewole et al.
3. Mehenaj Jerin Mohona
4. Selvaraj Nagasundari

الدحیدهاوی و همکاران (۲۰۲۰) در مقاله‌ای با عنوان تحلیل اثرات متغیرهای فین‌تک بر امنیت سایبری، میزان تأثیر متغیرهای فین‌تک را بر امنیت سایبری به‌عنوان متغیر وابسته اندازه‌گیری کردند. آن‌ها نشان‌دادند که حملات سایبری به‌نوبه خود منجر به تلاش‌های زیادی توسط متخصصان و محققان برای معرفی فنّاوری‌های هوشمند مانند هوش مصنوعی و سایر ابزارها برای تجزیه‌وتحلیل و دانستن چگونگی مقابله با حملات سایبری قبل از وقوع آن شد.

نجف و همکاران (۲۰۲۰) در مطالعه‌ای با عنوان مفهوم‌سازی خطر امنیت سایبری پایداری شرکت‌های فین‌تک و بانک‌ها نشان‌دادند که خطر امنیت سایبری آشکار مرتبط با شرکت‌های فین‌تک تأثیر منفی بر بانک‌های شریک دارد. خطر امنیت سایبری نه‌تنها زیان مالی قابل‌توجهی را شامل می‌شود، بلکه اعتماد سرمایه‌گذاران به شرکت‌های فین‌تک و شرکت‌های شریک آن‌ها (مؤسسات مالی) را نیز از بین می‌برد.

وجدانی و همکاران (۱۴۰۳) در تحقیقی به بررسی اثرگذاری حریم خصوصی و امنیت خدمات بانکداری الکترونیک بر وفاداری مشتریان بانکی با تأکید بر قابلیت اطمینان پرداختند و برای این منظور از روش معادلات ساختاری استفاده کردند. نتایج حاصل نشان از تأیید فرضیه‌های مقاله در سطح اطمینان ۹۵ درصد داشته است.

موسوی و همکاران (۱۴۰۳) در تحقیق به بررسی تأثیر ابعاد عینی امنیت سامانه‌های پرداخت الکترونیکی با واسطه درک مشتریان بانک ملی از امنیت و اعتماد پرداختند. در تحقیق مذکور، ۹ فرضیه مطرح شد که نتایج آزمون فرضیه‌های اصلی الگوی مفهومی در قالب الگوی ساختاری نشان‌داد، متغیرهای فرایندهای تراکنش و حفاظت فنی بر امنیت ادراک‌شده و متغیرهای فرایندهای تراکنش و بیانیه امنیت بر اعتماد ادراک‌شده و متغیر اعتماد ادراک‌شده بر میزان استفاده و متغیر امنیت ادراک‌شده بر اعتماد ادراک‌شده اثر مثبت و معنادار دارند.

آپرناک و همکاران (۱۴۰۱) در مقاله رابطه بین امنیت ادراک‌شده و اعتماد مشتریان به سامانه بانکداری الکترونیک مبتنی بر رویکرد NFC-Mobile نشان‌دادند که امنیت در رابطه بین ابعاد عینی و میزان استفاده از سامانه پرداخت الکترونیک واسطه‌گری می‌کند. همچنین اعتماد رابطه بین دو بعد حفاظت‌های فنی و فرایندهای تراکنش با میزان

استفاده از سامانه پرداخت الکترونیک را میانجی‌گری می‌کند ولی نقش واسط این بعد بین بیانیه‌های امنیتی و میزان استفاده از سامانه پرداخت الکترونیک غیر معنادار بود.

طهماسبی و همکاران (۱۴۰۰) در مقاله خود با نام ارائه چارچوب همکاری راهبردی بین نظام بانکی خصوصی و فین‌تک‌ها در ایران، چارچوب همکاری راهبردی بین نظام بانکی خصوصی و فین‌تک‌ها را ارائه دادند. بر اساس یافته‌های پژوهش، ابهامات محیطی می‌تواند زمینه را برای همکاری راهبردی طرفین فراهم کند که در آن از یک‌سو فرصت‌سنجی فین‌تک، رفتار دیجیتالی مشتریان، نیازسنجی مشتریان، شناخت مشتریان از فین‌تک، حفظ محیط رقابتی، اصول و قوانین مالی اسلامی و ارزش‌گذاری دقیق کسب‌وکارها به‌عنوان شرایط علّی و از سوی دیگر عوامل درونی نظام بانکی خصوصی به‌عنوان شرایط مداخله‌گر مؤثر است. این همکاری راهبردی برای طرفین رشد و پیامدهای مالی، فرایندی، عملیاتی و ارتباطی به همراه خواهد داشت.

تفاوت الگوی پژوهش حاضر با الگوهای موجود

- در بیشتر الگوهای موجود، متغیرها از طریق پژوهش‌های پیشین به‌دست‌آمده است نه از طریق مصاحبه با خبرگان.
- در الگوهای موجود، برخی از مهم‌ترین متغیرهای شرایط علی در نظر گرفته نشده‌اند. در پژوهش حاضر فنّاوری‌های جدید و پیشرفته، وضعیت داده‌ها، تهدیدات سایبری، رفتار کاربر، عوامل نگرشی در قالب مقوله شرایط علی مطرح شده‌اند.
- در الگوهای موجود، برخی از مهم‌ترین متغیرهای شرایط زمینه‌ای در نظر گرفته نشده‌اند. در پژوهش حاضر متغیرهای قوانین و مقررات، فرهنگ سازمانی، زیرساخت‌های فنّاورانه، صنعت بانکداری، اقتصاد دیجیتال در قالب مقوله شرایط زمینه‌ای مطرح شده‌اند.
- در الگوهای موجود، برخی از مهم‌ترین متغیرهای شرایط مداخله‌گر در نظر گرفته نشده‌اند. در پژوهش حاضر متغیرهای سامانه حفاظتی و امنیتی، رویه امنیت پیشرفته، پروتکل و استانداردهای امنیتی، وضعیت مدیریت خطر و پاسخ به بحران در قالب شرایط مداخله‌گر مطرح شده‌اند.

- با توجه روش تحقیق در برخی از الگوهای موجود، راهبردها در نظر گرفته نشدند. در پژوهش حاضر متغیرهای حفاظت از داده‌ها، آموزش و آگاهی، مدیریت آسیب‌پذیری، نظارت و گزارش‌دهی، سامانه داده‌پردازی، پشتیبان‌گیری و بازیابی، به‌کارگیری تکنیک‌های مدرن به‌عنوان راهبردها در نظر گرفته شدند.
- پیامدهای ارائه‌شده در برخی از الگوهای موجود با پیامدهای الگوی پژوهش حاضر متفاوت است. در پژوهش حاضر متغیرهای خشنودی مشتری، امنیت اطلاعات، مدیریت هزینه، بهره‌وری اقتصادی به‌عنوان پیامدها در نظر گرفته شدند.
- در برخی از الگوهای موجود، امنیت سایبری به‌عنوان مقوله مرکزی مطرح نشده است. در پژوهش حاضر، متغیر امنیت سایبری به‌عنوان مقوله مرکزی در نظر گرفته شده است.

۶- روش‌شناسی پژوهش

این پژوهش به‌صورت آمیخته (کیفی-کمی) انجام شد. روش تحقیق در بخش کیفی برمبنای هدف، بنیادی بود. تحلیل داده‌ها در بخش کیفی با استفاده از رویکرد گرندد تئوری انجام شد. جامعه آماری در این بخش، شامل ۱۵ نفر از خبرگان حوزه بانکداری الکترونیک و امنیت سایبری در بانک ملت، خبرگان امنیت سایبری در وزارت نفت و خبرگان دانشگاهی بودند. روش نمونه‌گیری از نوع هدفمند بود. ابزار گردآوری داده در بخش کیفی، مصاحبه‌های نیمه‌ساختاریافته با پرسش‌های نیمه‌باز پاسخ بود. برای تحلیل محتوای کیفی از نرم‌افزار ATLAS TI استفاده شد.

ازآنجاکه پرسشنامه مصاحبه، مبتنی بر مقایسه زوجی تمامی عناصر با یکدیگر بود، احتمال اینکه یک متغیر در نظر گرفته نشود صفر است؛ بنابراین چون تمامی معیارها در این سنجش موردتوجه قرار گرفت و طراح قادر به جهت‌گیری خاصی در طراحی سؤالات نبود، بنابراین این نوع پرسشنامه، فی‌نفسه از روایی برخوردار بود. به‌دلیل اینکه در پرسشنامه تمامی عوامل الگو در نظر گرفته شد و با یکدیگر مقایسه گردید، لذا تمام احتمالات مرتبط با در نظر نگرفتن یک متغیر از بین رفت. از طرفی چون پرسشنامه تمامی معیارها را به‌صورت دو به دو مقایسه و سنجش کرد، لذا حداکثر سؤالات ممکن با ساختاری مطلوب از مخاطب پرسیده شد، بنابراین نیازی به سنجش پایایی وجود نداشت.

در بخش کمی ازآنجاکه تمام اهداف این تحقیق در راستای کسب دانش لازم جهت برطرف‌کردن نیازهای شناخته‌شده در بانک ملت بود، روش تحقیق در بخش کمی از نظر هدف، کاربردی بود و از منظر اجرا از نوع توصیفی پیمایشی بود. برای تحلیل داده‌ها در بخش کمی از روش الگوسازی معادلات ساختاری استفاده شد. جامعه آماری در این بخش، شامل کلیه کاربران استفاده‌کننده از بانکداری الکترونیک از درگاه بانک ملت بود. جهت تعیین حجم نمونه از فرمول کوکران استفاده شد. بر اساس فرمول کوکران در جوامع نامحدود و با توجه به اینکه استفاده‌کنندگان بانکداری الکترونیک نامحدود هستند، نمونه آماری بخش کمی برابر ۳۸۴ نفر بودند. روش نمونه‌گیری از نوع تصادفی بود. در بخش کمی، از پرسشنامه محقق‌ساخته استفاده گردید. در این پرسشنامه از طیف پنج‌تایی لیکرت (از کاملاً بی‌اهمیت تا کاملاً بااهمیت) برای سنجش میزان اهمیت هر یک از ویژگی‌ها و طیف پنج‌تایی لیکرت از (کاملاً مخالفم تا کاملاً موافقم) مورداستفاده قرارمی‌گیرد. شکل کلی و امتیازبندی این طیف برای سؤالات به‌صورت زیر است: کاملاً مخالفم، مخالفم، نظری ندارم، موافقم، کاملاً موافقم. درنهایت با روش معادلات ساختاری، الگوی تحقیق آزمون شد. از نرم‌افزار Smart PLS برای تدوین الگوی تحلیل عاملی تأییدی و معادلات ساختاری و از نرم‌افزار SPSS برای آمار توصیفی استفاده شده است. در این تحقیق، نتایج داده‌های کیفی به نتایج داده‌های کمی در توسعه یا آزمون ابزار کمک می‌کند.

با توجه به اینکه در این پژوهش از نظرات ۱۵ متخصص بهره گرفته شده بود، مقدار شاخص CVR باید بیشتر از ۰٫۴۹ باشد، ازآنجاکه مقدار این شاخص برای تمامی گویه‌ها بیشتر از ۰٫۴۹ بود، بنابراین از روایی محتوایی برخوردار بود. حداقل مقدار قابل‌قبول برای شاخص CVI باید برابر با ۰٫۷۹ باشد، با توجه به اینکه در این پژوهش مقدار این شاخص برای تمامی گویه‌ها بیشتر از ۰٫۷۹ بود، بنابراین از روایی محتوایی برخوردار بود. مقدار میانگین واریانس تبیین شده برای سازه‌های الگوی بالاتر از ۰٫۵ شده است و نشان از تأیید روایی همگرا در الگو است. از دیگر شاخص‌های روایی همگرا شاخص رائو از نظر هنسلر و همکاران است که این شاخص نیز برای تمامی متغیرهای تحقیق بالاتر از ۰٫۶ بود. همچنین همه متغیرها روایی واگرای قابل‌قبولی داشتند. نتایج نسبت یکنواختی سازه‌های الگو نشان‌داد تمامی مقادیر از ۰٫۹۰ پایین‌تر بودند که بر اساس هنسلر و همکاران، روایی

واگـرا مـورد تأییـد اسـت. همچنین طبق شـاخص فورنل و لارکـر، در این پژوهش ریشـه دوم میانگین واریانس استخراج‌شـده (AVE) هر متغیر پنهان، از بالاترین همبسـتگی آن سـازه با سـایر سـازه‌های الگو بیشتر بود. ضریب آلفای کرونباخ به‌دست‌آمده برای تمام متغیرها بیشـتر از ۰٫۷ بـود، بنابرایـن همسـانی درونی بالایی بیـن گویه‌ها وجود دارد. شـاخص پایایی ترکیبـی بـرای تمامـی متغیرهای تحقیق از ۰٫۷ بزرگ‌تر بود و نشـان از پایایـی ابزار اندازه‌گیری دارد.

۷- یافته‌های پژوهش و تجزیه‌وتحلیل

ایـن بخـش بـه تجزیه‌وتحلیل اطلاعـات و نحوه اجـرای روش کیفی و کمـی اختصاص دارد.

بخش کیفی

بخـش کیفـی این مطالعه بر اسـاس دیدگاه ۱۵ نفر از خبرگان انجام شـده اسـت. از نظر جنسـیت ۱۳ نفـر مـرد و ۲ نفـر نیـز زن بودند. درنهایت ۴ نفر بین ۱۰ تا ۱۵ سـال سـابقه کاری داشته و ۱۱ نفر نیز بالای ۱۵ سال تجربه کاری داشتند.

بـرای تدویـن گراندد‌تئوری ۵ مرحله تحلیلی (و نه الزاماً متوالی) وجود دارد که درون این مراحـل ۹ گام دنبال می‌شـود: ۱-تدویـن طرح تحقیق ۲-گردآوری داده‌هـا ۳-تنظیم داده‌ها ۴-تحلیل داده‌ها ۵-مقایسه با متون.

در کدگـذاری بـاز، ابتدا داده‌هـای حاصل از مصاحبه‌ها به‌دقت موردمطالعه، بررسـی و تحلیل قرار گرفتند، سپس عمل مفهوم‌سازی صورت گرفت و به داده‌هایی که از نظر مفهوم شـبیه به یکدیگر بودند، با نام‌های متناسـب، برچسـب زده شـد. برچسـب‌گذاری کدها با اسـتناد به مصاحبه‌ها انجام‌شـده است و محققان سـعی کرده‌اند تا حد ضرورت به بینش افراد نسـبت به پاسخ‌داده‌شـده پایبند باشـند تا از هرگونه سـوگیری احتمالی و ناخواسته تا حـد امـکان جلوگیری شـود. محقق در تمـام فراینـد کدگذاری‌ها به حساسـیت نظری که از اصـول تحقیـق نظریه‌پـردازی داده‌بنیاد اسـت پایبند بوده اسـت و ایـن کار را جهت غنای هرچه بیشتر تحقیق انجام داده است.

نمونه کدها و مصاحبه‌های مرتبط در ادامه بیان شده است:

جدول ۱. نمونه کدهای شناسایی شده بر اساس مصاحبه

سؤالات مصاحبه	خبره	پاسخ خبره	کدهای شناسایی شده
سؤال اول) چه تحولاتی در تهدیدات سایبری در بانکداری الکترونیک در دوره اخیر مشاهده کرده‌اید؟	خبره اول	بحث سامانه عامل‌های بومی هست که ما واقعاً اینا رو نداریم و اینکه سیاست‌گذاری که میشه تا بخوان ابلاغ بشه تا بخوان برن خریداری بشه تا بیاد نصب شه تا پا یه جا پایلوت شه فلان شه یه سال دو سال طول می‌کشه ولی سیاست‌های امنیتی باید در لحظه انجام شود. توی بانک‌های الکترونیک خودتون می‌دونید زیرساخت‌های ما اغلب آمریکایی هست، مثلاً روتر سیسکو مال امریکاست. تو سازمانا همیشه اشخاص یا حالا کسایی هستند که اطلاعات میدن یعنی هر جای دنیا باشه این اتفاق میفته همیشه از اونجا بیشتر ضربه می‌خورن تا از بیرون بیشتر از داخله سازمان و نیاز به آموزش دارند. فرهنگی که در سازمان‌های ما وجود داره، اون بروکراسی اداری که هست برای تأیید که این باید تأیید کنه اون تأیید کنه اون فلان کنه اون رد میکنه جلسه بزار و فلان اینا باعث میشه که از این قافله ما دور بمونیم و ضربه بخوریم و فرهنگ امنیتی وجود نداره.	زیرساخت فنّاوری، بومی‌سازی فنّاوری، سیاست‌های امنیتی، تراکنش، سرور، آموزش کارکنان در زمینهٔ امنیت اطلاعات، فرهنگ سازمانی، فرهنگ امنیتی
	خبره هشتم	مهم‌ترین حملاتی که الان ما در حال حاضر داریم بحث حملات DOS و DDOS هست. بعد بحث حملات مرد میانی (MITM)، حملات فیشینگ، رو داریم انواع اقسام حملات حمله به رمز عبور، تزریق SQL، از حملاتی که خیلی رایجه توی بانک سال.	حملات DOS و DDOS، حملات مرد میانی (MITM)، حملات فیشینگ، حمله به رمز عبور، تزریق SQL
سؤال فرعی از سؤال اصلی اول) چه اقداماتی را برای جایگزینی زیرساخت‌های غیربومی انجام دادید؟	خبره اول	این سیاست‌های داخلی بانک و سیاست‌های دولتی و بالادستی که به ما ابلاغ می‌شه که این محصول امریکایی اگر جایگزین داره شما نباید از آمریکایی استفاده کنید خب حالا از یه سری فایروال‌هایی استفاده کردیم که طراحی روسیه هستش طراحی چین هستش. فایروال‌هایی رو جاهای دیگه گذاشتیم، تقریباً دو ساله که محصول مک‌کافی که محصول کاملاً آمریکایی بود رو داریم یه جورایی کنار می‌ذاریم و محصول کسپر رو جاش می‌ذاریم که روسیه. این بحث روترها رو داریم چک می‌کنیم و تو بحث نرم‌افزاری اون آنتی‌ویروس‌هایی که آمریکایی هستش رو روسی می‌کنیم ولی میگم این برمیگرده بحث حالا اون حفره‌های ویندوز داستان‌های بالایی که استفاده می‌کنیم سخت‌افزاری مون درواقع زیرساخت و ساختار شبکه. درواقع حالا لایه‌هایی که باید حذف بشه اون به‌روزرسانی‌هایی که باید انجام بشه.	سیاست‌های داخلی بانک، سیاست‌های دولتی و بالادستی، زیرساخت و ساختار شبکه، محصولات بومی، فایروال، آنتی‌ویروس، به‌روزرسانی

سؤالات مصاحبه	خبره	پاسخ خبره	کدهای شناسایی شده
سؤال دوم) چگونه از رویکردهای فنّاورانه برای تشخیص و پیش‌بینی تهدیدات سایبری در بانکداری الکترونیک استفاده می‌کنید؟	خبره هفتم	رویکردهای یادگیری ماشینی و هوش مصنوعی و این‌ها برای تشخیص پیش‌بینی تهدیدات سایبری به ما کمک می‌کنه بر اساس رفتار خاص مشتری. مثلاً یه رفتار خاصی که قبلاً نبود، این مشتری همیشه ۸ صبح تا ۱۲ شب خرید می‌کرده یا این مشتری فقط از مثلاً بازار داخلی خرید می‌کنه و رفتار مشکوک شناسایی می‌شه. یه اتفاقی متفاوت که تو هیچ خوشه‌ای نشینه اولاً خوشه‌بندی بشن همه مشتری‌ها یا همه رفتارهای مشتری خوشه‌بندی بشه کلاسترینگ بشه بعد یهو یه چیزی در هیچ کلاستری که نشینه بهش میگن نقطه پرته این باید کمک می‌کنه به بررسی رفتار مشتری.	یادگیری ماشینی، هوش مصنوعی، رفتار مشتری، شناسایی رفتار مشکوک
	خبره هشتم	فنّاوری‌های مانند هوش مصنوعی، یادگیری ماشینی برای تشخیص و پیش‌بینی تهدیدات سایبری هست و ما یه سامانه‌ای داریم به اسم مدیریت امنیت اطلاعات که میاد لاگ‌ها رو جمع‌آوری می‌کنه تجزیه تحلیل می‌کنه گاهی اوقات میاد بر اساس امضاهایی (سیگنیچرهایی) که بهش دادیم میاد پیدا می‌کنه یه سری از حملات رو به شما اعلام می‌کنه. یه قسمت دیگه‌ای هستش به اسم تحلیل رفتار کاربر (UBA) میاد الگوهای مشکوک رو شناسایی می‌کنه و طبق اون میاد یه سری هشدار میده.	مدیریت امنیت اطلاعات، تحلیل رفتار کاربر، شناسایی الگوهای مشکوک
	خبره یازدهم	هوش مصنوعی و یادگیری ماشینی می‌تواند در تشخیص و پیش‌بینی تهدیدات مؤثر باشند. استفاده و به‌کارگیری الگوریتم‌های یادگیرنده در تجهیزات کنترل شبکه و دیواره‌های آتشین می‌توانند در حداقل‌ترین کارکرد خود، مانع حملات تکراری شوند و یا از حملات سطح ساده تا سطح میانه جلوگیری نمایند. ولی با توجه به هوشمندی نفوذگران و پیچیده شدن سازوکارهای حمله، هنوز راه زیادی جهت بلوغ هوش مصنوعی و یادگیری ماشین در این حوزه وجود دارد. عموماً هوش مصنوعی و یادگیری ماشین در تجهیزات یا سامانه‌هایی به نام اطلاعات امنیتی و مدیریت رویدادها به‌کارگیری می‌شوند.	هوش مصنوعی، یادگیری ماشینی، تجهیزات کنترل شبکه، دیواره‌های آتشین (فایروال)، اطلاعات امنیتی و مدیریت رویدادها
سؤال سوم) چه اقداماتی برای افزایش امنیت در تراکنش‌های مالی الکترونیکی بانکی انجام داده‌اید؟	خبره سوم	بانک می‌تونه درواقع با ایجاد امنیت‌های چندلایه نظیر کنترل دسترسی، رمزنگاری و تأیید تراکنش، امکان دسترسی به اطلاعات مشتریان رو برای غیرخودی یا غیرمشتری از بین ببره یعنی بتونه با ایجاد لایه‌های چندگانه امنیتی امکان نفوذ به این سامانه را مهیا نکنه یکی از این کارها، استفاده از روش بلاک چین برای ذخیره‌کردن اطلاعات مشتریان هستش.	کنترل دسترسی بر اساس نقش، رمزنگاری و تأیید تراکنش

سؤالات مصاحبه	خبره	پاسخ خبره	کدهای شناسایی شده
	خبره دهم	بانک‌ها و سازمان‌های بانکداری الکترونیک از رویکردهای فنّاورانه مانند هوش مصنوعی و یادگیری ماشین برای تشخیص و پیش‌بینی تهدیدات سایبری استفاده می‌کنند. این فنّاوری‌ها به آن‌ها کمک می‌کنند تا به‌طور خودکار الگوهای مشکوک را تشخیص داده و تهدیدات امنیتی را پیش‌بینی کنند. نمونه‌هایی از استفاده این فنّاوری‌ها در بانکداری الکترونیک عبارتند از: ۱. تشخیص نفوذ ۲. تشخیص الگوهای مشکوک ۳. تحلیل داده‌های بزرگ ۴. پیش‌بینی رفتارهای مشکوک	هوش مصنوعی، یادگیری ماشین، تشخیص نفوذ، تشخیص الگوهای مشکوک، تحلیل داده‌های بزرگ، رفتارهای ناهنجار کاربران
سؤال فرعی از سؤال اصلی دوم) برای کشف تقلب چه سازوکاری در بانک وجود دارد؟	خبره اول	درواقع سازوکاری هست که میاد بازرسی کل اینا رو نظارت می‌کنه بر رفتارهای کاربران و رفتارهایی که مشکوک باشه بهش میگه چرا مثلاً از این حساب این حسابی که دو سال راکد بوده چرا الان داره کار می‌کنه و دو تا تراکنش می‌زنه دوباره میره تا یه سال دیگه دو تراکنش اون اختلاسه.	نظارت، شناسایی رفتارهای کاربر، ردگیری رفتار مشکوک، تراکنش مشکوک
سؤال چهارم) چگونه با چالش‌های مرتبط با حفاظت اطلاعات و حفظ حریم خصوصی مشتریان در برابر تهدیدات سایبری برخورد می‌کنید؟	خبره ششم	متأسفانه سامانه‌های بانکی ما به دلیل عدم نیازشون به اصطلاح رضایت مشتری خیلی تمایلی ندارند. چون مشتریاشون با همین اپلیکیشن‌ها و این روش‌ها و این به اصطلاح روالی که دارند راضی هستند مشتری خودش رو به اصطلاح ملزم به درخواست شاید هم مشتری‌های ما نمی‌دونن که روش‌های بانکداری الکترونیک یا سامانه بانکداری مجازی در دنیا چیه به همین‌ها قناعت می‌کنن. بهبود نگرش مشتری و اعتماد مشتری توی اون امنیتی که بانک می‌خواد داشته ایجاد کنه تأثیر داره چه در روش‌های پرداخت چه در روش‌های ارتباط مشتری با بانک چون خیلی ما فعالیت‌های گسترده‌ای نداریم با همین به اصطلاح نرم‌افزارهایی که داریم ما قناعت کردیم و شایدم یکی از دلایلش عدم به اصطلاح تجربه مثبت مشتری باعث شده که ما تو همین مقطع چندین و چندین ساله همچنان به اصطلاح بمونیم بله. مشتری نمی‌تونه کاری انجام بده بانک‌ها باید برای اطمینان بیشتر از رضایت مشتری و جذب مشتری و حفظ مشتری باید روش‌های فنّاورانه جدید را برای حفظ امنیت و حفظ اطلاعات شخصی مشتریان داشته باشد این. وظیفه بانکی که باید انجام بشه.	رضایت مشتری، بهبود نگرش مشتری، اعتماد مشتری، تجربه مثبت مشتری، حفظ اطلاعات شخصی مشتریان

سؤالات مصاحبه	خبره	پاسخ خبره	کدهای شناسایی شده
سؤال پنجم) چه استراتژی‌ها یا فرایندهایی برای آموزش و ارتقای آگاهی کارکنان درزمینهٔ امنیت سایبری به کار می‌برید؟	خبره اول	بخش آی تی بانک بهترین آموزش‌ها رو برای پیشگیری تهدیدات انتخاب می‌کنه و درواقع اون زیرمجموعه آی تی رو می‌فرسته یاد بگیرن و برای اینکه این کار کاملاً درست انجام شه از خود همون شرکت یه نفر به‌عنوان ناظر میاره مثلاً تو اداره کل که مطمئن شه این آموزش‌ها داره درست و کامل انجام می‌شه. توی بحث آموزش به نظر من بانک چیزی کم نمی‌ذاره بازخوردش یعنی خوب بود و بالاخره از هر ده تا کارشناسی که میاد یه نفرشون نخبه در میاد.	آموزش تخصصی، آموزش روش‌های پیشگیری تهدیدات، نظارت بر آموزش
	خبره دوازدهم	برای آموزش و ارتقاء آگاهی کارکنان درزمینهٔ امنیت سایبری، برخی از استراتژی‌ها و فرایندهای مؤثر عبارتند از: ۱. برگزاری دوره‌های آموزشی: برگزاری دوره‌های آموزشی با هدف آشنایی کارکنان با تهدیدات سایبری، روش‌های حفاظت اطلاعات و رفتارهای امنیتی موردنیاز است. این دوره‌ها باید به‌صورت منظم برگزار شوند تا کارکنان به طور دائمی با مفاهیم امنیت سایبری آشنا باشند. ۲. آزمون‌های آموزشی و فراگیری: برگزاری آزمون‌های آموزشی و فراگیری برای ارزیابی دانش و درک کارکنان از امنیت سایبری و اعمال اقدامات تصحیحی در صورت لزوم ازجمله روش‌های مؤثر برای ارتقاء آگاهی کارکنان است. ۳. ایجاد فرهنگ امنیتی: ایجاد فرهنگ و محیطی که اهمیت امنیت سایبری برای همه کارکنان واضح باشد، باعث افزایش اهمیت و توجه افراد به این موضوعات خواهد شد و آگاهی آن‌ها را ارتقا خواهد داد. ۴. آموزش در محیط‌های شبیه‌سازی: انجام آموزش‌های عملی و شبیه‌سازی از حملات سایبری و روش‌های مقابله با آن‌ها، می‌تواند به افزایش مهارت‌های کارکنان کمک کند و آموزش‌ها را تجربی‌تر و جذاب‌تر کند. ۵. ارزیابی عملکرد: ارزیابی عملکرد کارکنان در ارتباط با امنیت سایبری و اعمال تشویقات و تنبیهات مرتبط، می‌تواند به افزایش توجه و تعهد آن‌ها نسبت به امنیت سایبری کمک کند.	آشنایی کارکنان با تهدیدات سایبری، روش‌های حفاظت اطلاعات و رفتارهای امنیتی، درک کارکنان از امنیت سایبری، ارتقاء آگاهی کارکنان، ایجاد فرهنگ امنیتی، ارزیابی عملکرد

سؤالات مصاحبه	خبره	پاسخ خبره	کدهای شناسایی شده
سؤال ششم) از چه استانداردها و رویکردهایی برای افزایش امنیت در بانکداری الکترونیک استفاده می‌کنید؟ چگونه این استانداردها به بهبود الگوی امنیتی شما کمک کرده‌اند؟	خبره هشتم	استاندارد ایزو ۲۷۰۰۱، استاندارد بین‌المللیه برای نحوه مدیریت امنیت اطلاعات که توسط سازمان بین‌المللی استاندارد ایزو و کمیسیون بین‌المللی الکترونیک سال ۲۰۰۵ مورد استفاده قرار گرفت این استاندارد به نحوی می‌تونه به ما کمک کنه تو بحث هماهنگی با استانداردهای سامانه مدیریتی مثل ایزو ۹۰۰۱ و ایزو ۱۴۰۰۱ بعد شفاف‌سازی الزامات مستندسازی و سوابق موردنیازمونه. این استاندارد تأکید بر بهبود مستمر فرایندهای سامانه مدیریت امنیت اطلاعات داره و اینکه روش‌ها و فرایندهای مدیریت خطر فنّاوری و ارزیابی فرایندهای مدیریتی رو با به‌کارگیری یک الگوی فرایندی در برگرفته است. بانک‌ها باید استانداردها و سیاست‌های امنیتی را تعیین کنن و آن‌ها را به‌روز نگه دارن.	استاندارد ایزو ۲۷۰۰۱، ایزو ۹۰۰۱، ایزو ۱۴۰۰۱، مدیریت امنیت اطلاعات، روش‌ها و فرایندهای مدیریت خطر، استانداردها و سیاست‌های امنیتی
	خبره دهم	استاندارد ISO 27001 به‌عنوان یک استاندارد بین‌المللی در حوزه مدیریت امنیت اطلاعات، به منظور افزایش امنیت در بانکداری الکترونیک و سایر صنایع، استفاده می‌شود. این استاندارد شامل یک سری نکات و مفاهیم کلیدی است که به سازمان‌ها کمک می‌کند تا یک سامانه مدیریت امنیت را پیاده‌سازی کنند. استفاده از استاندارد ISO 27001 به بانک‌ها و سازمان‌های بانکداری الکترونیک کمک می‌کند تا به شیوه‌ای سازمان‌یافته و نظام‌مند، خطرها و تهدیدات امنیتی را شناسایی و مدیریت کنند. به طور خلاصه، استفاده از استاندارد ISO 27001 به بانکداری الکترونیک کمک می‌کند تا با تعیین سیاست‌ها و راهکارهای امنیتی، شناسایی خطرها، پیاده‌سازی تدابیر امنیتی مناسب و پیگیری مداوم، امنیت اطلاعات را بهبود دهد. این استاندارد یک چارچوب قوی و جامع برای مدیریت امنیت اطلاعات فراهم می‌کند و به سازمان‌ها کمک می‌کند تا رویکردهای استاندارد و مداوم در مقابله با تهدیدات امنیتی را اتخاذ کنند.	استاندارد ISO 27001، مدیریت امنیت اطلاعات، شناسایی خطرها و تهدیدات امنیتی، تعیین سیاست‌ها و راهکارهای امنیتی، شناسایی خطرها، پیاده‌سازی تدابیر امنیتی
سؤال هفتم) چه تغییراتی در الگوی امنیتی خود بر اثر تجربیات گذشته و تهدیدات فعلی انجام داده‌اید؟	خبره هفتم	ابزار احراز هویت مکرر داشتن الان خیلی خوب شده با موبایل، مکرر تأیید می‌کند و رمز یک‌بارمصرف میده. احراز هویت چندگانه می‌تونه یک راهکاری باشه که کلاه‌برداری رو به حداقل برسونه. اون کدها رو زیاد کردن عوامل تأیید هویت مثلاً انگشت‌نگاری یا چشم‌نگاری هم اضافه بشه مثلاً تأیید تراکنش با رمز پویا چقدر مشکلات کلاه‌برداری رو حل کرد.	احراز هویت، تأیید تراکنش، احراز هویت بیومتریک، انگشت‌نگاری، چشم‌نگاری، رمز پویا

سؤالات مصاحبه	خبره	پاسخ خبره	کدهای شناسایی شده
	خبره نهم	بانک‌ها و سازمان‌های بانکداری الکترونیک تلاش می‌کنند با نظارت مداوم بر ترافیک شبکه خود و به‌کارگیری فنّاوری‌های مدیریت امنیت شبکه، از حملات سایبری و نفوذهای ناخواسته جلوگیری کنند. این شامل استفاده از مجموعه‌ای از ابزارها و سامانه‌های مانیتورینگ شبکه، تحلیل ترافیک شبکه و اعمال سیاست‌های امنیتی مشخص است. بانک‌ها و سازمان‌های بانکداری الکترونیک با توسعه روابط بین‌بانکی، همکاری و تبادل اطلاعات امنیتی میان خود، توانایی مقابله با تهدیدات را افزایش می‌دهند.	نظارت مداوم بر ترافیک شبکه، مدیریت امنیت شبکه، سامانه‌های مانیتورینگ شبکه، تحلیل ترافیک شبکه، سیاست‌های امنیتی، روابط بین‌بانکی
	خبره دوازدهم	بانک‌ها باید برنامه‌های آمادگی و پاسخگویی به بحران برای مقابله با حملات سایبری را تدارک ببینند تا در صورت وقوع حمله، به‌سرعت واکنش مناسبی ارائه کنند. زیرساخت‌های امنیتی در برخی از بانک‌ها هنوز به‌روز نیست و کیفیت مناسبی ندارد و نیاز به استانداردسازی و به‌روزرسانی دارد تا از حفاظت مناسب برخوردار شوند.	پاسخگویی به بحران برای مقابله با حملات سایبری، کیفیت زیرساخت، استانداردسازی زیرساخت، به‌روزرسانی زیرساخت
	خبره یازدهم	استانداردها و به روش‌های این چنینی به‌دلیل پیاده‌سازی فرایندهای پیشگیرانه و بازرسی‌های مداوم، کمک شایانی به ارتقاء و بهبود امنیت در سازمان‌ها داشته‌اند و درزمینهٔ امنیت بانکداری الکترونیک تغییراتی در دسترسی‌های مجاز و کنترل دسترسی بر اساس نقش، اسکن و بررسی آسیب‌پذیری، پیشگیری آسیب‌های احتمالی، رفع آسیب‌ها و کاهش خطرها ایجاد شده است و به‌طورکلی محرمانگی، یکپارچگی و دردسترس‌بودن، افزایش یافته است که همه این موارد هم به افزایش رضایت مشتری، تجربه مثبت مشتری، افزایش اعتماد مشتری و کاهش سرقت اطلاعات و درنتیجه سودآوری بیشتر کسب‌وکار بانک منجر می‌گردد.	کنترل دسترسی، اسکن و بررسی آسیب‌پذیری، پیشگیری آسیب‌های احتمالی، رفع آسیب‌ها و کاهش خطرها، محرمانگی، یکپارچگی، دردسترس‌بودن، رضایت مشتری، تجربه مثبت مشتری، افزایش اعتماد مشتری و کاهش سرقت اطلاعات، افزایش سودآوری

شکل زیر ابرکدهای تشکیل‌شده از کدگذاری باز را نشان می‌دهد.

شکل ۱. ابرکدهای تشکیل‌شده از کدگذاری باز

کدگذاری محوری مرحله دوم تجزیه‌وتحلیل داده‌ها در نظریه‌پردازی زمینه‌ای در این پژوهش است. هدف این مرحله برقراری رابطه بین مقوله‌های تولیدشده در مرحله کدگذاری باز است. این کدگذاری، به این دلیل محوری نامیده شده که کدگذاری حول محور یک مقولهٔ محوری یعنی «امنیت سایبری در بانکداری الکترونیک» است. این مقوله به‌عنوان مقولهٔ محوری انتخاب‌شده و در مرکز الگو قرار گرفته است؛ زیرا می‌توان ردپا و اثر آن را در اغلب داده‌ها و نقل و قول‌های مصاحبه‌شوندگان، به‌وضوح مشاهده کرد؛ بنابراین می‌توان این مقوله را در مرکز الگو قرارداد و سایر مقوله‌ها را با آن مرتبط ساخت. برای کدگذاری محوری در این پژوهش از الگوی پارادایمی استراوس و کوربین استفاده شده است. این الگو به نظریه‌پرداز کمک می‌کند تا درکی کلی از فرایند تئوریک داشته باشد.

اجزای الگوی پارادایمی برای کدگذاری محوری عبارت‌اند: از مقوله‌محوری، شـرایط علی، شرایط زمینه‌ای، شرایط مداخله‌گر، راهبردها و پیامدها.

جدول ۲. کدگذاری ثانویه

ردیف	کدگذاری محوری	کدگذاری اولیه	ردیف	کدگذاری محوری	کدگذاری اولیه
۱	فنّاوری‌های جدید و پیشرفته	بلاک‌چین	۱۲	رویه امنیت پیشرفته	سکوهای مدیریت تهدیدات پیشرفته
		یادگیری ماشین			بهینه‌سازی و خودکارسازی فرایندهای امنیتی
		اینترنت اشیاء			احراز هویت و رمزنگاری در دستگاه‌های اینترنت اشیاء
		محاسبات ابری			مدیریت دستگاه‌های IOT
		هوش مصنوعی	۱۳	پروتکل و استانداردهای امنیتی	پیروی از استانداردها و پروتکل‌های امنیتی
۲	وضعیت داده‌ها	حجم بالای داده‌ها			پروتکل‌های ارتباطی و رمزنگاری
		پیچیدگی داده‌ها			استانداردهای احراز هویت و دسترسی
		مدیریت داده‌ها			استانداردهای امنیتی برای برنامه‌ها و سامانه‌ها
		به‌روزرسانی داده‌ها			مدیریت امنیت و پاسخ به تهدیدات
۳	تهدیدات سایبری	حملات سایبری	۱۴	وضعیت مدیریت خطر و پاسخ به بحران	روش‌ها و فرایندهای مدیریت خطر
		حملات رباتیک			آمادگی مدیریت خطر
		حملات DDoS			پاسخ به بحران برای مقابله با حملات سایبری
۴	رفتار کاربر	شناسایی رفتارهای کاربر	۱۵	حفاظت از داده‌ها	حریم خصوصی
		تحلیل پیشرفته الگوهای دسترسی کاربر			یکپارچگی داده‌ها
		شناسایی رفتارهای مشکوک			احراز هویت
		به‌روزرسانی مشخصات بیومتریک کاربر			کنترل دسترسی
		تطبیق هویتی در دسترسی‌های غیرمجاز			رمزنگاری

ردیف	کدگذاری محوری	کدگذاری اولیه	ردیف	کدگذاری محوری	کدگذاری اولیه
۵	عوامل نگرشی	درک امنیت اطلاعات			تأییدتراکنش
		بی‌ثباتی فرهنگ تجارت دیجیتال	۱۶	آموزش و آگاهی	آموزش کارکنان درزمینهٔ امنیت اطلاعات
		رفتارهای توده‌ای			آموزش روش‌های پیشگیری تهدیدات
		کمبود دانش تجارت دیجیتالی			اطلاع‌رسانی به کاربران
		سنتی بودن افکار غالب جامعه			آموزش روش‌های حفاظت از اطلاعات شخصی
		خطر درک شده	۱۷	مدیریت آسیب‌پذیری	اسکن و بررسی آسیب‌پذیری
		روند کند اطمینان افراد جامعه			پیش‌گیری آسیب‌های احتمالی
۶	قوانین و مقررات	قوانین محلی			رفع آسیب‌ها
		قوانین بین‌المللی			به‌روزرسانی و پچ گذاری
		قوانین بانکی و بومی	۱۸	نظارت و گزارش‌دهی	نظارت مداوم بر ترافیک شبکه
		سیاست‌های داخلی			ردگیری فعالیت‌های مشکوک
		سیاست‌های نظارتی و دولتی			گزارش‌دهی و تحلیل
۷	فرهنگ سازمانی	سطح آگاهی	۱۹	سامانه داده‌پردازی	شناسایی الگوهای مشترک
		فرهنگ امنیتی			استفاده از داده‌کاوی
		وضعیت آموزش ایمنی			الگوریتم‌سازی امنیتی
۸	زیرساخت‌های فنّاورانه	کیفیت زیرساخت			تحلیل داده‌های بزرگ
		به‌روزرسانی فنّاوری	۲۰	پشتیبان‌گیری و بازیابی	ایجاد نسخه‌های پشتیبان منظم
		بومی‌سازی فنّاوری			بازیابی از خرابی
		استانداردسازی فنّاوری			گروه متخصص پشتیبان‌گیری
		تطبیق فنّاوری			اشتراک‌گذاری منظم داده
		تعمیر و نگهداری فنّاوری	۲۱	به‌کارگیری تکنیک‌های مدرن	احراز هویت بیومتریک
۹	صنعت بانکداری	قوانین مالی			تشخیص صدای کاربر
		محیط داخلی بانک			رمزنگاری همگام

ردیف	کدگذاری محوری	کدگذاری اولیه	ردیف	کدگذاری محوری	کدگذاری اولیه
		شرایط صنعت بانکداری			رمزنگاری هومورفیک
		قوانین بین‌المللی مالی			تراکنش‌های شفاف بلاکچین
		شخصی سازی			قراردادهای هوشمند بلاکچین
		ساختار بانک			رمزنگاری داده‌ها بر اساس ابر
		روابط بین بانکی			کنترل دسترسی بر اساس نقش
		سطح‌بندی بانک	۲۲	خشنودی مشتری	رضایت مشتری
		انعطاف‌پذیری صنعت بانکداری			بهبود نگرش مشتری
		تمرکز صنعت بانکداری			افزایش وفاداری مشتری
		جایگاه بانک در جامعه			افزایش تعداد مشتری
		به‌روزرسانی صنعت			فرهنگ‌سازی مشتری
		سلسله مراتبی صنعت			تجربه مثبت مشتری
		وضعیت خصوصی و دولتی‌بودن			افزایش اعتماد مشتری
		شهرت بانک	۲۳	امنیت اطلاعات	کاهش سرقت اطلاعات
		وضعیت بانک در بورس اوراق بهادار			کاهش فاش شدن اطلاعات محرمانه
		معماری باز پیشران			کاهش سرقت پول
۱۰	اقتصاد دیجیتال	سیاست‌های داده‌ای باز	۲۴	مدیریت هزینه	کاهش بازپرداخت به مشتری
		سواد دیجیتالی			کاهش جبران خسارات
		سیاست‌گذاری بر اساس داده‌های تجربی و آزمایشی			کاهش جریمه‌های مقرراتی
		امنیت سایبری			کاهش هزینه‌های پروتکل‌های امنیتی
		هویت دیجیتال قابل‌اعتماد	۲۵	بهره‌وری اقتصادی	افزایش سرمایه‌گذاری
		هاب داده‌ای دیجیتالی قابل‌اعتماد			افزایش فعالیت‌های اقتصادی
		زیرساخت‌های عمومی برای اقتصاد دیجیتال			افزایش سودآوری

ردیف	کدگذاری محوری	کدگذاری اولیه	ردیف	کدگذاری محوری	کدگذاری اولیه
۱۱	سامانه حفاظتی و امنیتی	فایروال			
		سامانه‌های تشخیص نفوذ			
		سامانه‌های مدیریت رخداد			

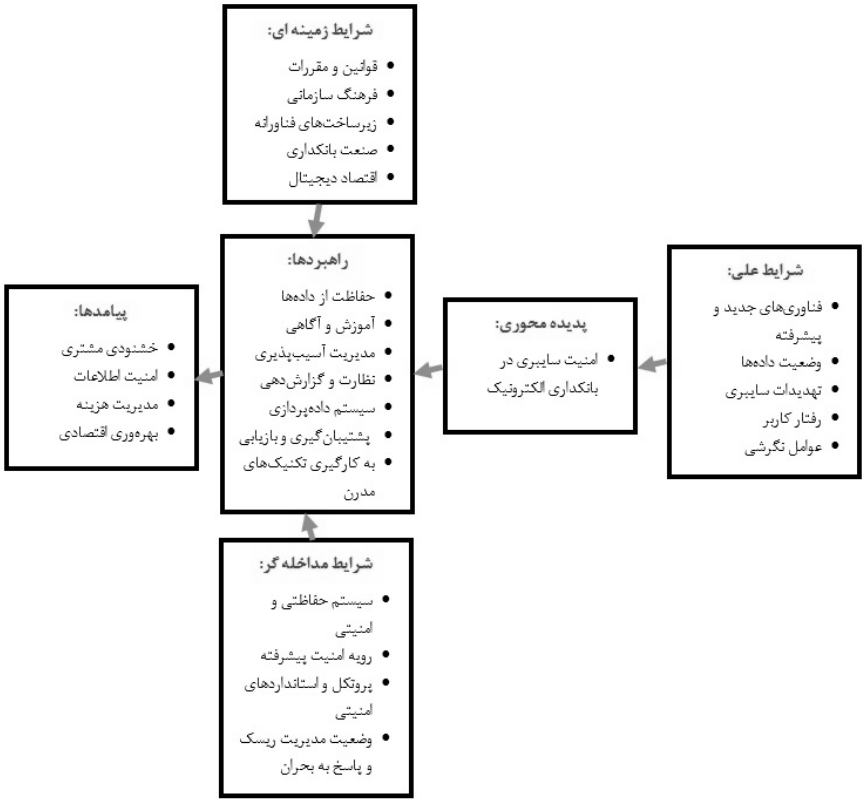
مرحله اصلی تحلیل داده‌بنیاد، کدگذاری انتخابی است که پژوهشگر بر اساس نتایج کدگذاری باز و محوری به ارائه نظریه پرداخته است. در این قسمت به ریشه‌یابی و دلایل شکل‌گیری این شرایط تحت عنوان یادداشت نظری که حاوی تأملات و اندیشه‌های تحلیل‌گر در مورد شرایط تحقیق است، بیان می‌شود. اجزای الگوی پارادایمی بر اساس استراوس و کوربین عبارتند از: از شرایط علی، شرایط زمینه‌ای، شرایط مداخله‌گر، راهبردها و پیامدها.

- شرایط علی، دلایل و عواملی هستند که باعث به وجود آمدن پدیده امنیت سایبری در بانکداری الکترونیک می‌شوند. شامل مؤلفه‌های تهدیدات سایبری، رفتار کاربر، عوامل نگرشی، فنّاوری‌های جدید و پیشرفته، وضعیت داده‌ها است.
- شرایط زمینه‌ای، بستر، محیط و ویژگی‌های خاصی هستند که بر نحوه اجرای راهبردهای امنیت سایبری در بانکداری الکترونیک تأثیر می‌گذارند. شامل مؤلفه‌های اقتصاد دیجیتال، زیرساخت‌های فنّاورانه، صنعت بانکداری، فرهنگ سازمانی، قوانین و مقررات است.
- شرایط مداخله‌گر، عواملی هستند که اجرای راهبردهای امنیت سایبری در بانکداری الکترونیک را تسهیل یا محدود می‌کنند. شامل مؤلفه‌های رویه امنیت پیشرفته، سامانه حفاظتی و امنیتی، وضعیت مدیریت خطر و پاسخ به بحران، پروتکل و استانداردهای امنیتی است.
- راهبردهای امنیت سایبری، مجموعه‌ای از اقدامات و واکنش‌هایی هستند که برای کنترل، مدیریت و بهبود امنیت سایبری در بانکداری الکترونیک اتخاذ می‌شوند. شامل مؤلفه‌های آموزش و آگاهی، به‌کارگیری تکنیک‌های مدرن، حفاظت از داده‌ها،

سامانه داده‌پردازی، مدیریت آسیب‌پذیری، نظارت و گزارش‌دهی، پشتیبان‌گیری و بازیابی است.

- پیامدهای امنیت سایبری، نتایج حاصل از اجرای راهبردهای امنیت سایبری در بانکداری الکترونیک هستند که می‌توانند مستقیم یا غیرمستقیم، مثبت یا منفی، کوتاه‌مدت یا بلندمدت باشند. شامل مؤلفه‌های امنیت اطلاعات، بهره‌وری اقتصادی، خشنودی مشتری، مدیریت هزینه است.

شکل ۱، پارادایم کدگذاری انتخابی و به‌عبارت‌دیگر الگوی پارادایمی فرایند کیفی پژوهش (الگوی مفهومی پژوهش) را نشان می‌دهد.



شکل ۲. الگوی پارادایمی پژوهش (الگوی امنیت سایبری در بانکداری الکترونیک)

تعریف فرضیات بر اساس الگوی مفهومی پژوهش

فرضیه ۱: متغیر شرایط علی (شامل: مؤلفه‌های فنّاوری‌های جدید و پیشرفته، وضعیت داده‌ها، تهدیدات سایبری، رفتار کاربر و عوامل نگرشی) تأثیر معنی‌داری بر پدیده‌محوری (امنیت سایبری در بانکداری الکترونیک) دارد.

فرضیه ۲: متغیر شرایط زمینه‌ای (شامل: مؤلفه‌های قوانین و مقررات، فرهنگ سازمانی، زیرساخت‌های فنّاورانه، صنعت بانکداری و اقتصاد دیجیتال) تأثیر معنی‌داری بر متغیر راهبردها (شامل: مؤلفه‌های حفاظت از داده‌ها، آموزش و آگاهی، مدیریت آسیب‌پذیری، نظارت و گزارش‌دهی، سامانه داده‌پردازی، پشتیبان‌گیری و بازیابی و به‌کارگیری تکنیک‌های مدرن) دارد.

فرضیه ۳: متغیر شرایط مداخله‌گر (شامل: مؤلفه‌های سامانه حفاظتی و امنیتی، رویه امنیت پیشرفته، پروتکل و استانداردهای امنیتی و وضعیت مدیریت خطر و پاسخ به بحران) تأثیر معنی‌داری بر متغیر راهبردها (شامل: مؤلفه‌های حفاظت از داده‌ها، آموزش و آگاهی، مدیریت آسیب‌پذیری، نظارت و گزارش‌دهی، سامانه داده‌پردازی، پشتیبان‌گیری و بازیابی و به‌کارگیری تکنیک‌های مدرن) دارد.

فرضیه ۴: پدیده‌محوری (امنیت سایبری در بانکداری الکترونیک) تأثیر معنی‌داری بر متغیر راهبردها (شامل: مؤلفه‌های حفاظت از داده‌ها، آموزش و آگاهی، مدیریت آسیب‌پذیری، نظارت و گزارش‌دهی، سامانه داده‌پردازی، پشتیبان‌گیری و بازیابی و به‌کارگیری تکنیک‌های مدرن) دارد.

فرضیه ۵: متغیر راهبردها (شامل: مؤلفه‌های حفاظت از داده‌ها، آموزش و آگاهی، مدیریت آسیب‌پذیری، نظارت و گزارش‌دهی، سامانه داده‌پردازی، پشتیبان‌گیری و بازیابی و به‌کارگیری تکنیک‌های مدرن) تأثیر معنی‌داری بر متغیر پیامدها (شامل: مؤلفه‌های خشنودی مشتری، امنیت اطلاعات، مدیریت هزینه و بهره‌وری اقتصادی) دارد.

فرضیه ۶: پدیده‌محوری (امنیت سایبری در بانکداری الکترونیک) رابطه بین شرایط علی (شامل: مؤلفه‌های فنّاوری‌های جدید و پیشرفته، وضعیت داده‌ها، تهدیدات سایبری، رفتار کاربر و عوامل نگرشی) و راهبردها (شامل: مؤلفه‌های حفاظت از داده‌ها،

آموزش و آگاهی، مدیریت آسیب‌پذیری، نظارت و گزارش‌دهی، سامانه داده‌پردازی، پشتیبان‌گیری و بازیابی و به‌کارگیری تکنیک‌های مدرن) را میانجی‌گری می‌کند.

فرضیه ۷: متغیر راهبردها (شامل: مؤلفه‌های حفاظت از داده‌ها، آموزش و آگاهی، مدیریت آسیب‌پذیری، نظارت و گزارش‌دهی، سامانه داده‌پردازی، پشتیبان‌گیری و بازیابی و به‌کارگیری تکنیک‌های مدرن) رابطه بین پدیده‌محوری (امنیت سایبری در بانکداری الکترونیک) و پیامدها (شامل: مؤلفه‌های خشنودی مشتری، امنیت اطلاعات، مدیریت هزینه و بهره‌وری اقتصادی) را میانجی‌گری می‌کند.

فرضیه ۸: متغیر راهبردها (شامل: مؤلفه‌های حفاظت از داده‌ها، آموزش و آگاهی، مدیریت آسیب‌پذیری، نظارت و گزارش‌دهی، سامانه داده‌پردازی، پشتیبان‌گیری و بازیابی و به‌کارگیری تکنیک‌های مدرن) رابطه بین شرایط زمینه‌ای (شامل: مؤلفه‌های قوانین و مقررات، فرهنگ سازمانی، زیرساخت‌های فنّاورانه، صنعت بانکداری و اقتصاد دیجیتال) و پیامدها (شامل: مؤلفه‌های خشنودی مشتری، امنیت اطلاعات، مدیریت هزینه و بهره‌وری اقتصادی) را میانجی‌گری می‌کند.

فرضیه ۹: متغیر راهبردها (شامل: مؤلفه‌های حفاظت از داده‌ها، آموزش و آگاهی، مدیریت آسیب‌پذیری، نظارت و گزارش‌دهی، سامانه داده‌پردازی، پشتیبان‌گیری و بازیابی و به‌کارگیری تکنیک‌های مدرن) رابطه بین شرایط مداخله‌گر (شامل: مؤلفه‌های سامانه حفاظتی و امنیتی، رویه امنیت پیشرفته، پروتکل و استانداردهای امنیتی و وضعیت مدیریت خطر و پاسخ به بحران) و پیامدها (شامل: مؤلفه‌های خشنودی مشتری، امنیت اطلاعات، مدیریت هزینه و بهره‌وری اقتصادی) را میانجی‌گری می‌کند.

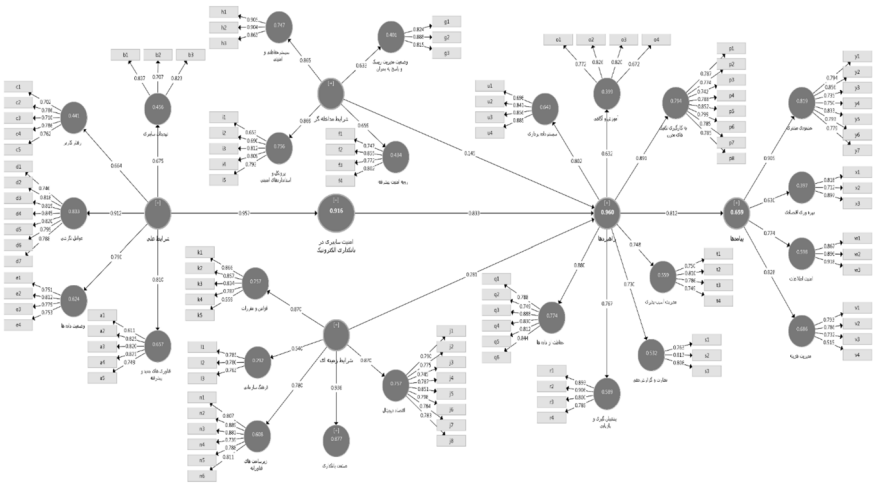
بخش کمی

در بخش کمی از مجموع ۳۸۴ نفر واحد پژوهش، ۲۱۹ نفر معادل ۵۳ درصد مرد و ۱۶۵ نفر معادل ۴۳ درصد زن بودند که ۱۱۱ نفر معادل ۲۹ درصد دارای سابقه کاری کمتر از ۱۰ سال، ۱۳۱ نفر معادل ۳۴ درصد دارای سابقه کاری ۱۰ تا ۱۵ سال، ۸۱ نفر معادل ۲۱ درصد ۱۶ تا ۲۰ سال و ۶۱ نفر معادل ۱۶ درصد بیشتر از ۲۰ سال بوده‌اند.

مقدارKMO ، ۰/۹۲۲ به دست آمد که نشان از کفایت حجم نمونه برای تحلیل عاملی دارد. هم‌چنین مقدار معناداری آزمون بارتلت نیز ۰/۰۰۰ بود که نشان می‌دهد نتایج معنادار

است. همچنین برای بررسی نرمال‌بودن توزیع داده‌ها، از آزمون کلموگروف- اسمیرنوف استفاده شد و با توجه به این‌که مقدار سطح معنی‌داری کوچک‌تر از مقدار خطای ۰/۰۵ بود، فرض صفر تأیید نشد، یعنی توزیع داده‌ها نرمال نبود و برای پاسخ به فرضیات تحقیق و اعتبارسنجی الگو می‌توان از تکنیک‌های تحلیل عاملی تأییدی (CFA) و الگوسازی معادلات ساختاری (SEM) با استفاده از روش حداقل مربعات جزئی[1] (PLS) با کمک نرم‌افزار SMART PLS استفاده کرد.

به منظور تحلیل ساختار پرسشنامه و کشف عوامل تشکیل‌دهنده هر متغیر از بارهای عاملی استفاده شد. بارعاملی نشان‌دهنده این موضوع است که چه میزان از واریانس‌های شاخص‌ها توسط متغیر پنهان خود توضیح داده می‌شود. مقدار این شاخص باید از ۰/۵ بزرگ‌تر و در فاصله اطمینان ۹۵٪ معنادار باشد. شاخصی که بار عاملی بیشتری داشته باشد، اهمیت بالاتری در اندازه‌گیری مؤلفه مربوطه دارد. تمامی شاخص‌ها دارای بارعاملی بزرگ‌تر از ۰/۵ و مقدار آماره تی بیشتر از ۱/۹۶ بوده‌اند (سطح معناداری کمتر از ۰/۰۵ شده است).



شکل۳. الگوی تحلیل عاملی تأییدی در حالت تخمین ضرایب استاندارد

1. Partial Least Square

یکی از شاخص‌های بررسی روایی همگرا، شاخص متوسط واریانس استخراج‌شده است. مقدار این متغیر برای سازه‌های الگو دارای مقدار میانگین واریانس تبیین شده بالاتر از ۰/۵ شده است و نشان از تأیید روایی همگرا در الگو است. از دیگر شاخص‌های روایی همگرا شاخص رائو از نظر هنسلر و همکاران است که این شاخص نیز برای تمامی متغیرهای تحقیق بالاتر از ۰/۶ بوده است.

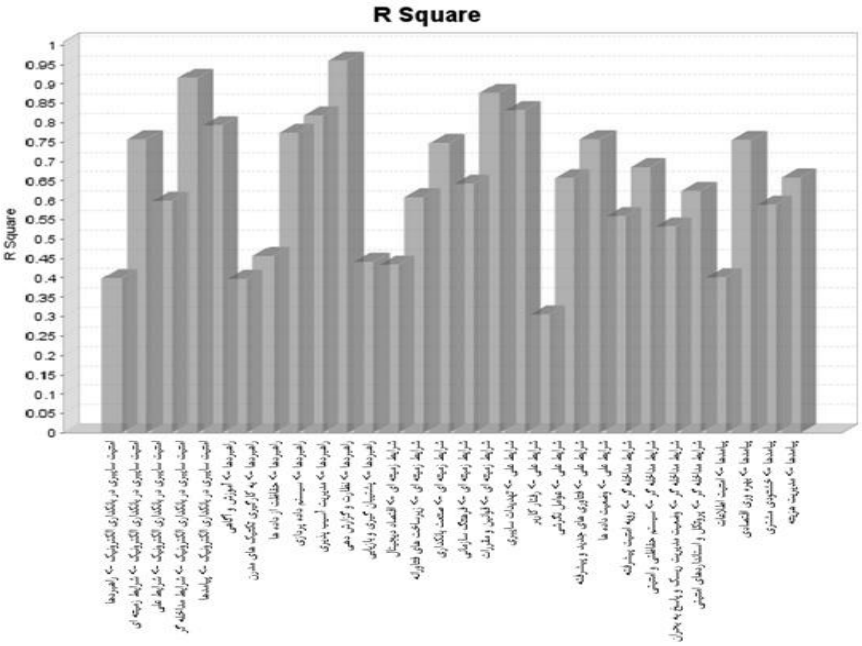
برای بررسی پایایی متغیرهای تحقیق از دو شاخص پایایی ترکیبی و آلفای کرونباخ استفاده شده است که برای تمامی متغیرهای تحقیق مقدار آلفای کرونباخ و پایایی ترکیبی از ۰/۷ بزرگ‌تر شده‌اند که نشان از پایایی ابزار اندازه‌گیری است.

جدول ۳. بررسی اعتبار همگرایی الگو

مؤلفه	Cronbach's Alpha	rho_A	Composite Reliability	AVE	Q2
آموزش و آگاهی	۰٫۷۸۰	۰٫۸۱۱	۰٫۸۵۷	۰٫۶۰۰	۰٫۳۴۲
اقتصاد دیجیتال	۰٫۹۱۳	۰٫۹۱۵	۰٫۹۳۰	۰٫۶۲۳	۰٫۴۹۷
امنیت اطلاعات	۰٫۸۷۴	۰٫۸۸۱	۰٫۹۲۳	۰٫۷۹۹	۰٫۵۳۴
امنیت سایبری در بانکداری الکترونیک	۰٫۹۷۸	۰٫۹۸۰	۰٫۹۷۹	۰٫۵۵۵	۰٫۳۱۹
به‌کارگیری تکنیک‌های مدرن	۰٫۹۱۳	۰٫۹۱۵	۰٫۹۳۰	۰٫۶۲۴	۰٫۴۹۷
بهره‌وری اقتصادی	۰٫۷۴۴	۰٫۷۸۹	۰٫۸۵۲	۰٫۶۶۰	۰٫۳۳۳
تهدیدات سایبری	۰٫۷۹۸	۰٫۷۰۹	۰٫۸۳۳	۰٫۶۲۶	۰٫۲۷۳
حفاظت از داده‌ها	۰٫۹۰۲	۰٫۹۰۶	۰٫۹۲۵	۰٫۶۷۲	۰٫۵۲۰
خشنودی مشتری	۰٫۹۰۱	۰٫۹۰۲	۰٫۹۲۲	۰٫۶۲۸	۰٫۴۸۹
راهبردها	۰٫۹۵۴	۰٫۹۵۸	۰٫۹۵۸	۰٫۵۱۷	۰٫۳۶۴
رفتار کاربر	۰٫۸۰۵	۰٫۸۰۹	۰٫۸۶۵	۰٫۵۶۳	۰٫۳۴۶
رویه امنیت پیشرفته	۰٫۸۰۷	۰٫۸۱۸	۰٫۸۷۳	۰٫۶۳۲	۰٫۳۸۱
زیرساخت‌های فنّاورانه	۰٫۹۰۲	۰٫۹۰۸	۰٫۹۲۵	۰٫۶۷۴	۰٫۵۲۴
سامانه حفاظتی و امنیتی	۰٫۸۷۰	۰٫۸۷۳	۰٫۹۲۰	۰٫۷۹۴	۰٫۵۲۶
سامانه داده‌پردازی	۰٫۸۴۱	۰٫۸۶۸	۰٫۸۹۳	۰٫۶۷۷	۰٫۴۵۳
شرایط زمینه‌ای	۰٫۹۵۹	۰٫۹۶۴	۰٫۹۶۲	۰٫۵۱۰	۰٫۳۶۲

مؤلفه	Cronbach's Alpha	rho_A	Composite Reliability	AVE	Q2
شرایط علی	۰٫۹۲۹	۰٫۹۳۴	۰٫۹۳۷	۰٫۵۸۷	۰٫۳۲۵
شرایط مداخله‌گر	۰٫۸۸۴	۰٫۸۹۸	۰٫۹۰۳	۰٫۵۹۱	۰٫۳۰۱
صنعت بانکداری	۰٫۹۲۲	۰٫۹۳۰	۰٫۹۳۲	۰٫۵۶۶	۰٫۳۸۸
عوامل نگرشی	۰٫۹۰۹	۰٫۹۱۱	۰٫۹۲۸	۰٫۶۴۸	۰٫۵۱۲
فرهنگ سازمانی	۰٫۷۸۰	۰٫۸۹۲	۰٫۸۲۰	۰٫۶۰۲	۰٫۲۲۷
فنّاوری‌های جدید و پیشرفته	۰٫۸۲۴	۰٫۸۳۴	۰٫۸۷۸	۰٫۵۹۲	۰٫۳۸۹
قوانین و مقررات	۰٫۸۴۳	۰٫۸۶۷	۰٫۸۹۰	۰٫۶۲۲	۰٫۴۳۴
مدیریت آسیب‌پذیری	۰٫۷۷۷	۰٫۷۸۰	۰٫۸۵۶	۰٫۵۹۹	۰٫۳۳۵
مدیریت هزینه	۰٫۷۷۷	۰٫۷۱۲	۰٫۸۰۴	۰٫۵۱۲	۰٫۲۲۷
نظارت و گزارش‌دهی	۰٫۷۱۲	۰٫۷۲۴	۰٫۸۳۷	۰٫۶۳۲	۰٫۲۷۶
وضعیت داده‌ها	۰٫۷۷۷	۰٫۷۷۹	۰٫۸۵۷	۰٫۵۹۹	۰٫۳۳۶
وضعیت مدیریت خطر و پاسخ به بحران	۰٫۷۹۶	۰٫۷۹۷	۰٫۸۸۰	۰٫۷۱۱	۰٫۳۹۹
پروتکل و استانداردهای امنیتی	۰٫۸۰۹	۰٫۸۲۱	۰٫۸۶۸	۰٫۵۶۹	۰٫۳۵۹
پشتیبان‌گیری و بازیابی	۰٫۸۶۹	۰٫۸۷۸	۰٫۹۱۱	۰٫۷۲۱	۰٫۵۰۷
پیامدها	۰٫۹۱۱	۰٫۹۱۸	۰٫۹۲۴	۰٫۶۲۴	۰٫۳۴۸

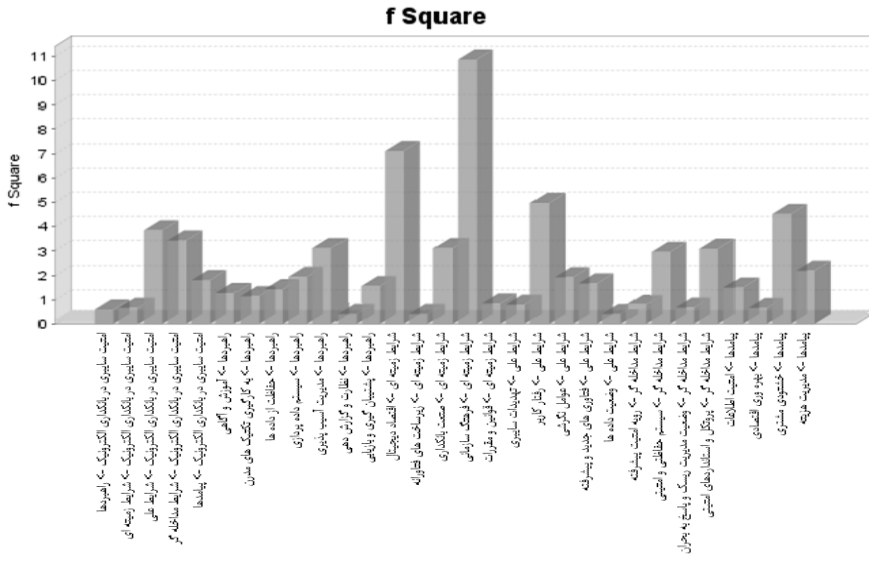
ضریب تعیین، بیانگر میزان تغییرات متغیرهای وابسته توسط متغیرهای مستقل است. هرچه مقدار ضریب تعیین سازه‌های درون‌زای الگو بیشتر باشد، نشان از برازش بهتر الگو است. سه مقدار ۰/۱۹، ۰/۳۳ و ۰/۶۷ به‌عنوان مقدار ملاک برای ضعیف، متوسط و قوی‌بودن برازش بخش ساختاری الگو به‌وسیله معیار ضریب تعیین است.



شکل ۴. ضریب تعیین متغیرهای پنهان تحقیق

از آزمون‌های دیگر ارزیابی الگوی اندازه‌گیری، آزمون بررسی کیفیت آن است. کیفیت الگوی اندازه‌گیری توسط شاخص اشتراک با روایی متقاطع (Q2) محاسبه می‌شود. این شاخص درواقع توانایی الگو مسیر را در پیش‌بینی متغیرهای مشاهده‌پذیر از طریق مقادیر متغیر پنهان متناظرشان می‌سنجد. چنان‌چه این شاخص عدد مثبتی را نشان دهد، الگوی اندازه‌گیری از کیفیت لازم برخوردار است. برای تمامی متغیرهای موجود در پژوهش این شاخص مثبت بوده و میانگین کل این شاخص برابر ۰/۳۹۱ است که نشان از کیفیت مطلوب و بالای الگوی اندازه‌گیری می‌دهد.

اندازه اثر میزان تغییراتی است که متغیرهای مستقل بر متغیرهای وابسته می‌گذارند. درواقع این شاخص نشان می‌دهد اگر یک متغیر مستقل حذف شود چه میزان تغییراتی در متغیر وابسته ایجاد می‌شود. مقادیر اندازه اثر در هیچ‌یک از موارد کمتر از ۰/۰۲ به دست نیامد و در اکثر موارد قوی برآورد شد.



شکل ۵. اندازه اثر متغیرهای پژوهش

آزمون فرضیات

جدول ۴ نتایج معادلات ساختاری را برای آزمون فرضیات پژوهش نشان می‌دهد؛ بنابراین همه فرضیات تأیید شدند.

جدول ۴. نتایج معادلات ساختاری فرضیات پژوهش

فرضیات	بتا	t	سطح معناداری	وضعیت فرضیه	جهت رابطه
شرایط علی -> امنیت سایبری در بانکداری الکترونیک	۰٫۹۵۷	۲۱۸٫۰۲۹	۰٫۰۰۰	تأیید	+
شرایط زمینه‌ای -> راهبردها	۰٫۲۸۱	۴٫۵۶۸	۰٫۰۰۰	تأیید	+
شرایط مداخله‌گر -> راهبردها	۰٫۱۴۵	۵٫۱۷۵	۰٫۰۰۰	تأیید	+
امنیت سایبری در بانکداری الکترونیک -> راهبردها	۰٫۸۳۳	۱۱٫۷۱۴	۰٫۰۰۰	تأیید	+
راهبردها -> پیامدها	۰٫۸۱۲	۳۹٫۰۹۵	۰٫۰۰۰	تأیید	+
شرایط علی -> امنیت سایبری در بانکداری الکترونیک -> راهبردها	۰٫۸۵۲	۱۰٫۹۴۴	۰٫۰۰۰	تأیید	+

فرضیات	بتا	t	سطح معناداری	وضعیت فرضیه	جهت رابطه
امنیت سایبری در بانکداری الکترونیک -> راهبردها -> پیامدها	۰٫۸۲۱	۹٫۶۹۲	۰٫۰۰۰	تأیید	+
شرایط زمینه‌ای -> راهبردها -> پیامدها	۰٫۶۱۱	۷٫۶۷۲	۰٫۰۰۰	تأیید	+
شرایط مداخله‌گر -> راهبردها -> پیامدها	۰٫۵۴۸	۶٫۴۱۲	۰٫۰۰۰	تأیید	+

جدول ۵ نتایج آزمون سوبل را برای آزمون فرضیات معنی‌داری تأثیر متغیرهای میانجی را نشان می‌دهد.

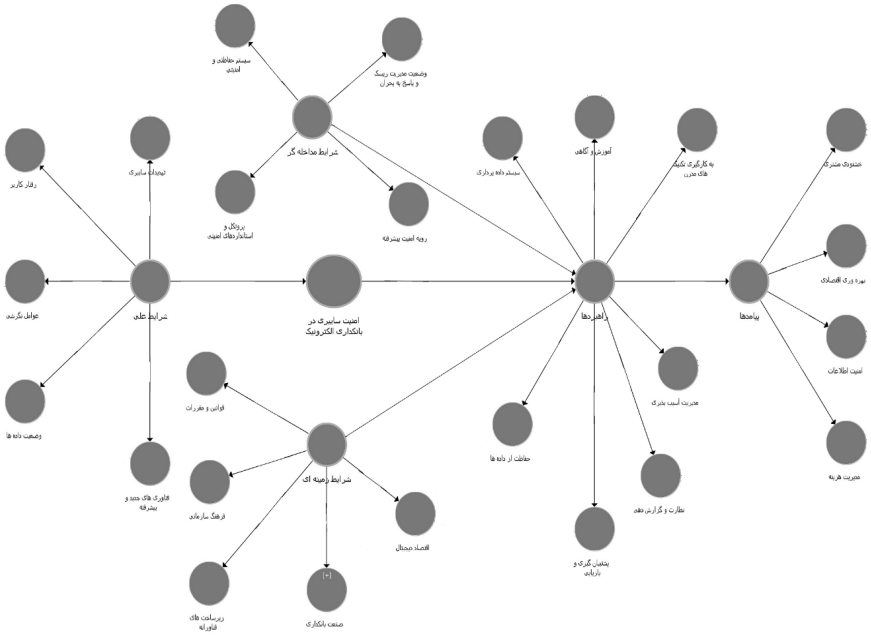
	ضریب مسیر میان‌متغیر مستقل و میانجی	ضریب مسیر میان‌متغیر میانجی و وابسته	خطای استاندارد مسیر میان متغیر مستقل و میانجی	خطای استاندارد مسیر میان متغیر میانجی و وابسته	نتیجه آزمون سوبل (Z-value)	وضعیت آزمون
شرایط علی -> امنیت سایبری در بانکداری الکترونیک -> راهبردها	۰٫۹۵۷	۰٫۸۳۳	۰٫۰۰۴	۰٫۰۷۱	۱۱٫۷۱۸	تأیید
امنیت سایبری در بانکداری الکترونیک -> راهبردها -> پیامدها	۰٫۸۳۳	۰٫۸۱۲	۰٫۰۷۱	۰٫۰۲۱	۱۱٫۲۲۶	تأیید
شرایط زمینه‌ای -> راهبردها -> پیامدها	۰٫۲۸۱	۰٫۸۱۲	۰٫۰۶۲	۰٫۰۲۱	۴٫۵۰۱	تأیید
شرایط مداخله‌گر -> راهبردها -> پیامدها	۰٫۱۴۵	۰٫۸۱۲	۰٫۰۲۸	۰٫۰۲۱	۵٫۱۳۲	تأیید

نتیجه‌گیری و پیشنهادها

این پژوهش با هدف ارائهٔ الگوی امنیت سایبری در بانکداری الکترونیک انجام شد. یافته‌های این پژوهش همسو با پژوهش‌های ژوانگ و همکاران (۲۰۲۰)، ریس و همکاران (۲۰۲۴)، کومار (۲۰۲۳)، ادماس و همکاران (۲۰۲۴)، گورینگ و همکاران (۲۰۲۴)، افراشته و همکاران (۱۴۰۳)، شکرزهی و همکاران (۱۴۰۳)، احمدی (۱۴۰۲)، شارما و همکاران (۲۰۲۳)،

مازندرانی و همکاران (۱۴۰۲)، کبیر و الم (۲۰۲۳)، نگه‌دار و همکاران (۱۴۰۲)، کاویانی و میرسپاسی (۱۴۰۰)، روهان و همکاران (۲۰۲۳) بود.

در بخش کیفی، با رویکردی نظام‌مند برمبنای نظریه داده‌بنیاد، متغیرهای الگوی امنیت سایبری در بانکداری الکترونیک شناسایی شد و در ۵ دسته مقوله قرار گرفت. الگوی پارادایمی این پژوهش، یک ساختار تحلیلی است که روابط بین شرایط علّی، شرایط زمینه‌ای، شرایط مداخله‌گر، راهبردها و پیامدها را مشخص می‌کند.



شکل ۵. الگوی نهایی پژوهش

در بخش کمی، الگوی پژوهش با تمرکز بر روایی واگرا، شاخص‌های برازش الگو و اولویت‌بندی مؤلفه‌های تأثیرگذار بر الگوی امنیت سایبری تحلیل شد. ازآنجاکه مقدار شاخص نیکویی برازش (GOF) برابر ۰٫۶۳۴ شده است و از مقدار ۰٫۴ بزرگ‌تر است، نشان از برازش مناسب الگو دارد. به بیان ساده‌تر داده‌های این پژوهش با ساختار عاملی و زیربنای نظری تحقیق برازش مناسبی دارد و این بیانگر همسو بودن سؤالات با سازه‌های نظری است. همچنین شاخص ریشه دوم برآورد واریانس خطای تقریب (SRMR) برای

الگـوی تحقیـق، برابـر ۰/۰۸۶ بود کـه از مقدار ۰/۱ کمتر اسـت و می‌توان گفـت الگوی برازش مناسـبی داشـته اسـت و داده‌های این پژوهش با سـاختار عاملی و زیربنای نظری تحقیق برازش مناسـبی دارد. از طرفی با توجه به اینکه تمامی شـاخص‌ها دارای بارعاملی بزرگ‌تر از ۰٫۵ و مقدار آماره تی بیشتر از ۱٫۹۶ در فاصله اطمینان ۹۵٪ (سطح معناداری کمتر از ۰٫۰۵) بودند، همه شـاخص‌ها تأیید می‌شـوند و هیچ شـاخصی نیاز به حذف شـدن ندارد و الگو از اعتبار کافی برخوردار است.

برمبنـای تحلیل‌هـای انجام‌شـده می‌توان گفت، الگـوی امنیت سـایبری در بانکداری الکترونیک بر اسـاس تحلیل بارهای عاملی مرتبه دوم، نشـان‌دهنده تأثیرگذاری قابل‌توجه متغیرهـای مختلـف بر امنیت اطلاعات و عملکرد بانک‌ها اسـت. در این الگو، در بخش شـرایط علّی، عوامل نگرشـی کاربران (۰٫۹۱۲) و فنّاوری‌های جدید (۰٫۸۱۰) از تأثیرگذارترین مؤلفه‌هـا هسـتند. این یافته‌ها نشـان می‌دهد که پذیـرش فنّاوری‌های نویـن و تغییر نگرش کاربران نسبت به امنیت سایبری، کلیدی‌ترین عوامل در ایجاد محیطی امن در بانکداری الکترونیک محسـوب می‌شـوند. همچنین، وضعیـت داده‌ها (۰٫۷۹۰) و تهدیدات سـایبری (۰٫۶۷۵) نیـز از عوامل مهمی هسـتند که نشـان می‌دهنـد بانک‌ها باید بـه کیفیت داده‌ها و مقابله با تهدیدات توجه ویژه‌ای داشته باشند.

شـرایط زمینـه‌ای نیـز در موفقیـت ایـن الگـو تأثیـر بسـزایی دارد، به‌طوری‌کـه صنعـت بانکـداری (۰٫۹۳۷) و قوانیـن و مقـررات (۰٫۸۷۱) مهم‌تریـن عوامـل در ایـن حـوزه شـناخته شـده‌اند. ایـن نتایج نشـان می‌دهـد که ایجاد زیرسـاخت‌های قوی و سیاسـت‌های قانونی مناسـب، بـرای توسـعه امنیـت سـایبری ضـروری اسـت. در کنـار آن، اقتصـاد دیجیتـال (۰٫۸۶۹) نیز نقش مهمی ایفا می‌کند که نشان از وابستگی بانکداری الکترونیک به تحولات اقتصادی و فنّاورانه دارد.

در شـرایط مداخله‌گـر، پروتکل‌هـا و اسـتانداردهای امنیتـی (۰٫۸۶۹) و سـامانه‌های حفاظتـی (۰٫۸۶۳) بیش‌تریـن اهمیـت را دارند. این نتایج بیانگر آن اسـت که پیاده‌سـازی اسـتانداردهای امنیتـی قـوی و ایجـاد سـامانه‌های حفاظتـی پیشـرفته می‌توانـد در کاهش تهدیدات و افزایش ایمنی داده‌ها بسیار مؤثر باشد.

راهبردهـای امنیتـی نقـش مهمـی در تقویـت امنیت سـایبری ایفـا می‌کنند کـه از میان آن‌هـا، به‌کارگیـری تکنیک‌های مدرن (بار عاملـی ۰٫۸۹۲) و حفاظـت از داده‌ها (بار عاملی ۰٫۸۸۰) بیش‌ترین اهمیت را دارند. این یافته نشان می‌دهد که استفاده از فنّاوری‌های نوین و تمرکز بر امنیت اطلاعات، ستون فقرات راهبردهای امنیت سایبری محسوب می‌شود.

درنهایـت، تحلیـل پیامدهـای امنیـت سـایبری نشـان می‌دهـد کـه افزایـش رضایـت مشتریان (۰٫۹۰۵) و مدیریت هزینه (۰٫۸۲۸) مهم‌ترین نتایج پیاده‌سازی صحیح راهبردهای امنیتی هسـتند. این یافته نشـان‌دهنده آن است که تقویت امنیت سایبری، نه‌تنها موجب حفاظـت از اطلاعـات می‌شـود، بلکه باعث افزایـش اعتماد مشـتریان و کاهش هزینه‌های عملیاتی بانک‌ها نیز خواهد شد.

ایـن پژوهـش با وجـود اهمیـت و نوآوری‌های خـود بـا محدودیت‌هایی نیـز مواجه بوده است.

محدودیت‌های این پژوهش عبارتند از

- داده‌های محدود که می‌تواند نتایج پژوهش را تحت‌تأثیر قرار دهد.
- محدودیت‌های زمانی که ممکن اسـت باعث شـود برخـی از متغیرهای طولانی‌مدت یا روندهای زمان‌بر از قلم بیفتند.
- محدودیت‌هـای منابـع مالـی که باعث می‌شـود امکان دسترسـی بـه نمونه‌هـای بزرگ و متنوع از داده‌ها یا انجام آزمایش‌های میدانی و نظرسـنجی‌های گسـترده وجود نداشـته باشد.
- قابلیـت تعمیـمِ نتایج که به‌دلیل شـرایط خاص محیطی یا جمعیتـی، قابلیت تعمیم به جمعیت‌های دیگر را ندارند.

بر اساس یافته‌های این پژوهش، پیشنهاد می‌شود که

- از داده‌های گسترده‌تر و متنوع‌تر از منابع مختلف استفاده شود.
- از فنّاوری‌های نوین مانند تحلیل داده‌های کلان، یادگیری ماشـین و الگوهای پیشـرفته تحلیل پیش‌بینی استفاده شود.

- پژوهش‌های میان‌رشته‌ای انجام شود تا تعامل بین زمینه‌های مختلف علمی مانند فنّاوری اطلاعات، علوم اجتماعی و اقتصاد را در نظر گرفته شود و به فهم بهتری از موضوعات پیچیده کمک کند.
- توجه بیشتری به ابعاد بین‌المللی و مقایسه‌ای داشت. پژوهش‌های آینده به ارزیابی اثرات بلندمدت فنّاوری‌ها و سیاست‌ها پرداخته شود.
- با توجه به اهمیت فرهنگ سازمانی و آموزش در موفقیت پیاده‌سازی فنّاوری‌های جدید، تحقیق بیشتر در این زمینه‌ها می‌تواند به بهبود عملکرد سازمان‌ها کمک کند.
- با توجه به گسترش حملات سایبری و تهدیدات جدید، پژوهش‌های آینده باید به شناسایی و تحلیل عمیق‌تری از این تهدیدات و راهکارهای مقابله با آن‌ها اختصاص یابد.

بهره‌برداران پژوهش

- بانک‌ها و مؤسسات مالی (مدیران ارشد بانک‌ها، واحدهای فنّاوری اطلاعات و امنیت، بخش‌های خطر و حسابرسی داخلی)
- نهادهای نظارتی و سیاست‌گذار (بانک مرکزی، نهادهای قانون‌گذار و تنظیم‌کنندگان مقررات)
- ارائه‌دهندگان خدمات و فنّاوری در حوزهٔ امنیت سایبری و زیرساخت‌های بانکی
- پژوهشگران، اساتید و دانشجویان
- مشتریان بانکداری الکترونیک (افراد و شرکت‌ها)

منابع

- آپرناک، آرش؛ گازری نیشابوری، آرزو و سراج بردیا. (۱۴۰۱). رابطه بین امنیت ادراک‌شده و اعتماد مشتریان به سامانه بانکداری الکترونیک مبتنی بر رویکردNFC-Mobile ، پنجمین کنفرانس بین‌المللی مطالعات بین‌رشته‌ای در مدیریت و مهندسی، ۶۷۴-۶۹۱.
- احمدی، سعیده. (۱۴۰۲). راهبردهای توسعه اقتصاد دیجیتال در ایران، ماهنامه علمی امنیت اقتصادی، ۱۱(۴)، ۴- ۱۶. https://civilica.com/doc/1717234
- افراشته، نسرین؛ محمدی، افسانه؛ آهنگری، آرام و آسور، امی. (۱۴۰۳). بررسی چالش‌ها و راهکارهای امنیت سایبری در دنیای امروز، دومین کنفرانس بین‌المللی پژوهش‌های مدیریت، تعلیم و تربیت در آموزش‌وپرورش، تهران،. https://civilica.com/doc/2039579.
- باطنی، زهره و شاهی قره‌بلاغ، پرویز. (۱۳۹۰). مدیریت فنّاوری امنیت اطلاعات، اولین همایش تخصصی سامانه‌های هوشمند کامپیوتری و کاربردهای آن‌ها، تهران:. https://civilica.com/doc/139258.
- شکرزهی، مبین؛ حسین‌بر، بهمن؛ حسین‌بر، معصومه و ارباب ناهوک، عنبرخاتون. (۱۴۰۲). نقش امنیت سایبری در آموزش فنّاوری اطلاعات، پانزدهمین کنفرانس بین‌المللی پژوهش‌های مدیریت و علوم انسانی در ایران، تهران: کنفرانس مدیریت و تحقیقات علوم انسانی در ایران، ۱۵(۱۵)، ۷۷۵-۷۸۰، https://civilica.com/doc/2013859.
- طهماسبی آقبلاغی؛ داریوش؛ سلطانی، مرتضی؛ شهبازی، میثم و اوضاعی، افسانه. (۱۴۰۰). ارائه چارچوب همکاری راهبردی بین نظام بانکی خصوصی و فین‌تک‌ها در ایران، مدیریت توسعه فنّاوری، ۹(۱)، ۴۱-۶۶.. doi: 10.22104/jtdm.2021.4781.2761
- عسکری، مریم و مدیری، ناصر. (۱۳۹۹). معماری خودارزیابی امنیت سایبری، چهارمین کنفرانس ملی پژوهشی کاربردی در علوم برق و کامپیوتر و مهندسی پزشکی. https://civilica.com/doc/1016778
- کاویانی، حسن و میرسپاسی، ناصر. (۱۴۰۰). طراحی الگوی قابلیت‌های سازمانی در حوزه امنیت سایبری، مطالعات راهبردی بسیج، ۲۴(۹۲)، ۱۲۱-۱۵۱،. https://civilica.com/doc/1472913
- مازندرانی، علی و خیرآبادی، محمدتقی و بزازی، امین. (۱۴۰۰). یک پروتکل احراز هویت سبک‌وزن آگاه از مکان برای اینترنت اشیا، مجله علمی محاسبات نرم و فنّاوری اطلاعات، ۱۲(۴)، ۱۲-۲۲.، https://civilica.com/doc/1447733
- موسوی، سید احمد. (۱۴۰۳). بررسی تأثیر ابعاد عینی امنیت سامانه‌های پرداخت الکترونیکی با واسطه درک مشتریان از امنیت و اعتماد (مطالعه موردی: شعب بانک ملی استان کهکیلویه و بویراحمد)، https://civilica.com/doc/1976050
- وجدانی، بنفشه. (۱۴۰۳). بررسی اثرگذاری حریم خصوصی و امنیت خدمات بانکداری الکترونیک بر وفاداری مشتریان بانکی با تأکید بر قابلیت اطمینان، اولین کنفرانس بین‌المللی مدیریت، مهندسی صنایع، حسابداری و اقتصاد در علوم انسانی،. https://civilica.com/doc/2025680
- نگهدار، ایرج و پورقهرمانی، بابک و بیگی، جمال. (۱۴۰۲). رهیافت‌های پیشگیری وضعی سیاست جنایی ایران در قبال نقض امنیت سایبری در پرتو اسناد بین‌المللی، سیاست عمومی، ۹(۲)، ۹۷-۱۱۴، https://civilica.com/doc/1654075.

- Adedoyin Tolulope Oyewole, Chinwe Chinazo Okoye, Onyeka Chrisanctus Ofodile & Chinonye Esther Ugochukwu, (2024), Cybersecurity risks in online banking: A detailed review and preventive strategies application, World Journal of Advanced Research and Reviews 21(3):625-643, https://doi.org/10.30574/wjarr.2024.21.3.0707
- Admass, W. S., Munaye, Y. Y., & Diro, A. A., (2024), Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031. https://doi.org/10.1016/j.csa.2023.100031
- Aldahidhavi, H. M. K., Abdulreza, J. Z. S., Sebai, M., & Harjan, S. A., (2020), An efficient model for financial risks assessment based on artificial neural networks. Journal of Southwest Jiaotong University, 55(3). https://doi.org/10.35741/issn.0258-2724.55.3.8
- Al-khawaja, H. A., & Aburub, F. A. (2025). Blockchain for Securing Data Storage in Digital Banking Services. SN Computer Science, 6(1), 56
- Anwaar, S., (2024), Harnessing Large Language Models in Banking: Banking Innovation with Operational and Security Risks. World Journal of Advanced Engineering Technology and Sciences, 13(1), https://dx.doi.org/10.30574/wjaets.2024.13.1.0426
- Ayinaddis, S. G., Mirete, T. G., & Getahun, B. W. (2025). Evaluating the factors influencing electronic banking adoption in Ethiopia: analysis from customer perspective. Journal of Innovation and Entrepreneurship, 14(1), 56
- Bixhaku, S., Polo, A., Zyberi, I., & Caca, E. (2025). Electronic banking risks: Challenges, security concerns, and mitigation strategies. Sustainable Regional Development Scientific Journal, 2(1), 44-53
- Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. Journal of Financial Crime, 32(1), 31-48
- Creado, Y., & Ramteke, V., (2020), Active cyber defence strategies and techniques for banks and financial institutions. Journal of Financial Crime, 27(3), 771-780. https://doi.org/10.1108/JFC-01-2020-0008
- Evren, R., & Milson, S., 2024, The Cyber Threat Landscape: Understanding and Mitigating Risks. Tech. rep. EasyChair.
- Goering, S., Beck, A., Dorfman, N., Schwarzwalder, S., & Wohns, N., (2024), Privacy protections in and across contexts: why we need more than contextual

integrity. AJOB neuroscience, 15(2), 149-151. https://doi.org/10.1080/21507740.2024.2326932

- Kenney, Martin & Patton, Donald, (2005), Entrepreneurial Geographies: Support Networks in Three High-Technology Industries, Economic Geography 81(2):201 - 228, DOI:10.1111/j.1944-8287.2005.tb00265.x
- Kabir, M. S., & Alam, M. N., (2023), IoT, Big Data and AI Applications in the Law Enforcement and Legal System: A Review. International Research Journal of Engineering and Technology (IRJET), 10(05), 1777-1789.
- Kim, Y., Park, Y. J., Choi, J., & Yeon, J., (2015), An empirical study on the adoption of "Fintech" service: Focused on mobile payment services. Advanced Science and Technology Letters, 114(26), 136-140, http://dx.doi.org/10.14257/astl.2015.114.26
- Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N., (2021), Digital transformation: An overview of the current state of the art of research. Sage Open, 11(3), 21582440211047576, https://doi.org/10.1177/21582440211047576
- Kumar, M., (2023), An overview of cyber security in digital banking Sector. East Asian Journal of Multidisciplinary Research, 2(1), 43-52, https://doi.org/10.55927/eajmr.v2i1.1671
- Mehenaj Jerin Mohona, 2024, Emerging cyber security threats in banking sector; Loopholes and solutions in the eye of law, International Journal of Law, International Journal of Law, Volume 10, Issue 3, 2024, Page No. 214-219
- Najaf, K., Schinckus, C., Mostafiz, M. I., & Najaf, R., (2020), Conceptualising cybersecurity risk of fintech firms and banks sustainability. https://shura.shu.ac.uk/id/eprint/27504
- Parlour, Richard & Bouyon, Sylvain & Krause, Simon, (2018), Cybersecurity in finance: Getting the policy mix right. Rowman & Littlefield
- Reis, O., Oliha, J. S., Osasona, F., & Obi, O. C., (2024), Cybersecurity dynamics in Nigerian banking: trends and strategies review. Computer Science & IT Research Journal, 5(2), 336-364. https://doi.org/10.51594/csitrj.v5i2.761
- Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H., (2023), A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon, 9(3), https://doi.org/10.1016/j.heliyon.2023.e14234
- Sadlakowski, D., & Sobieraj, A., (2017), The development of the FinTech industry in the Visegrad group countries. World Scientific News, 85, 20-28.

- Selvaraj Nagasundari, (2021), The essence of cybersecurity through fintech 3.5 in preventing and detecting financial fraud: a literature review, Electronic Journal of Business and Management (Volume 6, No. 2, 2021, Pages 18 to 29)
- Shaikh, A. A., Glavee-Geo, R., Karjaluoto, H., & Hinson, R. E., (2023), Mobile money as a driver of digital financial inclusion. Technological Forecasting and Social Change, 186, 122158. https://doi.org/10.1016/j.techfore.2022.122158
- Shakeel, waria & Mardani, Abbas & Gholamzadeh, Abdoulmohammad, Ariani Goni, Feybi, (2020), Anatomy of sustainable business model innovation, Journal of Cleaner Production, DOI:10.1016/j.jclepro.2020.121201
- Sharma, L. R., Bidari, S., Bidari, D., Neupane, S., & Sapkota, R., (2023), Exploring the mixed methods research design: types, purposes, strengths, challenges, and criticisms. Glob Acad J Linguist Lit, 5. 10.36348/gajll. 2023.v05i01.002
- Tristan Lim, Patrick Thang, (2021), Outsourcing life cycle model for financial services in the fintech era. https://ink.library.smu.edu.sg/sis_research/6116/
- Van Voorhis, C., Hatcher, W., Kalat, T., Wang, Y., & Hammad, E., (2024), Towards an Automated Cybersecurity Risk Assessment of Next Generation Emergency Communication Networks-NG911. In 2024 IEEE World Forum on Public Safety Technology (WFPST) (pp. 175-181). IEEE, https://doi.org/10.1109/WFPST58552.2024.00042
- Widodo, D. P., Syah, T. Y. R., & Negoro, D. A., (2020), Digital Channel and Customer Satisfaction on Financial Services. Journal of Multidisciplinary Academic, 4(3), 159-163. https://www.kemalapublisher.com/index.php/JoMA/article/view/461
- Yiu Ting Yan Azura, Muhammad Ajmal Azad & Yussuf Ahmed, (2025), An integrated cyber security risk management framework for online banking systems, Journal of Banking and Financial Technology, https://doi.org/10.1007/s42786-025-00056-3
- Zhuang, P., Zamir, T., & Liang, H., (2020), Blockchain for cybersecurity in smart grid: A comprehensive survey. IEEE Transactions on Industrial Informatics, 17(1), 3-19. https://doi.org/10.1109/TII.2020.2998479