Passive Defence

Vol. 16, No. 3, Autumn 2025, Serial No. 63

ISSN: 2980-8030 , E-ISSN: 2008-6849

Presenting a Cybersecurity Model in Electronic Banking

Hossein Babaee[1], Mansoureh Aligholi[2]*, Daryoush Gholamzadeh[3], Mohammadreza Radfar[4]

[1]PhD Student, Department of Information Technology Management, CT.C, Islamic Azad University, Tehran, Iran. Email Address: hossein.babaee@iau.ac.ir

[2]Correspondence: Associate Professor, Department of Business Administration, CT.C, Islamic Azad University, Tehran, Iran. Email Address: hossein.babaee@iau.ac.ir

[3]Assistant Professor, Department of Public Administration, CT.C, Islamic Azad University, Tehran, Iran. Email Address: d.gholam@iau.ac.ir

[4]Assistant Professor, Department of Financial Management and Accounting, ST.C, Islamic Azad University, Tehran, Iran. Email Address: radfar@iau.ac.ir

ARTICLE INFO

Article history:

Article Type: Research paper

Received: 8 January 2025

Received in revised form: 23 June 2025

Accepted: 20 September 2025

Available online: 22 October 2025

Keywords:

Cybersecurity

Electronic Banking

Cyber Threats

ABSTRACT

This research was a fundamental research in terms of purpose. The analysis of the present study was conducted qualitatively using the grounded theory approach. The statistical population consisted of 15 experts in the field of electronic banking and cybersecurity. The sampling method was purposive. The data collection tool was semi-structured interviews with semi-open-ended questions, for which the opinions of the supervisors and consultants were used. In this research, ATLAS TI software was used for qualitative content analysis. In this study, the interviews were first rewritten and analyzed, and then in subsequent interviews, an attempt was made to identify subcategories and the relationships between them using axial coding for theoretical saturation and better understanding of the subject. Using selective coding and with internal consistency and determining the dimensional levels of the categories, the relationships between the concepts were validated. Accordingly, the linear relationship between the research categories, including the central category, causal conditions, underlying conditions, intervening conditions, strategies, and consequences, was determined, and finally, the qualitative research model was presented.

Cite this article: H. Babaee, M. Aligholi, D. Gholamzadeh, and M. R. Radfar, "Presenting a Cybersecurity Model in Electronic Banking," Journal of Passive Defence, vol. 16, no. 3, pp. 39-54, 2025. **DOR: 20.1001.1.20086849.1404.16.3.3.1**

Publisher: Imam Hossein University.

پدافند غیرعامل

سال پانزدهم، شماره ۳، پاییز ۱۴۰۴، (پیاپی ۶۳): صص ۵۴-۳۹

شاپای چاپی: ۶۹۴۹-۲۰۰۸ | **شاپای الکترونیکی:** ۸۰۳۰-۲۹۸۰

ارائه مدل امنیت سایبری در بانکداری الکترونیک

حسین بابایی[۱]، منصوره علیقلی[۲*]، داریوش غلامزاده[۳]، محمدرضا رادفر[۴]

[۱] دانشجوی دکتری گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: hossein.babaee@iau.ac.ir

[۲] دانشیارگروه مدیریت بازرگانی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: man.aligholi@iau.ac.ir

[۳] استادیارگروه مدیریت دولتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: d.gholam@iau.ac.ir

[۴] استادیار گروه مدیریت مالی و حسابداری، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: radfar@iau.ac.ir

چکیده

این پژوهش از نظر هدف، پژوهشی بنیادی بود. تحلیل مطالعه حاضر به صورت کیفی با استفاده از رویکرد نظریه‌پردازی داده‌بنیاد 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 نیمه ساختاریافته با پرسش‌های نیمه باز پاسخ بود که بدین منظور از نظرات اساتید راهنما و مشاور استفاده گردید. در این پژوهش برای تحلیل محتوای کیفی از نرم‌افزار ATLAS TI استفاده شد. در این مطالعه، ابتدا مصاحبه‌ها بازنویسی و مورد تحلیل قرار گرفت و سپس در مصاحبه‌های بعدی تلاش شد برای اشباع نظری و درک بهتر موضوع، با استفاده از کدگذاری محوری مقوله‌های فرعی و روابط بین آنها شناسایی شود. با استفاده از کدگذاری انتخابی و با انسجام درونی و تعیین سطوح ابعادی مقوله‌ها، روابط میان مفاهیم اعتباربخشی شد. بر این اساس ارتباط خطی میان مقوله‌های پژوهش شامل مقوله محوری، شرایط علی، شرایط زمینه‌ای، شرایط مداخله‌گر، راهبردها و پیامدها مشخص شد و در نهایت مدل کیفی پژوهش ارائه شد.

مشخصات مقاله

تاریخچه مقاله:

نوع مقاله: علمی پژوهشی

دریافت: ۱۴۰۳/۱۰/۱۹

بازنگری: ۱۴۰۴/۰۴/۰۲

پذیرش: ۱۴۰۴/۰۶/۲۹

ارائه آنلاین: ۱۴۰۴/۰۷/۳۰

کلیدواژه‌ها:

امنیت سایبری

بانکداری الکترونیک

تهدیدات سایبری

استناد: بابایی، حسین، علیقلی، منصوره، غلامزاده، داریوش، رادفر، محمدرضا، " ارائه مدل امنیت سایبری در بانکداری الکترونیک"، نشریه پدافند غیرعامل، دوره ۱۶، شماره۳، صفحات ۵۴-۳۹، ۱۴۰۴. DOR: 20.1001.1.20086849.1404.16.3.3.1

ناشر: دانشگاه جام امام حسین(ع).

۱- مقدمه و بیان مساله

عصری که در آن زندگی می‌کنیم را می‌توان عصر سایبری نام نهاد. در حال حاضر شاهد شکل‌گیری فضایی هستیم که در آن فعالیت‌های گوناگونی مانند اطلاع‌رسانی، ارائه خدمات، مدیریت و کنترل ارتباطات، از طریق سازوکارهای فضای سایبری انجام می‌پذیرد. تهدید امنیتی را باید در عصر ارتباطات و جهانی‌شدن برای کشورها از جمله تهدیدات حوزه سایبری دانست. یکی از ابزارهای جهانی شدن، فناوری‌های سایبری می‌باشد در کنار فرصت‌های بی‌شماری که برای کشور ایجاد می‌کند، یک تهدید بسیار جدی است که عمدتا خیلی به صورت جدی به آن پرداخته نمی‌شود. لذا نیاز است این موضوع، به طور مشخص بررسی گردد تا بتوان مناسب با آن اقدامات لازم به عمل آورد[۱].

امروزه ورود به فضای سایبری حاصل از فناوری اطلاعات و ارتباطات، دوره جدیدی از تمدن بشر را به وجود آورده است. در این راستا حضور نظام بانکی پیشرفته جهت ورود به بازارهای بین‌المللی، جز الزامات هر کشوری می‌باشد که در حال حاضر با پیشرفت فناوری اطلاعات تمامی صنایع در جهان از جمله صنعت بانکداری به سرعت به سمت این تحولات پیش رفته است. بنابراین همراه با ارتقا و توسعه فناوری‌های نوین، به دلیل وجود ضعف‌هایی که بانکداری سنتی با خود به همراه داشت، سبب شد تا سازوکار بانکی جز نخستین سازمان‌هایی باشد که از دستاوردهای فناوری اطلاعات، شبکه و اینترنت استفاده نماید. بدین ترتیب بانکداری الکترونیکی جایگزین بانکداری سنتی گردید[۲].

پس از گسترش اینترنت، دستگاه‌های هوشمند و دستگاه‌های تلفن همراه، در زمان ما، توجه به امنیت سایبری و نحوه محافظت از خود در فضای دیجیتال، ضروری شده است و امنیت سایبری یکی از رایج‌ترین موضوعات در روزگار ما است. سطح بالای ناامنی در فضای سایبری و زیرساخت‌های اساسی آن در برابر طیف گسترده‌ای از خطرات ناشی از تهدیدات الکترونیکی و خطرات مادی آسیب‌پذیر شده است زیرا بازیگران به‌صورت الکترونیکی و همچنین دولت-ملت‌ها از نقاط ضعف مخالفان خود برای سرقت اطلاعات و منابع مالی و توسعه قابلیت‌ها سوء استفاده می‌کنند [۳].

علیرغم منافعی که پیشرفت فناوری برای بشر در برداشته، در معرض تهدید و سوء استفاده نیز بوده است. جهت جلوگیری از این خطرها، مبحث امنیت مطرح می‌گردد که عامل موثری جهت پذیرش و استفاده بیشتر افراد از خدمات بانکداری الکترونیک می‌باشد[۴].

حملات سایبری که در سال‌های اخیر به برخی از بانک‌های ایرانی شده است و موجب افشای اطلاعات مربوط به حساب مشتریان شده است، اهمیت توجه به مسئله امنیت در بانکداری الکترونیک را ضروری می‌سازد. اجرای اقدامات موفق امنیت سایبری برای تضمین یک محیط شبکه‌ای امن در فضای سایبری و تلاش مشترک سازمان‌ها، دولت و مشارکت بین کشوری، کارایی و اثربخشی راه‌حل‌های امنیت سایبری را بیشتر می‌کند. مطالعات صورت گرفته قبلی، بیشتر به بررسی ریسک‌های امنیت سایبری در حوزه بانکی پرداخته‌اند و تاثیر متغیرهای این حوزه را بر امنیت سایبری بررسی نکرده‌اند. در برخی دیگر از تحقیقات، متغیرهای مهم را در مدل ارائه شده در نظر نگرفته‌اند. همچنین در تحقیقات داخلی صورت گرفته در حوزه بانکداری الکترونیک، از منظر امنیت سایبری به این مسئله، پرداخته نشده است و هیچ مدلی نیز در این خصوص ارائه نگردیده است.

بنابراین شکاف نظری در تحقیقات، وجود یک مدل است که بتواند بانکداری الکترونیک را از منظر امنیت سایبری مورد ارزیابی قرار دهد و معیاری از سطح امنیت را برآورده سازد. هدف از این پژوهش، به دست آوردن داده‌های موجود در بانکداری الکترونیک و تعیین متغیرهای مهم امنیت سایبری و در نهایت ارائه مدل امنیت سایبری در بانکداری الکترونیک می‌باشد. لذا با ارائه مدلی بر اساس نظرات خبرگان این صنعت، برای استفاده بانک از فناوری اطلاعات و ارتباطات برای ارائه خدمات الکترونیک به مشتریان، می توان 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. با توجه به مباحث مطرح شده، مسئله اصلی پژوهش حاضر این است که: "مدل امنیت سایبری در بانکداری الکترونیک چگونه است؟"

سوالات پژوهش عبارتند از:

- در بانکداری الکترونیک متغیرهای مهم امنیت سایبری کدامند؟
- مدل امنیت سایبری در بانکداری الکترونیک چگونه است؟

۲- مبانی نظری

بانکداری الکترونیک، یکپارچه‌سازی بهینه همه فعالیت‌های یک بانک از طریق به‌کارگیری فناوری اطلاعات است که امکان ارائه کلیه خدمات مورد نیاز مشتریان را بدون حضور فیزیکی فراهم می‌کند[۵].

امنیت در بانکداری الکترونیک به طور عمومی شامل دور نگهداشتن افراد غیرمجاز از دسترسی به اطلاعات و اجازه دادن به افراد مجاز جهت دسترسی به دارایی‌های با ارزش می‌باشد. اکثر فعالیت‌های بانک‌ها با اطلاعات شخصی و حساس مشتریان و خریداران درگیر هستند پس امنیت این اطلاعات از ارزش زیادی برخوردار است[۶]. برای افزایش و توسعه امنیت در بانکداری الکترونیک، از روش‌هایی مثل استفاده از رمز عبور، اعمال سازوکارهای رمزنگاری، به کار بردن امضاهای الکترونیکی، گواهی‌های دیجیتال، دیوارهای آتش و دستورالعمل‌های امنیتی استفاده می‌شود[۷].

امنیت سایبری، مجموعه ابزارها، سیاست‌ها، مفاهیم امنیتی، اعمال امنیتی، رویکردهای مدیریت بحران، آموزش و فناوری‌هایی می‌باشد که در راستای در دسترس بودن، مورد اطمینان بودن و صحت اطلاعات می‌باشد که به منظور حفاظت از فضای سایبری و دارایی کاربران و سازمان‌ها به کار می‌رود. دارایی‌های کاربران و سازمان‌ها شامل خدمات زیربنایی، برنامه‌های کاربردی، خدمات مخابراتی و کلیت اطلاعات ذخیره شده یا انتقال یافته در فضای سایبری می‌باشد[۸].

تهدیدهای سایبری پدیده‌ای است که در دهه‌های اخیر، همزمان با تحول فناوری اطلاعات و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت در سراسر جهان ظهور پیدا کرده است، به گونه‌ای که امروزه چالش تهدیدهای سایبری، هم مهم و هم پیچیده به نظر می‌رسد. این اهمیت و پیچیدگی ناشی از ماهیت جدید تهدیدهای سایبری و ویژگی‌ها و نمودهای منحصربه‌فردی است که شناخت از آن را بسیار مهم و ضروری می‌نماید[۹].

بنابراین، تعریف مفهومی امنیت سایبری عبارتست از: امنیت سایبری شامل تمام فعالیت‌های لازم برای محافظت از فضای سایبری، کاربران و افراد تحت تاثیر آن در برابر تهدیدات سایبری است. تعریف عملیاتی امنیت سایبری عبارتست از: منظور از امنیت سایبری در این پژوهش میزان نمره‌ای است که مشارکت‌کنندگان، استادان، صاحب‌نظران و متخصصین آشنا به حوزه امنیت سایبری از پرسشنامه محقق به دست می‌آورند. تعریف مفهومی بانکداری الکترونیک عبارتست از: بانکداری الکترونیک استفاده از فناوری‌های پیشرفته نرم‌افزاری و سخت‌افزاری مبتنی بر شبکه و مخابرات برای تبادل منابع و اطلاعات مالی به صورت الکترونیکی است و نیازی به حضور فیزیکی مشتری در شعبه نیست. تعریف عملیاتی بانکداری الکترونیک عبارتست از: منظور از بانکداری الکترونیک در این پژوهش میزان نمره‌ای است که مشارکت‌کنندگان، استادان، صاحب نظران و متخصصین آشنا به حوزه بانکداری الکترونیک از پرسشنامه محقق به دست می‌آورند.

۳- پیشینه پژوهش

مدل ارائه شده در پژوهش وجدانی و همکاران[۸] برای بررسی اثر گذاری حریم خصوصی و امنیت خدمات بانکداری الکترونیک بر وفاداری مشتریان بانکی با تاکید بر قابلیت اطمینان، با روش تحقیق کمی براساس مدل مفهومی شانکار و همکاران بصورت پیمایشی ارائه گردید. متغیرهای قابلیت اطمینان، حریم خصوصی و امنیت، طراحی وب سایت، خدمات مشتری و پشتیبانی خدمات بانکداری الکترونیکی به عنوان متغیرهای مستقل موثر در امنیت سایبری در نظر گرفته شدند و سایر شرایط علی در نظر گرفته نشدند. متغیر مشارکت مشتری در بانکداری الکترونیکی به عنوان متغیر تعدیل کننده مشخص شد و سایر راهبردها در نظر گرفته نشدند. متغیر اعتماد اولیه به عنوان متغیر مداخله گر بررسی شد و سایر شرایط مداخله گر بررسی نشدند. متغیر وفاداری مشتریان به عنوان متغیر وابسته در نظر گرفته شده است و سایر پیامدها در نظر گرفته نشدند.

مدل ارائه شده در پژوهش موسوی و همکاران[۹] برای بررسی تاثیر ابعاد عینی امنیت سامانه‌های پرداخت الکترونیکی بر درک مشتریان از امنیت و اعتماد، بر اساس پرسشنامه کیم و همکاران با روش کمی و بصورت پیمایشی با هدف کاربردی در شعب بانک ملی استان کهگیلویه و بویر احمد، بود. متغیرهای حفاظت‌های فنی و فرآیندهای تراکنش، بیانیه‌های امنیتی به عنوان متغیرهای مستقل در نظر گرفته شده‌اند. متغیرهای امنیت ادراک شده و اعتماد اداراک شده به عنوان متغیرهای میانجی در نظر گرفته شده‌اند. متغیر بکارگیری سامانه‌ی پرداخت الکترونیکی به عنوان متغیر وابسته در نظر گرفته شده است. در مدل مذکور،

فقط ابعاد عینی امنیت در سامانه‌ی پرداخت الکترونیکی بانکی بر اساس درک مشتریان از امنیت و اعتماد بانکداری الکترونیک، به عنوان شرایط علی مورد بررسی قرار گرفت و سایر ابعاد امنیت مورد بررسی قرار نگرفت. از طرفی فقط اعتماد مشتری به عنوان پیامد امنیت در نظر گرفته شد و سایر پیامدها در نظر گرفته نشد.

مدل ارائه شده توسط آپرناک و همکاران[۱۰] برای بررسی رابطه بین امنیت ادراک‌شده و اعتماد مشتریان به بانکداری الکترونیک مبتنی بر رویکرد NFC-Mobile، بر اساس پژوهش کیم و همکاران بصورت پیمایشی و کاربردی برای بانک ملی شعب تهران بود. فقط امنیت درک شده و اعتماد درک شده به عنوان دومتغیر میانجی در رابطه بین ابعاد عینی به عنوان شرایط علی و میزان استفاده از سامانه‌ی پرداخت الکترونیک به عنوان پیامد بررسی گردید و سایر شرایط زمنیه ای بررسی نگردید.

الگوی ارائه شده توسط نجفی و همکاران[۶] برای شناسایی و رتبه‌بندی عوامل مؤثر بر تعامل بانک‌ها و فناوری‌های نوین مالی (فین‌تک‌ها) با رویکرد ترکیبی- اکتشافی و بصورت توصیفی-پیمایشی با هدف کاربردی انجام شد. عوامل ذینفعان شامل: ویژگی های فین‌تک‌ها، ویژگی‌های مشتریان، ویژگی‌های تامین‌کنندگان و ویژگی‌های سهامداران بود و سایر شرایط علی در نظر گرفته نشد. عوامل سازمانی شامل: فرهنگ سازمانی، ساختار سازمانی و ریسک‌های سازوکارهای بانکی بودند و سایر عوامل زمینه‌ای در نظر گرفته نشدند. عوامل محیطی: شامل: محیط سیاسی و قانونی، محیط اقتصادی، محیط رقابتی، محیط فناوری بود ولی سایر شرایط مداخله‌گر در نظر گرفته نشد. عوامل مالی شامل: دسترسی بانک‌ها به منابع مالی و نیاز شرکت‌های ارائه دهنده خدمات فناوری به منابع مالی و تمایل به سرمایه-گذاری در فین‌تک بود و سایر شرایط راهبردی در نظر گرفته نشد. مقوله اصلی تعامل بین بانک‌ها و فین‌تک‌ها بود و از منظر امنیت سایبری مورد بررسی قرار نگرفت.

چارچوب ارائه شده توسط آدِدویین و همکاران[۱۱] برای بررسی ابعاد مختلف امنیت سایبری در صنعت، تحلیل حوادث اخیر امنیت سایبری، پیچیدگی‌های تهدیدات سایبری، پیامدهای مالی نقض‌ها و استحکام اقدامات فعلی امنیت سایبری در بانکداری با روش کیفی انجام شد. جمع‌آوری داده‌ها با تمرکز بر تحلیل اسناد و کاوش مطالعات موردی انجام شد. تجزیه و تحلیل کلان‌داده، هوش مصنوعی و روش‌های ارزیابی مداوم ریسک برای پیمایش مؤثر به عنوان شرایط علی مطرح شد. ارزیابی تأثیر مالی حملات سایبری، ارزیابی اثربخشی چارچوب‌های موجود امنیت سایبری و تدوین توصیه‌های استراتژیک به عنوان شرایط مداخله-گر مطرح شد. عوامل سرمایه‌گذاری‌های استراتژیک در فناوری، آموزش و همکاری به عنوان راهبردها مطرح شد. تاب‌آوری امنیت سایبری در حفاظت از دارایی‌های مالی و اعتماد مشتری در برابر پس‌زمینه تحول دیجیتال به عنوان پیامدها ارائه گردید.

چارچوب ارائه شده توسط موهونا[۱۲] برای بررسی تهدیدات نوظهور امنیت سایبری در بخش بانکداری بر اساس داده‌های اولیه حاصل از یک نظرسنجی و داده‌های ثانویه حاصل از گزارش‌های دولتی، وب‌سایت، روزنامه‌ها، وبلاگ‌های آنلاین، مجلات و مقالات تحقیقاتی و با هدف کاربردی برای کمک به قانونگذارانی و توسعه بانکداری الکترونیکی بنگلادش و یافتن چالش‌های امنیتی سایبری موجود در بخش بانکداری الکترونیکی بود. در دسترس بودن شبکه، استفاده ساده، سریع و کاربرپسند، گسترش فیبر نوری برای زیرساخت‌های بانکداری الکترونیک به عنوان شرایط علی بررسی شد. تقویت چارچوب قانونی، مقررات مربوط به جرایم سایبری، مجازات و سازوکار محاکمه به عنوان شرایط زمینه‌ای بررسی شد. افزایش آگاهی، درک مردم از نقش‌ها و مسئولیت‌های خود، ادامه تشدید اجرای قانون، آموزش کافی و حمایت فناورانه برای توسعه نیروی انسانی به عنوان راهبردها بررسی شد. امنیت داده‌های مشتری و تراکنش‌های امن مؤسسه مالی به عنوان پیامدها بررسی شد.

مدل ارائه شده توسط الدحیدهاوی و همکاران[۳] برای تحلیل اثرات متغیرهای فین‌تک بر امنیت سایبری با روش کمی با هدف کاربردی برای بانک‌های عراقی و لبنانی با استفاده از پرسشنامه بود. متغیرهای خود کارآمدی (SE)، به عنوان شرایط علی، فرهنگ فناوری (TC) به عنوان شرایط زمینه‌ای، شایستگی و مهارت (CS) به عنوان شرایط مداخله‌گر، آزمایش امنیت اطلاعات (IS)، به عنوان راهبرد در نظر گرفته شدند. متغیر امنیت سایبری به عنوان متغیر وابسته و مقوله اصلی در نظر گرفته شد در نظر گرفته شد. پیامد ها نیز شامل ۱۶ مقوله بودند.

مدل امنیتی القازو و همکاران[۱۳] برای تحلیل امنیت سایبری بانکداری اینترنتی در کشورهای نوظهور، یک مدل جدید برای کاهش خطر امنیت سایبری برای پر کردن شکاف بین

بانک‌ها و مشتریان بود. مدل پیشنهادی بر اساس نتایج نظرسنجی‌های انجام شده در مورد بانکداری اینترنتی در عربستان سعودی، پاکستان و هند است. سوالات نظرسنجی بر اساس دانش کاربر از امنیت سایبری و آگاهی از تهدیدات رایج در بانکداری اینترنتی بود. این مدل بیان می‌کند که بانک‌ها می‌توانند سیاست‌های امنیتی خود را برای تضمین تجربه بانکی امن‌تر برای کاربران اعمال کنند. از سوی دیگر، کاربران باید دستورالعمل‌های ارائه شده توسط بانک را برای اطمینان از تجربه بانکداری اینترنتی ایمن دنبال کنند.

مدل ارائه شده توسط کیم و همکاران[۱۴] در مورد پذیرش خدمات فین‌تک با تمرکز بر خدمات پرداخت موبایلی، مشخص کرد وقتی کاربر از طریق عوامل مختلف احساس «مفید بودن» می‌کند، این تأثیر زیادی بر «نیت استفاده» دارد. تحرک شخصی، سودمندی، سهولت استفاده، تأثیر اجتماعی به عنوان شرایط علی در نظر گرفته شدند. خودکارآمدی و حفظ حریم خصوصی به عنوان راهبرد و اعتبار به عنوان مقوله اصلی و متغیر وابسته قصد استفاده به عنوان پیامد در نظر گرفته شد.

۴- روش شناسی پژوهش

این پژوهش از نظر هدف، پژوهشی بنیادی است. تحلیل مطالعه حاضر به صورت کیفی با استفاده از رویکرد نظریه‌پردازی داده‌بنیاد 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 بودکه از نظرات اساتید راهنما و مشاور استفاده گردید. در این پژوهش برای تحلیل محتوای کیفی از نرم‌افزار ATLAS TI استفاده شد.

برای تدوین نظریه داده‌بنیاد، ۵ مرحله تحلیلی وجود دارد که درون این مراحل ۹ گام دنبال می‌شود:

۱ - تدوین طرح تحقیق

طرح تحقیق : طراحی پیکربندی کلی یک تحقیق است. تعیین اینکه چه اطلاعاتی از کجا و به چه میزان باید برای ارائه پاسخ-های مناسب به سوال اصلی پژوهش گردآوری و تفسیر شود.

گام اول : مرور متون تخصصی و طراحی سوال تحقیق:

تعیین سوال تحقیق تلاش‌ها را متمرکز، پراکندگی را محدود و روایی بیرونی را تقویت می‌کند.

گام دوم : انتخاب ویژگی‌های کلی موردها : این گام تلاش‌ها را بر موردهایی که از لحاظ نظری مفید هستند متمرکز می‌کند.

۲ - گردآوری داده‌ها

گام سوم : تدوین دستورالعمل گردآوری داده‌ها

گام چهارم : ورود به میدان تحقیق و گردآوری و تحلیل داده‌ها به صورت همزمان

۳ - تنظیم داده‌ها

گام پنجم : پیاده‌سازی داده‌ها و ضمیمه کردن یادداشت‌های میدانی به آن

۴ - تحلیل داده‌ها

گام ششم : آغاز فرایند تحلیل، با تحلیل داده‌ها

استفاده از کدگذاری باز، محوری و انتخابی، تدوین مفاهیم، مقولات و قضایا، ایجاد پیوند بین یک مقوله و مقوله‌های فرعی آن، تلفیق مقولات برای تدوین چارچوب نظری.

گام هفتم : فرایند نمونه‌گیری نظری و گردآوری داده‌ها برای نظریه پردازی

گام هشتم : پایان فرآیند (اشباع نظری زمانی که میسر شد)

فرایند دستیابی به نظریه داده‌بنیاد هم نظام‌مند و دقیق و هم خلاقانه است و با گردآوری، کدگذاری، و تجزیه و تحلیل همزمان داده‌ها از هنگام اولین مصاحبه یا اولین مشاهده آغاز می‌شود.

لازمهٔ تجزیه و تحلیل غوطه‌ور شدن محقق در اطلاعات است. به موازات غوطه‌ور شدن محقق در داده‌ها، به جملات و مفاهیم اصلی آن دست می‌یابد.

۵ - مقایسه متون

گام نهم : مقایسه نظریه در حال ظهور با متون موجود.

۵- یافته‌های پژوهش

این مطالعه بر اساس دیدگاه ۱۵ نفر از خبرگان انجام شده‌است. از نظر جنسیت ۱۳ نفر مرد و ۲ نفر نیز زن بودند. در نهایت ۴ نفر بین ۱۰ تا ۱۵ سال سابقه‌کاری داشته و ۱۱ نفر نیز بالای ۱۵ سال سال تجربه کاری داشتند.

در کدگذاری باز، ابتدا داده‌های حاصل از مصاحبه‌ها به دقت مورد مطالعه، بررسی و تحلیل قرار گرفتند، سپس عمل مفهوم‌سازی صورت گرفت و به داده‌هایی که از نظر مفهوم شبیه به یکدیگر بودند، با نام‌های متناسب، برچسب زده شد. برچسب‌گذاری کدها با استناد به مصاحبه‌ها انجام شده‌است و محقق سعی کرده‌است تا حد ضرورت به بینش افراد نسبت به پاسخ داده شده پایبند باشد تا از هرگونه سوگیری احتمالی و ناخواسته تا حدامکان جلوگیری

شود. محقق در تمام فرایند کدگذاری‌ها به حساسیت نظری که از اصول تحقیق نظریه‌پردازی داده‌بنیاد است پایبند بوده است و این کار را جهت غنای هرچه بیشتر تحقیق انجام داده‌است. نمونه کدها و مصاحبه‌های مرتبط در جدول (۱) آمده است:

جدول(۱): کدهای شناسایی شده براساس مصاحبه

کد باز	مصاحبه
بلاک‌چین	بلاک‌چین به عنوان یک دفتر کل توزیع‌شده و تغییرناپذیر می‌تواند باعث افزایش شفافیت و امنیت تراکنش‌ها در سامانه‌های بانکداری الکترونیک شود. به دلیل ساختار غیرمتمرکز آن، تغییر یا دستکاری داده‌ها بسیار دشوار است، که این امر سطح امنیت را به‌طور قابل‌توجهی افزایش می‌دهد. همچنین، استفاده از بلاک‌چین در فرآیندهای احراز هویت و قراردادهای هوشمند می‌تواند از حملات سایبری جلوگیری کند.
یادگیری ماشین	الگوریتم‌های یادگیری ماشین به تجزیه و تحلیل داده‌های بزرگ کمک می‌کنند تا الگوهای مشکوک و غیرمعمول را شناسایی کرده و پیش‌بینی حملات سایبری را بهبود بخشند. همچنین، یادگیری ماشین می‌تواند در شناسایی تقلب‌های مالی، کاهش ریسک‌های امنیتی و بهبود فرآیندهای تصمیم‌گیری در بانکداری الکترونیکی مؤثر باشد.
اینترنت اشیاء	دستگاه‌های متصل به اینترنت اشیاء به بانک‌ها امکان می‌دهند تا اطلاعات بیشتری از کاربران خود دریافت کنند و خدمات بهتری ارائه دهند. اما این دستگاه‌ها نیز ممکن است نقاط ضعف جدیدی برای حملات سایبری ایجاد کنند. امنیت در IoT برای بانکداری الکترونیکی به معنای محافظت از تمام دستگاه‌ها و ارتباطات آنها است تا از حملات سایبری جلوگیری شود.
محاسبات ابری	استفاده از فضای ابری برای ذخیره و پردازش داده‌های بانکی می‌تواند انعطاف‌پذیری و کارایی سامانه‌های بانکداری را افزایش دهد. با این حال، امنیت داده‌های ابری چالش‌های جدیدی به همراه دارد. مدل امنیتی باید شامل دستورالعمل‌های امنیتی قوی مانند رمزگذاری داده‌ها و مدیریت دسترسی باشد تا اطلاعات حساس کاربران محافظت شود.
هوش مصنوعی	هوش مصنوعی در امنیت سایبری به عنوان یک ابزار قدرتمند برای تشخیص تهدیدات پیشرفته و واکنش سریع به حملات عمل می‌کند. سامانه‌های مبتنی بر هوش مصنوعی می‌توانند به‌طور مداوم فعالیت‌های شبکه را پایش کرده و از حملات شناسایی‌شده جلوگیری کنند. همچنین، هوش مصنوعی می‌تواند در بهینه‌سازی راهکارهای امنیتی و خودکارسازی فرآیندهای امنیتی مؤثر باشد.
حجم بالای داده‌ها	بانکداری الکترونیک روزانه حجم وسیعی از تراکنش‌ها و اطلاعات حساس مالی را مدیریت می‌کند. افزایش حجم داده‌ها به معنای نیاز به زیرساخت‌های قدرتمند برای ذخیره، پردازش، و انتقال این داده‌ها است. امنیت در این حجم از داده‌ها چالش‌برانگیز است زیرا با افزایش حجم، ریسک بیشتری برای نشت داده‌ها و حملات سایبری وجود دارد. به‌کارگیری فناوری‌هایی نظیر هوش مصنوعی و محاسبات ابری می‌تواند به مدیریت حجم عظیم داده‌ها کمک کند و از دسترسی غیرمجاز جلوگیری کند.
پیچیدگی داده‌ها	داده‌های بانکداری الکترونیک نه تنها از نظر حجم، بلکه از نظر ساختار و ارتباطات پیچیده هستند. این داده‌ها شامل تراکنش‌های مالی، اطلاعات شخصی کاربران، و اطلاعات سامانه‌ای می‌باشند که هر کدام از جنبه‌های مختلفی نیاز به محافظت دارند. پیاده‌سازی یک مدل امنیتی که بتواند این پیچیدگی‌ها را مدیریت کند، مستلزم استفاده از فناوری‌های پیشرفته‌ای مانند بلاک‌چین و یادگیری ماشین است که بتوانند به تجزیه و تحلیل داده‌های پیچیده و پیش‌بینی تهدیدات کمک کنند.
مدیریت داده‌ها	مدیریت داده‌ها به معنای نحوه ذخیره‌سازی، دسترسی، و حفاظت از داده‌ها در بانکداری الکترونیک است. ایجاد ساختارهای قوی برای مدیریت مجوزها و دسترسی، رمزگذاری داده‌ها، و اجرای سامانه‌های نظارتی می‌تواند از نفوذهای احتمالی و دسترسی غیرمجاز به داده‌های حساس جلوگیری کند. استفاده از بلاک‌چین برای تضمین شفافیت و تغییرناپذیری داده‌ها نیز در این زمینه موثر است.
به‌روزرسانی داده‌ها	در بانکداری الکترونیک، به‌روزرسانی داده‌ها به معنای به‌روزرسانی مستمر سامانه‌ها، پایگاه‌های داده، و زیرساخت‌های امنیتی است. به‌روزرسانی به موقع داده‌ها و دستورالعمل‌های امنیتی می‌تواند آسیب‌پذیری‌ها را کاهش دهد و از سوءاستفاده از نقص‌های امنیتی جلوگیری کند. هوش مصنوعی می‌تواند برای شناسایی نقاط ضعف و پیشنهاد به‌روزرسانی‌های موردنیاز به‌کار گرفته شود.

جدول(۱): کدهای شناسایی شده براساس مصاحبه

کد باز	مصاحبه
حملات سایبری	تهدیدات سایبری مانند حملات DDoS، فیشینگ، و هک سامانه‌های بانکی در بانکداری الکترونیک بسیار رایج هستند. مدل امنیتی باید توانایی شناسایی و جلوگیری از این حملات را داشته باشد. استفاده از الگوریتم‌های یادگیری ماشین و هوش مصنوعی می‌تواند به پیش‌بینی و شناسایی تهدیدات کمک کند، در حالی که بلاک‌چین و رمزنگاری قوی می‌توانند از دسترسی غیرمجاز و تغییر داده‌ها جلوگیری کنند.
حملات رباتیک	حملات رباتیک به حملاتی اطلاق می‌شود که توسط ربات‌ها یا نرم‌افزارهای خودکار انجام می‌شوند. این نوع حملات معمولاً شامل فعالیت‌هایی مانند خودکار کردن فرآیندهای فیشینگ، انجام تراکنش‌های تقلبی یا تلاش برای نفوذ به سامانه‌های بانکی هستند. برای مقابله با این نوع حملات، استفاده از سامانه‌های امنیتی پیشرفته و ابزارهای تشخیص نفوذ (IDS) می‌تواند کمک‌کننده باشد. همچنین، اجرای تدابیر امنیتی مانند CAPTCHA می‌تواند مانع از ورود ربات‌ها به سامانه‌ها شود.
حملات DDoS	این نوع حملات به هدف قرار دادن سرورهای بانک‌ها با حجم زیادی از ترافیک غیرمجاز انجام می‌شود، به طوری که سامانه قادر به پاسخگویی به درخواست‌های مشروع نخواهد بود. حملات DDoS می‌تواند باعث از کار افتادن سامانه‌های بانکداری آنلاین و کاهش اعتماد مشتریان شود. برای مقابله با این حملات، استفاده از راهکارهای توزیع بار (load balancing)، فایروال‌های پیشرفته و سامانه‌های شناسایی و پاسخ به تهدیدات ضروری است.
شناسایی رفتارهای کاربر	شناسایی رفتارهای کاربر به معنای تجزیه و تحلیل نحوه تعامل کاربران با سامانه‌های بانکداری الکترونیک است. این فرآیند به شناسایی الگوهای عادی و غیرعادی کمک می‌کند. اطلاعات جمع‌آوری‌شده از این تجزیه و تحلیل می‌تواند برای شناسایی رفتارهای مشکوک یا حملات سایبری مورد استفاده قرار گیرد. فناوری یادگیری ماشین می‌تواند به شناسایی و پیش‌بینی رفتارهای غیرعادی کمک کند.
تحلیل پشرفته الگوهای دسترسی کاربر	این فرآیند شامل تجزیه و تحلیل دقیق الگوهای دسترسی کاربران به اطلاعات و خدمات بانکی است. با استفاده از الگوریتم‌های پیشرفته و یادگیری ماشین، می‌توان به شناسایی الگوهای معمول و غیرمعمول دسترسی پرداخت. این اطلاعات می‌تواند به تشخیص حملات و سوءاستفاده‌های احتمالی کمک کند. همچنین، تحلیل الگوهای دسترسی می‌تواند در پیشگیری از تقلب‌های مالی مؤثر باشد.
شناسایی رفتارهای مشکوک	رفتارهای مشکوک می‌توانند شامل تلاش‌های مکرر برای ورود به سامانه، تغییرات غیرمعمول در الگوهای تراکنش، یا دسترسی از مکان‌های غیرمعمول باشند. با استفاده از ابزارهای تحلیلی و یادگیری ماشین، می‌توان به شناسایی این نوع رفتارها و هشدار به مسئولین امنیتی پرداخت تا اقدامات پیشگیرانه انجام شود.
به‌روزرسانی مشخصات بیومتریک کاربر	این فرآیند شامل حفظ و به‌روزرسانی اطلاعات بیومتریک کاربران مانند اثر انگشت، تشخیص چهره، و اسکن چشم است. به‌روزرسانی‌های منظم این مشخصات برای اطمینان از صحت و دقت آن‌ها ضروری است. تغییرات در وضعیت کاربر، مانند جراحت‌های فیزیکی یا تغییرات ظاهری، می‌تواند بر دقت سامانه‌های بیومتریک تأثیر بگذارد. بنابراین، به‌روزرسانی مداوم این اطلاعات می‌تواند به جلوگیری از سوءاستفاده‌های هویتی و دسترسی‌های غیرمجاز کمک کند.
تطبیق هویتی در دسترسی‌های غیرمجاز	سامانه‌های تطبیق هویتی باید قادر به شناسایی و رد کردن تلاش‌های غیرمجاز باشند. استفاده از چندین لایه احراز هویت، مانند احراز هویت دو عاملی (FA۲) و سامانه‌های هوش مصنوعی برای شناسایی الگوهای مشکوک، می‌تواند به این فرآیند کمک کند.
درک امنیت اطلاعات	ایجاد فرهنگ امنیتی قوی در میان کارکنان و مشتریان می‌تواند به پیشگیری از حملات سایبری و کاهش ریسک‌ها کمک کند. آموزش‌های مستمر درباره امنیت سایبری و شناسایی تهدیدات می‌تواند به بهبود درک و اقدامات امنیتی افراد کمک کند.
بی‌ثباتی فرهنگ تجارت دیجیتال	با توجه به تغییرات سریع در فناوری و رفتار مصرف‌کنندگان، بانک‌ها باید توانایی انعطاف‌پذیری و تطبیق با شرایط جدید را داشته باشند. این بی‌ثباتی می‌تواند چالش‌هایی برای امنیت سایبری ایجاد کند، زیرا مهاجمان ممکن است از ضعف‌ها و نقاط ضعف جدید استفاده کنند. بنابراین، یک مدل امنیتی باید توانایی پیش‌بینی و پاسخ به این تغییرات را داشته باشد و

جدول(۱): کدهای شناسایی شده براساس مصاحبه

کد باز	مصاحبه
	راهبردهای لازم برای مقابله با تهدیدات جدید را شامل شود.
رفتارهای توده‌ای	رفتارهای توده‌ای به الگوهای رفتاری کاربران در یک جامعه یا گروه بزرگ اشاره دارد که می‌تواند تأثیرات مثبت یا منفی بر امنیت سایبری داشته باشد. به عنوان مثال، اگر اکثریت کاربران نسبت به استفاده از فناوری‌های جدید مانند بانکداری الکترونیک خوش‌بین باشند، ممکن است به سرعت پذیرش بالایی منجر شود. اما اگر ترس‌ها و نگرانی‌های عمومی نسبت به امنیت اطلاعات وجود داشته باشد، این امر می‌تواند به کاهش استفاده از این خدمات و افزایش آسیب‌پذیری‌ها منجر شود. شناخت رفتارهای توده‌ای می‌تواند به طراحان مدل‌های امنیت سایبری کمک کند تا راهکارهای مناسب‌تری برای افزایش اعتماد عمومی ارائه دهند.
کمبود دانش تجارت دیجیتالی	عدم آگاهی از روش‌های ایمن استفاده از خدمات بانکداری الکترونیک می‌تواند کاربران را در معرض تهدیدات سایبری قرار دهد. آموزش و ارتقاء سطح دانش کاربران در زمینه امنیت سایبری و تجارت دیجیتال ضروری است تا از سوءاستفاده‌ها جلوگیری شود و اطمینان افراد از خدمات الکترونیکی افزایش یابد.
سنتی بودن افکار غالب جامعه	جامعه‌هایی که به‌طور سنتی به روش‌های قدیمی و غیردیجیتالی پایبند هستند، ممکن است در برابر تغییرات جدید مقاومت کنند. این سنت‌گرایی می‌تواند مانع از پذیرش فناوری‌های جدید و به‌ویژه بانکداری الکترونیک شود. در چنین شرایطی، برای موفقیت در پیاده‌سازی مدل‌های امنیت سایبری، نیاز به تغییر نگرش‌ها و فرهنگ جامعه و ارائه اطلاعات و مزایای واضح از بانکداری دیجیتال وجود دارد.
ریسک درک شده	ریسک درک شده به احساس و ادراک افراد از خطرات امنیتی مرتبط با استفاده از خدمات بانکداری الکترونیک اشاره دارد. اگر کاربران احساس کنند که استفاده از این خدمات خطرناک است، ممکن است از پذیرش آنها خودداری کنند. بنابراین، مدیریت ریسک درک شده از طریق آموزش و افزایش آگاهی، ارائه اطلاعات شفاف در مورد امنیت سامانه‌ها و بهبود دستورالعمل‌های امنیتی می‌تواند به افزایش اعتماد کاربران کمک کند.
روند کند اطمینان افراد جامعه	این مولفه به تأخیر در افزایش اعتماد افراد به سامانه‌های جدید و دیجیتالی اشاره دارد. در بسیاری از جوامع، پذیرش فناوری‌های جدید ممکن است به‌طور تدریجی صورت گیرد و این روند می‌تواند ناشی از تجربیات منفی قبلی، عدم آگاهی یا عدم فهم مناسب از این سامانه‌ها باشد. برای تسریع این روند، لازم است که بانک‌ها و ارائه‌دهندگان خدمات مالی به‌طور مداوم ارتباطات مؤثری با مشتریان برقرار کنند و از طریق تبلیغات و آموزش‌های مستمر، اعتماد را در میان افراد جامعه تقویت کنند.
قوانین محلی	قوانین محلی به مجموعه‌ای از مقررات و قوانینی اشاره دارند که به‌طور خاص در یک کشور یا منطقه جغرافیایی اعمال می‌شوند. این قوانین ممکن است شامل الزامات مربوط به حریم خصوصی، حفاظت از داده‌ها و مسئولیت‌های قانونی در برابر نقض امنیتی باشند. بانک‌ها باید اطمینان حاصل کنند که سامانه‌های امنیتی و شیوه‌های عملیاتی آن‌ها با این قوانین همخوانی دارد. تطابق با قوانین محلی نه تنها به کاهش ریسک‌های حقوقی کمک می‌کند، بلکه اعتماد مشتریان را نیز افزایش می‌دهد.
قوانین بین‌المللی	قوانین بین‌المللی شامل توافق‌نامه‌ها و استانداردهایی است که توسط سازمان‌های بین‌المللی و کشورهای مختلف به تصویب رسیده‌اند. این قوانین می‌توانند شامل مواردی مانند توافق‌نامه‌های امنیت سایبری، قوانین مربوط به مبارزه با پولشویی و حفاظت از داده‌ها باشند. بانک‌ها و مؤسسات مالی که به عملیات بین‌المللی می‌پردازند، باید از این قوانین آگاه باشند و با آن‌ها مطابقت داشته باشند تا از مشکلات حقوقی و اقتصادی جلوگیری کنند.
قوانین بانکی و بومی	این قوانین به مقررات خاصی اشاره دارند که به‌طور ویژه برای صنعت بانکداری طراحی شده‌اند و معمولاً توسط نهادهای نظارتی مالی تصویب می‌شوند. این قوانین ممکن است شامل الزامات مربوط به احراز هویت مشتریان، مدیریت ریسک، و الزامات امنیت سایبری باشد. رعایت این قوانین برای بانک‌ها حیاتی است و به ایجاد یک محیط ایمن برای انجام تراکنش‌های مالی کمک می‌کند.
سیاست‌های داخلی	سیاست‌های داخلی به خط‌مشی‌ها و رویه‌های اجرایی داخلی یک بانک یا مؤسسه مالی اشاره دارد که به مدیریت ریسک‌های امنیتی و حفاظت از اطلاعات حساس می‌پردازد. این سیاست‌ها ممکن است شامل فرآیندهای واکنش به حوادث، برنامه‌های آموزشی برای کارکنان، و راهکارهای مدیریت بحران باشند. داشتن سیاست‌های داخلی قوی می‌تواند به تسهیل تطابق با قوانین

جدول(۱): کدهای شناسایی شده براساس مصاحبه

کد باز	مصاحبه
	و مقررات خارجی و محلی کمک کند.
سیاست‌های نظارتی و دولتی	این سیاست‌ها شامل چارچوب‌های قانونی و نظارتی هستند که توسط دولت‌ها و نهادهای نظارتی برای حفاظت از سامانه‌های مالی و بانکداری ایجاد می‌شوند. این سیاست‌ها می‌توانند شامل الزامات مربوط به نظارت بر فعالیت‌های بانکی، بررسی‌های امنیتی، و الزامات گزارش‌دهی باشند. اجرای مؤثر این سیاست‌ها به افزایش امنیت در بانکداری الکترونیک و حفظ اعتماد عمومی به سامانه‌های مالی کمک می‌کند.
سطح آگاهی	سطح آگاهی به میزان اطلاعات و دانش کاربران و کارکنان در مورد تهدیدات امنیتی و شیوه‌های حفظ امنیت اطلاعات اشاره دارد. افزایش سطح آگاهی به کاربران کمک می‌کند تا خطرات احتمالی را شناسایی کرده و از رفتارهای ناامن پرهیز کنند. برنامه‌های آموزشی و اطلاع‌رسانی منظم می‌توانند به افزایش آگاهی درباره بهترین شیوه‌های امنیت سایبری و شیوه‌های مقابله با تهدیدات کمک کنند.
فرهنگ امنیتی	فرهنگ امنیتی به نگرش‌ها، باورها و رفتارهای مشترک در یک سازمان یا جامعه در زمینه امنیت سایبری اشاره دارد. یک فرهنگ امنیتی قوی می‌تواند به ایجاد محیطی امن و پشتیبانی از شیوه‌های صحیح امنیت اطلاعات کمک کند. این فرهنگ شامل تعهد به رعایت سیاست‌های امنیتی، اشتراک‌گذاری اطلاعات درباره تهدیدات و تشویق به بهبود مستمر در فرآیندهای امنیتی است.
وضعیت آموزش ایمنی	وضعیت آموزش ایمنی به کیفیت و سطح آموزش‌هایی اشاره دارد که به کارکنان و کاربران در زمینه امنیت سایبری ارائه می‌شود. آموزش‌های موثر باید به‌طور منظم برگزار شوند و شامل محتوای به‌روز و متناسب با تهدیدات جدید باشد. این آموزش‌ها می‌تواند به شناسایی رفتارهای مشکوک، مقابله با حملات سایبری و رعایت بهترین شیوه‌های امنیتی کمک کند.
کیفیت زیرساخت	کیفیت زیرساخت به شرایط و قابلیت‌های فناوری اطلاعات و سامانه‌های امنیتی موجود در بانک‌ها و مؤسسات مالی اشاره دارد. زیرساخت‌های با کیفیت بالا باید قادر به حفاظت از داده‌ها و اطلاعات حساس در برابر حملات سایبری باشند. این شامل شبکه‌های امن، سرورهای قوی، سامانه‌های رمزنگاری و فناوری‌های پیشرفته برای شناسایی و پاسخ به تهدیدات است. کیفیت زیرساخت به‌طور مستقیم بر قابلیت‌های امنیتی سازمان تأثیر می‌گذارد.
به‌روزرسانی فناوری	به‌روزرسانی فناوری به معنای به‌روز نگه‌داشتن سامانه‌ها، نرم‌افزارها و دستورالعمل‌های امنیتی برای مقابله با تهدیدات جدید است. فناوری‌های امنیتی باید به‌طور مداوم بررسی و به‌روزرسانی شوند تا از پیشرفت‌های اخیر در زمینه امنیت سایبری بهره‌برداری شود. به‌روزرسانی منظم نرم‌افزارها، نصب وصله‌های امنیتی و ارتقاء سخت‌افزارها از جمله اقداماتی هستند که می‌توانند به افزایش امنیت و کاهش آسیب‌پذیری‌ها کمک کنند.

کدگذاری محوری مرحله دوم تجزیه و تحلیل داده‌ها در نظریه‌پردازی زمینه‌ای در این پژوهش است. هدف این مرحله برقراری رابطه بین مقوله‌های تولید شده در مرحله کدگذاری باز است. این کدگذاری، به این دلیل محوری نامیده شده که کدگذاری حول محور یک مقوله تحقیق است. این مقوله به عنوان مقوله‌محوری انتخاب شده و در مرکز مدل قرار گرفته است؛ زیرا می‌توان ردپا و اثر آن را در اغلب داده‌ها و نقل و قول‌های مصاحبه‌شوندگان، به وضوح مشاهده کرد. بنابراین می‌توان این مقوله را در مرکز مدل قرار داد و سایر مقوله‌ها را با آن مرتبط ساخت. اجزای الگوی پارادایمی برای کدگذاری محوری عبارت‌اند: از مقوله محوری، شرایط علی، شرایط زمینه‌ای، شرایط مداخله‌گر، راهبردها و پیامدها.

مرحله اصلی تحلیل داده بنیاد، کدگذاری انتخابی است که پژوهشگر براساس 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.

شرایط علی: عبارتست از حوادث یا رویدادهایی که به وقوع یا گسترش پدیده‌ای می انجامد. در پژوهش حاضر براساس دیدگاه مشارکت‌کنندگان مقوله‌های فناوری‌های جدید و پیشرفته، وضعیت داده‌ها، تهدیدات سایبری رفتار کاربر و عوامل نگرشی شناسایی شده و آن را به مقوله وسیع‌تر دیگری به نام شرایط علی ارتباط داده شده است. در جدول (۲) به مصاحبه‌هایی که به صورت غیرمستقیم کد محوری را مشخص کردند اشاره شده است:

جدول(۲): شرایط علی

کدگذاری انتخابی	کدگذاری محوری	کدگذاری باز
شرایط علی	فناوری‌های جدید و پیشرفته	بلاک‌چین
		یادگیری ماشین
		اینترنت اشیاء
		محاسبات ابری
		هوش مصنوعی
	وضعیت داده‌ها	حجم بالای داده‌ها
		پیچیدگی داده‌ها
		مدیریت داده‌ها
		به‌روزرسانی داده‌ها
	تهدیدات سایبری	حملات سایبری
		حملات رباتیک
		حملات DDoS
	رفتار کاربر	شناسایی رفتارهای کاربر
		تحلیل پشرفته الگوهای دسترسی کاربر
		شناسایی رفتارهای مشکوک
		به‌روزرسانی مشخصات بیومتریک کاربر
		تطبیق هویتی در دسترسی‌های غیرمجاز
	عوامل نگرشی	درک امنیت اطلاعات
		بی‌ثباتی فرهنگ تجارت دیجیتال
		رفتارهای توده‌ای
		کمبود دانش تجارت دیجیتالی
		سنتی بودن افکار غالب جامعه
		ریسک درک شده
		روند کند اطمینان افراد جامعه

شرایط زمینه‌ای: بستر یا زمینه، مجموعه مشخصه‌های ویژه‌ای است که به پدیده مورد نظر دلالت می‌کند؛ یعنی محل حوادث و وقایع متعلق به پدیده. بستر نشانگر مجموعه شرایط خاصی است که در آن راهبردهای کنش و واکنش صورت می‌پذیرد. قوانین و مقررات، فرهنگ سازمانی، زیرساخت‌های فناورانه، صنعت بانکداری و اقتصاد دیجیتال به عنوان شرایط زمینه‌ای مشخص شدند. در جدول (۳) به مصاحبه‌هایی که به صورت غیرمستقیم

کد محوری را مشخص کردند اشاره شده است:

جدول(۳): شرایط زمینه‌ای

کدگذاری انتخابی	کدگذاری محوری	کدگذاری باز
شرایط زمینه‌ای	قوانین و مقررات	قوانین محلی
		قوانین بین‌المللی
		قوانین بانکی و بومی
		سیاست‌های داخلی
		سیاست‌های نظارتی و دولتی
	فرهنگ سازمانی	سطح آگاهی
		فرهنگ امنیتی
		وضعیت آموزش ایمنی
	زیرساخت‌های فناورانه	کیفیت زیرساخت
		به‌روزرسانی فناوری
		بومی‌سازی فناوری
		استاندارسازی فناوری
		تطبیق فناوری
		تعمیر و نگهداری فناوری
	صنعت بانکداری	قوانین مالی
		محیط داخلی بانک
		شرایط صنعت بانکداری
		قوانین بین‌المللی مالی
		شخصی سازی
		ساختار بانک
		روابط بین‌بانکی
		سطح‌بندی بانک
		انعطاف‌پذیری صنعت بانکداری
		تمرکز صنعت بانکداری
		جایگاه بانک در جامعه
		به‌روزرسانی صنعت
		سلسله مراتبی صنعت
		وضعیت خصوصی و دولتی بودن
		شهرت بانک
		وضعیت بانک در بورس اوراق بهادار
	اقتصاد دیجیتال	معماری باز پیشران
		سیاست‌های داده‌ای باز
		سواد دیجیتالی
		سیاست‌گذاری براساس داده‌های تجربی و آزمایشی
		امنیت سایبری
		هویت دیجیتال قابل اعتماد
		مرکز داده‌ای دیجیتالی قابل اعتماد
		زیرساخت‌های عمومی برای اقتصاد دیجیتال

شرایط مداخله‌گر: شرایط ساختاری که به پدیده‌ای تعلق دارند و بر راهبردهای کنش و واکنش اثر می‌گذارند. آنها راهبردها را در درون زمینه خاصی سهولت می بخشند یا آنها را محدود و مقید می‌کنند. مولفه‌های: سامانه‌ی حفاظتی و امنیتی، رویه امنیت پیشرفته، دستورالعمل‌ها و استانداردهای امنیتی و وضعیت مدیریت ریسک و پاسخ به بحران به عنوان شرایط مداخله‌گر شناسایی شدند. در جدول (۴) به مصاحبه‌هایی که به صورت غیرمستقیم کد محوری را مشخص کردند اشاره شده است:

جدول(۴): شرایط مداخله‌گر

کدگذاری انتخابی	کدگذاری محوری	کدگذاری باز
شرایط مداخله‌گر	سامانه‌ی حفاظتی و امنیتی	فایروال
		سامانه‌های تشخیص نفوذ
		سامانه‌های مدیریت رخداد
	رویه امنیت پیشرفته	سکوهای مدیریت تهدیدات پیشرفته
		بهینه‌سازی و خودکارسازی فرآیندهای امنیتی
		احراز هویت و رمزنگاری در دستگاه‌های اینترنت اشیاء
		مدیریت دستگاه‌های IOT
	دستورالعمل‌ها و استانداردهای امنیتی	پیروی از استانداردها و دستورالعمل‌های امنیتی
		دستورالعمل‌های ارتباطی و رمزنگاری
		استانداردهای احراز هویت و دسترسی
		استانداردهای امنیتی برای برنامه‌ها و سامانه‌ها
		مدیریت امنیت و پاسخ به تهدیدات
	وضعیت مدیریت ریسک و پاسخ به بحران	روش‌ها و فرآیندهای مدیریت ریسک
		آمادگی مدیریت ریسک
		پاسخ به بحران برای مقابله با حملات سایبری و آسیب‌های امنیتی.

راهبردها: مبتنی بر کنش‌ها و واکنش‌هایی برای کنترل، اداره و بازخورد پدیده مورد بررسی هستند. راهبردها هدفمند هستند به دلیلی صورت می‌گیرند. همواره شرایط مداخله‌گری نیز حضور دارند که راهبردها را سهولت می‌بخشند و یا آن را محدود می‌کنند. راهبردهای شناسایی شده عبارتند از : حفاظت از داده‌ها، آموزش و آگاهی، مدیریت آسیب‌پذیری، نظارت و گزارش‌دهی، سازوکار داده‌پردازی، پشتیبان‌گیری و بازیابی و به کارگیری فناوری‌های مدرن. در جدول (۵) به مصاحبه‌هایی که به صورت غیرمستقیم کد محوری را مشخص کردند اشاره شده است:

جدول(۵): راهبردها

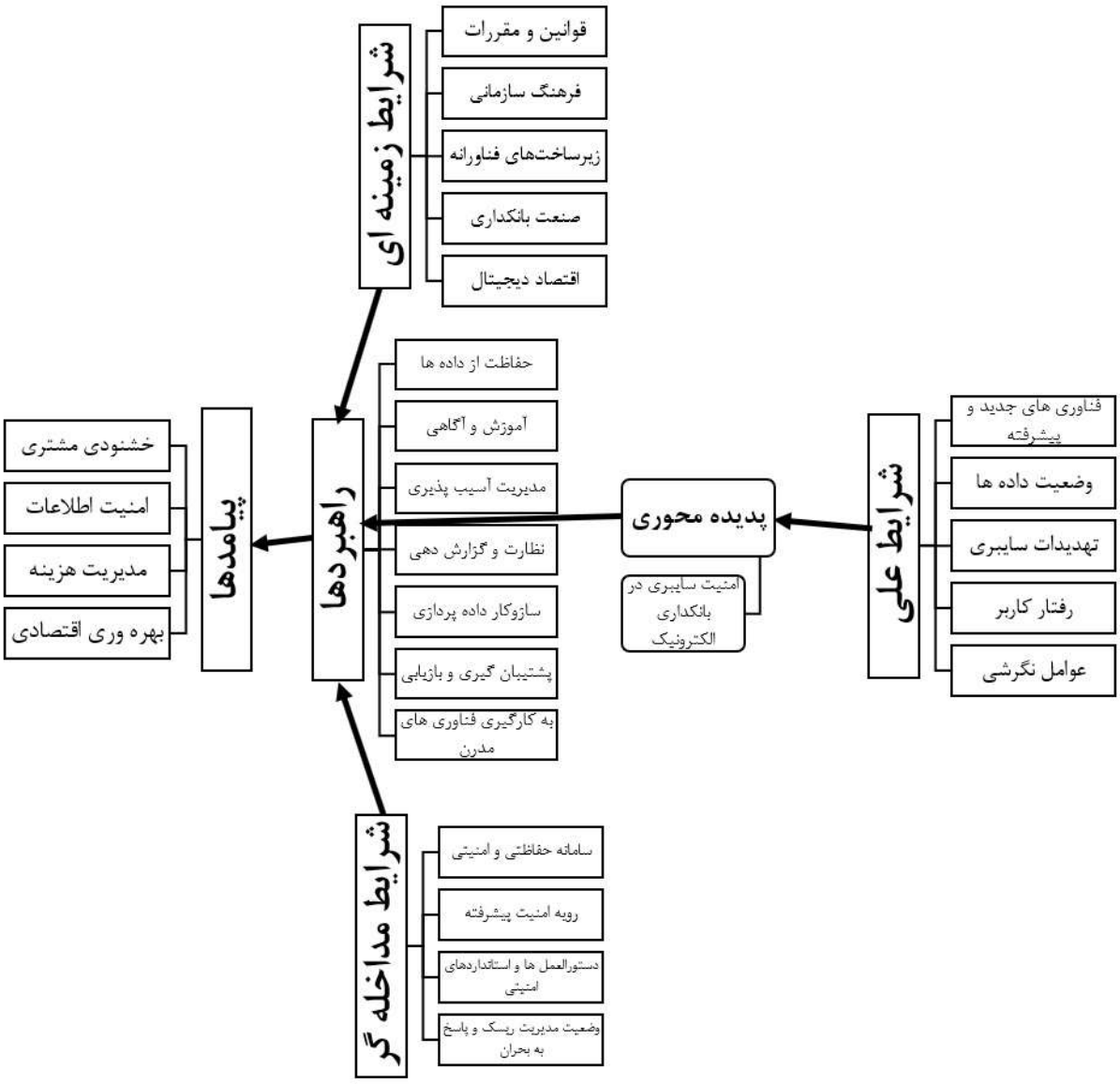
کدگذاری انتخابی	کدگذاری محوری	کدگذاری باز
راهبردها	حفاظت از داده‌ها	حریم خصوصی
		یکپارچگی داده‌ها
		احراز هویت
		کنترل دسترسی
		رمزنگاری
		تائید تراکنش
	آموزش و آگاهی	آموزش کارکنان در زمینه امنیت اطلاعات
		آموزش روش‌های پیشگیری تهدیدات
		اطلاع رسانی به کاربران
		آموزش روش‌های حفاظت از اطلاعات شخصی
	مدیریت آسیب‌پذیری	اسکن و بررسی آسیب‌پذیری
		پیش‌گیری آسیب‌های احتمالی
		رفع آسیب‌ها
		به‌روزسانی و پچ‌گذاری
	نظارت و گزارش‌دهی	نظارت مداوم بر ترافیک شبکه
		ردگیری فعالیت‌های مشکوک
		گزارشدهی و تحلیل
	سازوکار داده‌پردازی	شناسایی الگوهای مشکوک
		استفاده از داده کاوی
		الگوریتم‌سازی امنیتی
		تحلیل داده‌های بزرگ
	پشتیبان‌گیری و بازیابی	ایجاد نسخه‌های پشتیبان منظم
		بازیابی از خرابی
		تیم متخصص پشتیبان‌گیری
		اشتراک‌گذاری منظم داده
	به‌کارگیری فناوری‌های مدرن	احراز هویت بیومتریک
		تشخیص صدای کاربر
		رمزنگاری همگام
		رمزنگاری هومورفیک
		تراکنش‌های شفاف بلاک‌چین
		قراردادهای هوشمند بلاک‌چین
		رمزنگاری داده‌ها براساس ابر
		کنترل دسترسی براساس نقش

پیامدها: نتایجی که در اثر راهبردها پدیدار می‌شود. پیامدها نتایج و حاصل کنش‌ها و واکنش‌ها هستند. پیامدها را همواره نمی‌توان پیش‌بینی کرد و الزاما همان‌هایی نیستند که افراد قصد آن را داشته‌اند. پیامدها ممکن است حوادث و اتفاقات باشند، شکل منفی به خود بگیرند، واقعی یا ضمنی باشند و در حال یا آینده به وقوع بپیوندند. هم چنین این امکان وجود دارد که آن چه که در برهه‌ای از زمان پیامد به شمار می‌رود در زمانی دیگر به بخشی از شرایط و عوامل تبدیل شوند. پیامدهای شناسایی شده عبارتند از خشنودی مشتری، امنیت اطلاعات، مدیریت هزینه و بهره‌وری اقتصادی. در جدول (۶) به مصاحبه‌هایی که به صورت غیرمستقیم کد محوری را مشخص کردند اشاره شده است:

جدول(۶): پیامدها

کدگذاری انتخابی	کدگذاری محوری	کدگذاری باز
پیامدها	خشنودی مشتری	رضایت مشتری
		بهبود نگرش مشتری
		افزایش وفاداری مشتری
		افزایش تعداد مشتری
		فرهنگ سازی مشتری
		تجربه مثبت مشتری
		افزایش اعتماد مشتری
	امنیت اطلاعات	کاهش سرقت اطلاعات
		کاهش فاش شدن اطلاعات محرمانه
		کاهش سرقت پول
	مدیریت هزینه	کاهش بازپرداخت به مشتری
		کاهش جبران خسارات
		کاهش جریمه‌های مقرراتی
		کاهش هزینه‌های دستورالعمل‌های امنیتی
	بهره‌وری اقتصادی	افزایش سرمایه‌گذاری
		افزایش فعالیت‌های اقتصادی
		افزایش سودآوری

ارائه الگوی پارادایمی: درکدگذاری‌باز، مقوله‌ها و مضامین اصلی پیرامون پدیده مورد مطالعه شناسایی شدند. در کدگذاری محوری، مقوله‌ها به‌طور نظام‌مند بهبودیافته و با زیرمقوله‌ها پیوند داده شدند. در نهایت از طریق، کدگذاری گزینشی، الگوی پارادایمی پژوهش ارائه شد. 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 عبارت‌اند: از مقوله محوری، شرایط علی، شرایط زمینه‌ای، شرایط مداخله‌گر، راهبردها و پیامدها. ارتباط سایر مقوله‌ها با مقوله اصلی(مرکزی) طبق الگوی پارادایم به صورت شکل (۱) می‌باشد.



شکل(۱): مدل پارادایمی پژوهش (مدل امنیت سایبری در بانکداری الکترونیک)

۶- نتیجه‌گیری و پیشنهادها

این پژوهش با هدف ارائه مدل امنیت سایبری در بانکداری الکترونیک انجام شد. پژوهش‌ها نشان داده‌اند 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. حال آنکه علی‌رغم پژوهش‌های فراوان در خصوص در بانکداری الکترونیک، هنوز فقدان بررسی تأثیر برخی از پدیده‌های جدید سازمانی بر این رویکرد مشهود است. همچنین پدیده امنیت سایبری و نقش آن در توسعه این رویکرد نیز از جمله عواملی است که کمتر مورد توجه قرار گرفته است و اکثر محققان در این زمینه تحقیق و تفحص نموده‌اند. لذا با توجه به اهمیت موضوع پژوهش، محقق کوشیده است تا مدل امنیت سایبری در بانکداری الکترونیک را مورد واکاوی قرار دهد. در این مطالعه، ابتدا مصاحبه‌ها بازنویسی و مورد تحلیل قرار گرفت و سپس در مصاحبه‌های بعدی تلاش شد برای اشباع نظری و درک بهتر موضوع، با استفاده از کدگذاری محوری مقوله‌های فرعی و روابط بین آنها شناسایی شود. در نهایت، با استفاده از کدگذاری انتخابی و با انسجام درونی و تعیین سطوح ابعادی مقوله‌ها، روابط میان مفاهیم اعتباربخشی شد.

این پژوهش با وجود اهمیت و نوآوری‌های خود با محدودیت‌هایی نیز مواجه بوده است. **از محدودیت‌های این مطالعه عبارتند از:**

تغییرات سریع در فناوری: با توجه به اینکه فناوری‌های امنیت سایبری به‌سرعت در حال تغییر و تحول هستند، نتایج این پژوهش

ممکن است در آینده به‌سرعت تغییر کنند و نیاز به به‌روزرسانی مداوم داشته باشند.

محدودیت‌های زمانی: پژوهش‌ها اغلب در بازه‌های زمانی کوتاه انجام می‌شوند، که ممکن است باعث شود برخی از متغیرهای طولانی‌مدت یا روندهای زمان‌بر از قلم بیفتند و نتایج نهایی در مقایسه با شرایط واقعی ممکن است دقیق نباشد.

تنوع فرهنگی و اجتماعی: تفاوت‌های فرهنگی و اجتماعی بین کاربران می‌تواند بر درک و رفتار آنها نسبت به امنیت سایبری تأثیر بگذارد. این موضوع می‌تواند به تنوع در نتایج پژوهش منجر شود و نیاز به تحقیقات بیشتری در این زمینه احساس شود.

عدم دسترسی به برخی از داده‌ها: در برخی موارد، عدم دسترسی به داده‌های دقیق و معتبر از سوی بانک‌ها و مؤسسات مالی می‌تواند بر کیفیت و دقت نتایج پژوهش تأثیر بگذارد.

براساس یافته‌های این پژوهش، پیشنهاد می‌شود که:

توسعه و پیاده‌سازی فناوری‌های نوین: پیشنهاد می‌شود بانک‌ها، سرمایه‌گذاری بیشتری در فناوری‌های جدید داشته باشند. این فناوری‌ها می‌توانند به شناسایی و مدیریت تهدیدات سایبری کمک کنند و امنیت اطلاعات را افزایش دهند.

آموزش و آگاهی کارکنان: پیشنهاد می‌شود که بانک‌ها برنامه‌های آموزشی منظم و دوره‌های کارگاه‌های عملی برای کارکنان خود برگزار کنند تا آنها را با تهدیدات سایبری و روش‌های مقابله با آنها آشنا کنند.

تقویت زیرساخت‌های امنیتی: بانک‌ها باید به‌روزرسانی و استانداردسازی زیرساخت‌های خود را در اولویت قرار دهند. این شامل ارتقاء سامانه‌های فایروال، سامانه‌های تشخیص نفوذ و سایر ابزارهای امنیتی است.

ارزیابی اثرات بلندمدت: پیشنهاد می‌شود پژوهش‌های آینده به ارزیابی اثرات بلندمدت فناوری‌ها و سیاست‌ها پرداخته و به‌ویژه تاثیرات آنها بر نهادهای اجتماعی و اقتصادی در آینده مورد توجه قرار گیرد.

مدیریت ریسک و پاسخ به بحران: بانک‌ها باید روش‌ها و فرآیندهای مؤثری برای مدیریت ریسک و آمادگی برای پاسخ به بحران‌ها داشته باشند. این شامل ایجاد برنامه‌های پاسخ به بحران برای مقابله با حملات سایبری و آسیب‌های امنیتی است.

۷- مراجع

[1] M. Askari and N. Modiri, "Cybersecurity Self-Assessment Architecture", Fourth National Conference on Applied Research in Electrical and Computer Sciences and Medical Engineering, 2019.[In Persian] https://civilica.com/doc/1016778

[2] T. Lim and P. Thang, "Outsourcing life cycle model for financial services in the fintech era" , 2021. https://ink.library.smu.edu.sg/sis_research/6116/

[3] H. AlDuhaidahawi, J. Abdulreza, M. Sebai, and S. Harjan, "An efficient model for financial risks assessment based on artificial neural networks", Journal of Southwest Jiaotong University, 55(3) , 2020. https://doi.org/10.35741/issn.0258-2724.55.3.8

[4] W. A. Douglas, J. Barberis and R. P. Buckley, "FinTech, RegTech, and the Reconceptualization of Financial Regulation", 37 Nw. J. Int'l L. & Bus. 371, 2017. https://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2

[5] J. Shakeel, A. Mardani, A. Gholamzadeh and F. A. Goni, "Anatomy of sustainable business model innovation", Journal of Cleaner Production, 2020. https://doi.org/10.1016/j.jclepro.2020.121201

[6] F. Najafi, M. Irandoost, H. Soltanpanah and A. Sheikh Ahmadi, "Identifying and ranking factors affecting the interaction of banks and financial technologies with a hybrid approach", Quarterly Journal of Innovation Management, Volume 9, Issue 3, pp. 171-196, 2019. [In Persian] https://civilica.com/doc/1895359

[7] E. Jahangashte,F. Damani and S. Raisi, "Investigating the importance of cyberspace security", 8th National Conference on Computer Science, Engineering and Information Technology, 2019. [In Persian] https://civilica.com/doc/984818

[8] B. Vejdani, "Studying the impact of privacy and security of electronic banking services on bank customer loyalty with emphasis on reliability", First International Conference on Management, Industrial Engineering, Accounting and Economics in Humanities, 2024. [In Persian] https://civilica.com/doc/2025680

[9] S. A. Mousavi, "Investigating the impact of objective dimensions of security of electronic payment systems through customer perception of security and trust (Case study: branches of Bank Melli Kohgiluyeh and Boyer Ahmad Province)", Payashahr Monthly, Volume: 6, Issue: 60 , 2024. [In Persian] https://civilica.com/doc/1976050

[10] A. Aparnak,A. Gazeri Neishabouri and B. Seraj, "The relationship between perceived security and customer trust in the electronic banking system based on the NFC-Mobile approach", 5th International Conference on Interdisciplinary Studies in Management and Engineering, 674-691, 2012. [In Persian] https://civilica.com/doc/1507286

[11] A. T. Oyewole, C. C. Okoye, O. C. Ofodile and C. E. Ugochukwu, "Cybersecurity risks in online banking: A detailed review and preventive strategies application", World Journal of Advanced Research and Reviews 21(3):625-643, 2024. https://doi.org/10.30574/wjarr.2024.21.3.0707

[12] M. J. Mohona, "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, Page No. 214-219, 2024.

[13] J. M. Alghazo, Z. Kazmi and GH. Latif, "Cyber Security Analysis of Internet Banking in Emerging Countries: User and Bank perspectives", 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS) , 2017. DOI:10.1109/ICETAS.2017.8277910

[14] Y. Kim, Y. J. Park, J. Choi and J. Yeon, "An empirical study on the adoption of "Fintech" service: Focused on mobile payment services", Advanced Science and Technology Letters, 114(26), 136-140, 2015. http://dx.doi.org/10.14257/astl.2015.114.26

[15] A. Alizadeh, K. Fathi, A. Shah Mansouri and A. Arab Sorkh, "Presenting a conceptual model for classifying types of threats in the security and cyber defense of knowledge-based organizations in the country". Passive Defense, 15(2), 75-100, 2024. [In Persian] https://dor.isc.ac/dor/20.1001.1.20086849.1403.15.2.6.5

[16] H. Hakim and R. Esfahani, "Defensive strategies to combat psychological deception in the field of information security". Passive Defense, 15(1), 13-27, 2024. [In Persian] https://dor.isc.ac/dor/20.1001.1.20086849.1403.15.1.2.9

[17] M. Akhtari, M. A. Keramati, and S. A. Mousavi, "Comparative comparison of cybersecurity and information security maturity models and the calculation of common cybersecurity indicators", Passive Defense, 13(4), 21-38, 2022. [In Persian] https://dor.isc.ac/dor/20.1001.1.20086849.1401.13.4.3.2

[18] M. Rastgoo and M. Jalali, "Detecting cybercrimes in online communications with a data mining approach", Passive Defense, 11(1), 63-70, 2019. [In Persian] https://dor.isc.ac/dor/20.1001.1.20086849.1401.13.4.3.2