University of Tehran
Central Library
and Documentation Center

Academic Librarianship and Information Research

Online ISSN: 2783 - 4638

Homepage: https://jlib.ut.ac.ir/

Designing a Comprehensive Model for Data Security Management in the Country's Banking Network

Hamid Ghafari[1], and **Mohammad Khandan**[2]✉

1. Department of Knowledge and Information Science, Faculty of Management, University of Tehran, Kish International Campus, Kish International Campus Tehran, Iran. E-mail: ghafari.hamid@ut.ac.ir
2. Corresponding author, Department of Knowledge and Information Science, Faculty of Management, University of Tehran, Tehran, Iran. E-mail: khandan@ut.ac.ir

Article Info

Article type:
Research Article

Article history:
Received 22 March 2025
Received in revised form 23 May 2025
Accepted 22 June 2025
Available online 30 June 2025

Keywords:
targeted management,
data security,
banking,
network,
banking.

ABSTRACT

Objective: In today's digital landscape, data is widely regarded as an organization's most valuable asset and a critical strategic resource, necessitating robust measures to ensure its security. Accordingly, this study aims to develop a comprehensive data security management model tailored to the national banking network.

Method: This study adopts an exploratory sequential mixed-methods design, integrating both library-based (documentary) and field-based data collection approaches. The library-based component draws on scholarly books, peer-reviewed articles, and academic journals to construct the theoretical framework. The field component employs semi-structured interviews and structured questionnaires. The study population comprises two distinct groups: (1) banking network managers and subject-matter experts, who participate in the interviews, and (2) bank managers, deputy managers, and staff, who complete the questionnaires. Qualitative data were analyzed using MAXQDA software, and quantitative data were analyzed using SmartPLS to develop and validate a comprehensive data security management model for the national banking network.

Results: The analysis identified eight key components that significantly influence data security management in the national banking network ($p < 0.05$): (1) primary causes of security incidents in banks, (2) barriers and concerns related to implementing enhanced security compliance, (3) security strategies employed over the past six months, (4) existing data security measures, (5) the data security lifecycle, (6) additional security measures required to strengthen data protection, (7) data security mechanisms in online banking services, and (8) financial services impacted by data security mechanisms.

Conclusions:

Security strategies should prioritize employee training, compliance with emerging regulatory requirements, and the enhancement of inter-bank coordination to foster sustainability and reinforce trust within the banking network. Collectively, these elements contribute to a more robust data security management framework, elevating the maturity and coherence of data protection practices across the national banking system.

Cite this article: Ghafari, H., & Khandan, M. (2025). Designing a comprehensive model for data security management in the country's banking network. *Academic Librarianship and Information Research*, 59 (2), 1-28. https://doi.org/10.22059/jlib.2025.397490.1783

Publisher: University of Tehran.
DOI: https://doi.org/ 10.22059/jlib.2025.397490.1783

Introduction

In today's digital landscape, data is widely regarded as an organization's most valuable asset and a critical strategic resource, necessitating robust measures to ensure its security. Accordingly, this study aims to develop a comprehensive data security management model tailored to the national banking network.

The financial sector plays a leading role in the modern economy, serving as a financial intermediary among diverse market participants and establishing the essential preconditions for social reproduction. A sound and efficient financial sector encourages productive investment, thereby fostering innovation and economic growth (Rezvani, 2018). Bank credit is also instrumental in financing household needs, particularly in balancing consumption patterns and enabling greater investment toward self-reliance, sustainability, and future development. A high level of financial security within the banking system not only determines the operational efficiency and macroeconomic stability of a society but also fundamentally shapes the state's fiscal capacity and national security (Sharma et al., 2021).

Data security management constitutes an integral component of an organization's overarching governance framework, grounded in a business risk–oriented approach. Its objective is to establish, implement, operate, monitor, review, maintain, and continually improve data security. When properly implemented, such a management system can significantly contribute, by mitigating external and internal risks, to ensuring a defined level of security assurance (Khrushch et al., 2020). This becomes especially critical in the context of the banking system, given the heightened sensitivity surrounding business security and financial transactions, which amplifies the necessity of robust data security management.

Maintaining trust between banks and their customers is imperative, and timely, accurate information is essential for sound investment and decision-making. Any unauthorized disclosure, deletion, or manipulation of data, or its unavailability when needed, can severely impact a bank's revenues and capital, leading to potentially irreversible consequences (Doroudi & Jamshidi, 2021). Moreover, the implementation of a data security management system in banks differs from that in other organizations due to the nature of their assets (primarily financial information), the architecture of their information exchange infrastructure, the specific business processes employed, and the structural characteristics of their data. Within this context, the banking community continues to seek effective strategies for developing comprehensive data security programs (Diesch et al., 2020). Consequently, banks must select data security frameworks aligned with their organizational scale, technological complexity, and usage patterns, and then manage these frameworks through tailored, institution-specific models. Concurrently, with the exponential growth in processing power and rapid technological advancements, all businesses, including private and public sector organizations, face escalating threats to their complex information systems. These threats primarily stem from cybercrime, human error, and various vulnerabilities embedded in business processes, technologies, and human interactions, with their nature and severity varying across organizations. The intricate interdependencies among these components have

further exacerbated vulnerabilities within modern information systems, particularly in enterprise resource planning (ERP) software, since the adoption of such integrated platforms has significantly blurred traditional organizational boundaries compared to legacy systems. Substantial efforts are underway to counter this spectrum of threats, primarily through the application of diverse data management frameworks, standards, and techniques aimed at reducing vulnerabilities to acceptable levels (Li et al., 2021).

Network data security remains a growing challenge, as these networks are inherently vulnerable to external threats specifically designed to disrupt services (Kimiagari & Baei, 2021). Networked environments continue to face numerous security threats, including insider attacks, routing attacks, denial-of-service (DoS), and distributed denial-of-service (DDoS) attacks. These pose significant security challenges that demand innovative solutions and heightened vigilance. Recent studies indicate that the proliferation of emerging technologies, such as the Internet of Things (IoT), cloud computing, and 5G networks, has increased both the complexity and diversity of cyberattacks. Advanced threats, including AI-driven attacks and autonomous malware, have introduced novel risks to data management systems. Such attacks can inflict severe damage on applications and services within smart environments, particularly in critical infrastructures such as smart power grids or intelligent transportation systems (Ahmadi, 2023).

To counter these evolving threats, novel approaches have been proposed, including the use of blockchain technology to ensure data integrity, advanced cryptographic methods, and artificial intelligence for real-time threat detection and prevention. Furthermore, up-to-date security standards, such as the NIST Cybersecurity Framework and ISO/IEC 27001, enable organizations to implement more resilient security architectures (Kazemi, 2024). Ultimately, securing data management within networked environments has emerged as a pressing concern for organizations, particularly banks, and for information security professionals alike.

Method

This study adopts an exploratory sequential mixed-methods design, integrating both library-based (documentary) and field-based data collection approaches. The library-based component draws on scholarly books, peer-reviewed articles, and academic journals to construct the theoretical framework. The field component employs semi-structured interviews and structured questionnaires. The study population comprises two distinct groups: (1) banking network managers and subject-matter experts, who participate in the interviews, and (2) bank managers, deputy managers, and staff, who complete the questionnaires. Qualitative data were analyzed using MAXQDA software, and quantitative data were analyzed using SmartPLS to develop and validate a comprehensive data security management model for the national banking network.

Results

The analysis identified eight key components that significantly influence data security management in the national banking network ($p < 0.05$): (1) primary causes of security

incidents in banks, (2) barriers and concerns related to implementing enhanced security compliance, (3) security strategies employed over the past six months, (4) existing data security measures, (5) the data security lifecycle, (6) additional security measures required to strengthen data protection, (7) data security mechanisms in online banking services, and (8) financial services impacted by data security mechanisms.

Conclusions

Security strategies should prioritize employee training, compliance with emerging regulatory requirements, and the enhancement of inter-bank coordination to foster sustainability and reinforce trust within the banking network. Collectively, these elements contribute to a more robust data security management framework, elevating the maturity and coherence of data protection practices across the national banking system.

Author Contributions

All authors contributed equally to the conceptualization of the article and writing of the original and subsequent drafts.

Data Availability Statement

Data available on request from the authors.

Acknowledgements

The authors would like to thank all participants in the present study.

Ethical Considerations

The authors avoided data fabrication, falsification, plagiarism, and misconduct.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The authors declare no conflict of interest.

تحقیقات کتابداری و اطلاع رسانی دانشگاهی
شاپا الکترونیکی: ۴۶۳۸-۲۷۸۳
Homepage: https://jlib.ut.ac.ir/

طراحی مدل جامع مدیریت امنیت داده در شبکه بانکی کشور

حمید غفاری[۱]، و محمد خندان[۲]✉

۱. گروه علم اطلاعات و مدیریت دانش، دانشکده مدیریت دولتی و علوم سازمانی، دانشگاه تهران، پردیس بین‌المللی کیش، تهران، ایران. رایانامه: ghafari.hamid@ut.ac,ir

۲. نویسنده مسئول، گروه علم اطلاعات و مدیریت دانش، دانشکده مدیریت دولتی و علوم سازمانی، دانشگاه تهران، تهران، ایران. رایانامه: khandan@ut.ac.ir

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی

تاریخ دریافت: ۱۴۰۴/۰۱/۰۲
تاریخ بازنگری: ۱۴۰۴/۰۳/۰۲
تاریخ پذیرش: ۱۴۰۴/۰۴/۰۱
تاریخ انتشار: ۱۴۰۴/۰۴/۰۹

کلیدواژه‌ها:
مدیریت هدفمند،
امنیت داده،
شبکه بانکی،
بانکداری.

چکیده

هدف: داده‌ها در دنیای کنونی ارزشمندترین دارایی هر سازمان محسوب می‌شود، باید آن را کالای اساسی هر سازمان دانست و جهت افزایش امنیت آن کوشش نمود. براین‌اساس هدف از پژوهش حاضر طراحی مدل جامع مدیریت امنیت داده در شبکه بانکی کشور است.

روش پژوهش: روش پژوهش حاضر آمیخته اکتشافی است و برای گردآوری اطلاعات از دو روش کتابخانه‌ای و میدانی استفاده خواهد شد. جامعه آماری پژوهش حاضر شامل گروه کیفی (مصاحبه از مدیران و خبرگان در حوزه شبکه بانکی کشور) و گروه کمی (پرسش‌نامه از مدیران، معاونان و کارکنان بانک‌های کشور) جهت جمع‌آوری اطلاعات استفاده شد. جهت تجزیه‌وتحلیل داده‌ها از نرم‌افزارهای MAXQDA و SmartPLS استفاده شد.

یافته‌ها: یافته‌های به دست آمده نشان داد که هشت مؤلفه (علل عمده حوادث امنیتی در بانک، موانع و نگرانی‌ها در اجرای انطباق امنیتی بهتر، استراتژی‌های امنیتی در شش ماه اخیر، اقدامات امنیت داده‌ها، چرخه امنیت داده‌ها، اقدامات امنیتی اضافی لازم برای بهبود امنیت داده‌ها، مکانیسم‌های امنیت داده در خدمات بانکداری برخط، خدمات مالی تحت‌تأثیر مکانیسم‌های امنیت داده‌ها) بر مدیریت امنیت داده در شبکه بانکی کشور تأثیر معناداری دارند ($P<۰/۰۵$).

نتیجه‌گیری: استراتژی‌های امنیتی باید با تمرکز بر آموزش کارکنان، تطبیق با مقررات جدید و تقویت هماهنگی بین‌بانکی، جهت بهبود پایداری و اعتماد در شبکه بانکی باشد. در مجموع، عوامل یاد شده با ایجاد یک چارچوب امنیتی منسجم، مدیریت امنیت داده را در شبکه بانکی کشور به سطح بالاتری ارتقا می‌دهند.

استناد: غفاری، حمید، و خندان، محمد (۱۴۰۴). طراحی مدل جامع مدیریت امنیت داده در شبکه بانکی کشور. *تحقیقات کتابداری و اطلاع‌رسانی دانشگاهی*، ۵۹ (۲)، ۱-۲۸. https://doi.org/ 10.22059/jlib.2025.397490.1783

ناشر: دانشگاه تهران.

مقدمه

بخش مالی نقش پیشرو در اقتصاد مدرن دارد و واسطه‌گری مالی بین بازیگران مختلف در بازار مالی و ایجاد پیش‌شرط‌های اساسی برای بازتولید اجتماعی است. یک بخش مالی سالم و کارآمد، سرمایه‌گذاری مولد را تشویق می‌کند، بنابراین از نوآوری و رشد اقتصادی حمایت می‌کند (رضوانی، ۱۳۹۷). اعتبار بانکی همچنین برای تامین مالی نیازهای خانوارها، به ویژه برای ایجاد تعادل در ساختار مصرف و سرمایه گذاری بیشتر برای خودکفایی، پایداری و توسعه آینده استفاده می‌شود. سطح بالای امنیت مالی سیستم بانکی نه تنها کارایی عملکرد و ثبات اقتصادی جامعه را تعیین می‌کند، بلکه قدرت مالی و امنیت ملی دولت را نیز در کل تعیین می‌کند (شارما[1] و همکاران، ۲۰۲۱).

مدیریت امنیت داده، بخشی از سیستم مدیریت کلی و سراسری در هر سازمان است که بر پایه رویکرد مخاطرات کسب‌وکار قرار دارد و هدف آن پایه‌گذاری، پیاده‌سازی، بهره‌برداری، نظارت، بازبینی، نگهداری و بهبود امنیت داده است، در صورت پیاده‌سازی صحیح این نوع مدیریت می‌توان با کاهش ریسک‌های پیرامونی به عنوان عامل مهم، در تضمین سطح امنیتی تعریف شده، نقش بسزایی را ایفا کرد (خروشچ[2] و همکاران، ۲۰۲۰). درصورتی‌که سازمان مدنظر سیستم بانکی باشد، به دلیل حساسیت فراوان در امنیت کسب‌وکار و گردش مالی، اهمیت به‌کارگیری این مدیریت دوچندان می‌شود. با درنظرگرفتن این موضوع که ایجاد و حفظ اعتماد میان بانک و مشتریان آن ضرورت دارد و اطلاعات به‌موقع و معتبر برای اجرای سرمایه‌گذاری‌ها و تصمیم‌گیری‌های صحیح لازم است، چنانچه اطلاعات افشا، حذف یا دستکاری شوند یا در صورت نیاز در دسترس نباشند، درآمدها و سرمایه‌های بانک تحت‌تأثیر قرار گرفته و پیامدهای جبران‌ناپذیری را در برخواهد داشت (درودی و همکاران، ۱۴۰۰). همچنین پیاده‌سازی سیستم مدیریت امنیت داده بانک‌ها به دلیل نوع دارایی‌ها که از جنس اطلاعات مالی هستند، تفاوت در زیرساخت تبادل اطلاعات، نوع فرایندهای به کار گرفته شده و نیز ساختار داده‌ها در بانک، در مقوله امنیت متفاوت از سایر سازمان‌هاست. در این میان، جامعه بانکداران در تلاش هستند تا بدانند چگونه می‌توان برنامه‌های امنیت داده را توسعه داد (دیسچ[3] و همکاران، ۲۰۲۰). به همین دلیل، بانک‌ها باید برنامه امنیت داده در شبکه خود را بر اساس اندازه ساختار، پیچیدگی و نوع استفاده از فناوری انتخاب کنند، سپس از طریق مدل منحصربه‌فردی به مدیریت آن بپردازند.

از سویی با شروع افزایش قدرت پردازش و پیشرفت‌های تکنولوژیکی؛ همه کسب‌وکارها، سازمان‌های بخش خصوصی و دولتی با تهدیدات زیادی برای سیستم‌های اطلاعاتی پیچیده خود مواجه هستند. این تهدیدها عمدتاً ناشی از جرایم سایبری، خطاها و آسیب‌پذیری‌های مختلف در فرایندهای تجاری، فناوری و تعامل با افراد است که از سازمانی به سازمان دیگر متفاوت است. روابط پیچیده تجاری بین این مؤلفه‌های منفرد، این آسیب‌پذیری‌ها را در سیستم‌های اطلاعاتی مودم/نرم‌افزارهای برنامه‌ریزی منابع سازمانی بیشتر تشدید کرده است، زیرا مرزهای بخش سازمانی با استفاده از این نرم‌افزارهای مدرن در مقایسه با نرم‌افزارهای سنتی کاهش‌یافته است. تلاش‌های زیادی برای مبارزه مؤثر با این طیف تهدید، به‌حداقل‌رساندن این آسیب‌پذیری‌ها در حد قابل‌قبول توسط چارچوب‌ها، استانداردها و تکنیک‌های مختلف مدیریت داده انجام می‌شود (لی[4] و همکاران، ۲۰۲۱).

حفظ امنیت داده در شبکه یک مشکل روبه‌رشد است؛ زیرا این شبکه‌ها در برابر تهدیدات و حملات خارجی که برای اختلال در خدمات طراحی شده‌اند آسیب‌پذیر هستند (کیمیاگر و بائی[5]، ۲۰۲۱). امنیت داده در شبکه‌ها همچنان در معرض تهدیدات متعددی از جمله حملات شخصی، حملات مسیریابی، حملات انکار سرویس (DoS) و حملات توزیع‌شده انکار سرویس (DDoS) قرار دارد. این تهدیدات چالش‌های امنیتی قابل‌توجهی را ایجاد می‌کنند که نیازمند توجه و راه‌حل‌های نوین هستند. تحقیقات اخیر نشان می‌دهند که با گسترش فناوری‌های نوین مانند اینترنت اشیا (IoT)، رایانش ابری و شبکه‌های G۵،

---

1. Sharma
2. Khrushch
3. Diesch
4. Li
5. Kimiagari, S., & Baei

پیچیدگی و تنوع حملات سایبری افزایش‌یافته است. حملات پیشرفته‌تر مانند حملات مبتنی بر هوش مصنوعی و بدافزارهای خودکار، تهدیدات جدیدی را برای مدیریت داده‌ها ایجاد کرده‌اند. این حملات می‌توانند به خدمات و برنامه‌های کاربردی در محیط‌های هوشمند، به ویژه در زیرساخت‌های حیاتی مانند شبکه‌های برق هوشمند یا سیستم‌های حمل‌ونقل، آسیب‌های جدی وارد کنند (احمدی، ۱۴۰۲). برای مقابله با این تهدیدات فزاینده، راهبردهای نوینی مطرح شده‌اند که هر یک به‌گونه‌ای به تقویت امنیت سیستم‌های اطلاعاتی کمک می‌کنند. از جمله این راهبردها می‌توان به استفاده از فناوری بلاک‌چین برای تضمین یکپارچگی داده‌ها، استفاده از روش‌های رمزنگاری پیشرفته برای محافظت از اطلاعات حساس، و به‌کارگیری هوش مصنوعی در شناسایی الگوهای غیرعادی و پیشگیری از حملات سایبری به صورت بلادرنگ اشاره کرد. علاوه‌براین، پیاده‌سازی چارچوب‌های استاندارد امنیتیِ به‌روز، از جمله چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری (NIST Cybersecurity Framework) و استاندارد بین‌المللی ISO/IEC 27001، به سازمان‌ها امکان می‌دهد تا سیستم‌های مدیریت امنیت اطلاعات خود را به صورت ساختاریافته، جامع و متناسب با بهترین روش‌های جهانی توسعه دهند. در نهایت، ایمن‌سازی مدیریت داده در شبکه به یک نگرانی قابل‌توجه برای سازمان‌ها بخصوص بانک‌ها و متخصصان امنیت فناوری اطلاعات تبدیل شده است.

از سویی رواج هر فناوری در جامعه، نیاز به جلب اعتماد استفاده‌کنندگان از آن دارد. اعتماد به عنوان قلب سیستم بانکداری اینترنتی، مطرح شده است. در واقع اعتماد به عنوان عنصری مهم بر رفتار مصرف‌کننده، تأثیر می‌گذارد و موفقیت پذیرش تکنولوژی‌های جدید را تعیین می‌کند و امروزه بانکداران، خود را در آیینه وجود شهروندان می‌بینند و سعی می‌کنند در محیط پر از رقابت خواسته‌ها و تمایلات مشتریان خود را درک کنند و تلاش نمایند که مشتریان از آنها رضایت و خرسندی کامل داشته باشند. از این‌رو، شناسایی سطوح نیازها و انتظارات و عوامل مؤثر تأثیرگذار بر رضایت‌مندی شهروندان و بررسی نتایج نظرسنجی‌ها و سنجش میزان رضایت‌مندی مردم از خدمات بانک‌ها می‌تواند گامی اساسی برای ایجاد تحول در نظام ارائه خدمت باشد. در نتیجه، فناوری نوین باید زیرساخت‌هایی برای پذیرش و جلب اطمینان، اعتماد و رضایت شهروندان فراهم کند. آنچه در این زیرساخت‌ها باید گنجانده شود، جنبه امنیتی است که جزء زیرساخت‌های مهم برای تداوم رشد و رونق هر فناوری نوین در جامعه است؛ زیرا استفاده‌کننده باید به آن اطمینان داشته باشد. از این‌رو، مدلی جامع برای مدیریت امنیت داده در شبکه بانکی کشور احساس می‌شود که هم در جب مصرف‌کننده و هم رشد امنیت شبکه بانکی مؤثر واقع گردد. دراین‌خصوص دستورالعمل‌های بسیاری برای رعایت استانداردهای حفاظت از داده از سوی نهادهای نظارتی در اختیار بانک‌ها، شرکت‌های اصلی بانک و سایر شرکت‌های تابعه بانکی قرار می‌گیرد. بر اساس این دستورالعمل‌ها، بانک باید برنامه امنیت داده معتبر را طوری اجرا کند که شامل حراست اداری، فنی و فیزیکی مناسب بر اساس اندازه و پیچیدگی‌های بانک، ماهیت یا دامنه فعالیت آن باشد. این برنامه باید به‌نوعی طراحی شود که متضمن حفظ امنیت داده بوده و دارایی‌های اطلاعاتی را در برابر هرگونه تهدید پیش‌بینی‌ناپذیر یا خطرهای امنیتی حفظ کند (عزیزی و کردلوئی، ۱۳۹۵).

در نهایت، به دلیل آنکه بانک‌ها با تراکنش‌های مالی افراد سروکار دارند، باید به حفظ محرمانگی و امنیت دارایی‌های داده آنها بیشتر از سایر سازمان‌ها توجه کنند. از این‌رو، مدیریت هدفمند امنیت داده در بانکداری اهمیت ویژه‌ای دارد. البته ممکن است ابتدا حرکت بر اساس سیستم مدیریت امنیت داده آن هم منطبق بر استانداردهای اروپایی که تطابق کمتری با شرایط زیرساختی سازمان‌های ایرانی دارند، کمی دشوار به نظر برسد؛ اما با نگاهی عمیق‌تر می‌توان دریافت که استقرار این نظام بر اساس روش منحصربه‌فرد، تأثیر بسزایی در پیشگیری از حوادث اطلاعاتی دارد. در این وضعیت نبود مدل بهینه برای مدیریت داده در شبکه بانک‌های ایرانی کاملاً مشهود است. در این خصوص استانداردها، چارچوب‌ها و تجربه‌های زیادی در حوزه بین‌المللی ارائه شده است؛ اما آنچه اهمیت دارد، تمرکز این روش‌ها بر تعاریف و اصول مدیریت امنیت داده است، به طوری که حجم عظیمی از داده‌ها را به افراد منتقل می‌کند؛ حال‌آنکه حلقه گم شده در این بخش، به مدل گام به گامی نیاز دارد که متخصصان حوزه بانکی، متناسب با شرایط خود از آن بهره ببرند. در این پژوهش تلاش شده است با طراحی مدل خلاقانه‌ای در سطوح معین و منطبق بر نیازهای صنعت بانکداری ایران، نسبت به اجرای صحیح مدیریت امنیت داده در شبکه بانک‌های ایرانی، گامی مؤثر برداشته شود، این بررسی می‌تواند در رشد شبکه امنیت داده در شبکه بانکی کشور و سوگیری‌های امنیتی کمک شایانی نماید و همچنین این

پژوهش می‌تواند خلأ ادبیاتی مورد نظر در حیطه را پوشش دهد. از این‌رو، پژوهش حاضر درصدد این است که به طراحی مدل جامع مدیریت امنیت داده در شبکه بانکی کشور بپردازد.

ادبیات موضوع و پیشینه پژوهش

چرخه عمر داده‌ها[1]

چرخه عمر داده‌ها به مجموعه مراحلی اشاره دارد که داده‌ها از زمان ایجاد تا حذف یا آرشیو شدن طی می‌کنند. این چرخه شامل مراحل ایجاد، ذخیره‌سازی، استفاده، اشتراک‌گذاری، آرشیو و حذف است. از منظر اجتماعی، مدیریت چرخه عمر داده‌ها نقش مهمی در تضمین دسترسی عادلانه به اطلاعات و جلوگیری از تبعیض در استفاده از داده‌ها دارد. به عنوان مثال، در جوامع دیجیتال، داده‌های تولید شده توسط کاربران می‌توانند برای ارائه خدمات بهتر یا تبلیغات هدفمند استفاده شوند، اما بدون مدیریت مناسب، ممکن است به نقض حریم خصوصی یا سوءاستفاده منجر شود. سیاست‌های مؤثر چرخه عمر داده‌ها می‌توانند اعتماد عمومی را تقویت کرده و از سوءاستفاده‌های اجتماعی مانند تبعیض نژادی یا جنسیتی در تحلیل داده‌ها جلوگیری کنند.

مدیریت چرخهٔ عمر داده‌ها همچنین به سازمان‌ها کمک می‌کند تا با مقررات اجتماعی و قانونی، مانند قانون محافظت از داده‌های عمومی[2] در اروپا، هم‌راستا شوند. این مقررات بر حفاظت از داده‌های شخصی و حقوق افراد در جوامع دیجیتال تأکید دارند. یک چارچوب قوی چرخه عمر داده‌ها می‌تواند به کاهش ریسک‌های اجتماعی، مانند نقض داده‌ها یا استفاده غیراخلاقی از اطلاعات، کمک کند. برای مثال، در مرحله حذف داده‌ها، اطمینان از نابودی امن داده‌های غیرضروری می‌تواند از دسترسی غیرمجاز و سوءاستفاده‌های اجتماعی جلوگیری کند. از سوی دیگر، چرخه عمر داده‌ها می‌تواند در توانمندسازی جوامع از طریق شفافیت و دسترسی به داده‌های عمومی نقش داشته باشد. داده‌های باز[3] که به درستی مدیریت شوند، می‌توانند به شهروندان امکان مشارکت فعال در تصمیم‌گیری‌های اجتماعی و نظارت بر عملکرد نهادها را بدهند. بااین‌حال، چالش‌هایی مانند عدم دسترسی برابر به فناوری یا سواد داده‌ای پایین در برخی جوامع می‌تواند شکاف دیجیتال را تشدید کند (کایلان[4]، ۲۰۲۳).

معماری اطلاعات[5]

معماری اطلاعات به سازماندهی و ساختاردهی اطلاعات به‌گونه‌ای اشاره دارد که دسترسی و استفاده از آن‌ها برای کاربران آسان‌تر شود. از منظر اجتماعی، معماری اطلاعات در ایجاد تجربه‌های کاربری فراگیر و عادلانه نقش کلیدی دارد. یک معماری اطلاعات خوب می‌تواند به کاهش شکاف‌های دیجیتال در جوامع کمک کند، به ویژه برای گروه‌هایی که دسترسی محدودی به فناوری دارند یا مهارت‌های دیجیتال ضعیفی دارند. برای مثال، طراحی وب‌سایت‌های دولتی با معماری اطلاعات ساده و قابل‌فهم می‌تواند مشارکت اجتماعی را افزایش دهد.

در سطح اجتماعی، معماری اطلاعات بر نحوه تعامل افراد با سیستم‌های دیجیتال تأثیر می‌گذارد. طراحی ضعیف معماری اطلاعات می‌تواند به سردرگمی، کاهش اعتماد به پلتفرم‌های دیجیتال و حتی محرومیت برخی گروه‌ها از خدمات منجر شود. به عنوان مثال، در سیستم‌های سلامت دیجیتال، معماری اطلاعات ناکارآمد ممکن است مانع دسترسی بیماران به اطلاعات پزشکی خود شود که این امر به ویژه برای جوامع محروم تأثیرات منفی بیشتری دارد. علاوه بر این، معماری اطلاعات می‌تواند به تقویت شفافیت اجتماعی کمک کند. با سازماندهی داده‌ها به‌گونه‌ای که قابل‌جستجو و قابل‌فهم باشد، افراد می‌توانند به اطلاعات عمومی

---

1. Data Lifecycle
2. General Data Protection Regulation
3. Open Data
4. Kalyan
5. Information Architecture

دسترسی پیدا کنند و از حقوق خودآگاه شوند. این امر به ویژه در زمینه‌هایی مانند آموزش‌وپرورش یا خدمات عمومی اهمیت دارد، جایی که معماری اطلاعات قوی می‌تواند به کاهش نابرابری‌های اجتماعی کمک کند (استرنگلوت[1]، ۲۰۲۳).

مدل‌های حاکمیت داده[2]

مدل‌های حاکمیت داده چارچوب‌هایی هستند که سیاست‌ها، فرایندها و استانداردها را برای مدیریت داده‌ها در سازمان‌ها تعریف می‌کنند. از منظر اجتماعی، حاکمیت داده به تضمین اعتماد عمومی و حفاظت از حقوق افراد در برابر سوءاستفاده از داده‌ها کمک می‌کند. این مدل‌ها می‌توانند از تبعیض در تحلیل داده‌ها جلوگیری کرده و اطمینان حاصل کنند که داده‌ها به صورت عادلانه و شفاف استفاده می‌شوند. برای مثال، مدل‌های بلوغ حاکمیت داده شرکت ارائه‌دهنده محصولات و خدمات فناوری (IBM)[3] بر یازده حوزه کلیدی تمرکز دارند که شامل کیفیت داده، امنیت و یکپارچگی است و این امر به کاهش سوگیری‌های اجتماعی در تصمیم‌گیری‌های مبتنی بر داده کمک می‌کند. حاکمیت داده همچنین به ایجاد مسئولیت‌پذیری اجتماعی در سازمان‌ها کمک می‌کند. با پیاده‌سازی سیاست‌های قوی، سازمان‌ها می‌توانند از داده‌ها برای بهبود خدمات عمومی، مانند برنامه‌ریزی شهری یا مراقبت‌های بهداشتی، استفاده کنند بدون اینکه به حریم خصوصی افراد لطمه بزنند. این امر به ویژه در جوامعی که اعتماد به نهادها پایین است، اهمیت دارد. مدل‌های حاکمیت داده می‌توانند با ارائه چارچوب‌های شفاف، اعتماد عمومی را تقویت کنند. چالش‌های اجتماعی در حاکمیت داده شامل تفاوت‌های فرهنگی در درک حریم خصوصی و مدیریت داده است. در برخی جوامع، آگاهی عمومی از حقوق داده‌ای پایین است که می‌تواند به سوءاستفاده از داده‌ها منجر شود. مدل‌های بلوغ، مانند مدل IBM، می‌توانند به سازمان‌ها کمک کنند تا این چالش‌ها را شناسایی و برطرف کنند (موسوی و همکاران، ۲۰۲۳).

اعتماد دیجیتال[4]

اعتماد دیجیتال به اطمینان افراد و جوامع به سیستم‌های دیجیتال، فناوری‌ها و سازمان‌هایی که داده‌های آن‌ها را مدیریت می‌کنند، اشاره دارد. از منظر اجتماعی، اعتماد دیجیتال برای پذیرش فناوری‌های جدید، مانند هوش مصنوعی یا اینترنت اشیا، ضروری است. بدون اعتماد، افراد ممکن است از مشارکت در خدمات دیجیتال خودداری کنند که این امر می‌تواند شکاف دیجیتال را در جوامع تشدید کند. برای مثال، در جوامعی باسابقه نقض داده‌ها، اعتماد دیجیتال پایین‌تر است و نیاز به شفافیت و امنیت بیشتر دارد. اعتماد دیجیتال همچنین به برابری در دسترسی به فناوری وابسته است. در جوامع محروم، عدم دسترسی به آموزش دیجیتال یا زیرساخت‌های مناسب می‌تواند اعتماد به سیستم‌های دیجیتال را کاهش دهد. سازمان‌ها با ارائه سیستم‌های شفاف و کاربرمحور می‌توانند اعتماد دیجیتال را تقویت کنند. برای مثال، استفاده از فناوری‌های بلاک‌چین برای تضمین شفافیت داده‌ها می‌تواند اعتماد عمومی را افزایش دهد. چالش دیگر در اعتماد دیجیتال، تأثیرات اجتماعی ناشی از نقض داده‌ها یا استفاده غیراخلاقی از اطلاعات است. این موضوع می‌تواند به کاهش مشارکت اجتماعی و افزایش بدبینی نسبت به فناوری منجر شود. سیاست‌های قوی حفاظت از داده‌ها و آموزش عمومی می‌توانند این چالش‌ها را کاهش دهند (سارکر[5] و حسین، ۲۰۲۴).

حریم خصوصی[6]

حریم خصوصی به حق افراد برای کنترل اطلاعات شخصی خود و نحوه استفاده از آن‌ها اشاره دارد. از منظر اجتماعی، حریم خصوصی به عنوان یک حق اساسی در جوامع دیجیتال شناخته می‌شود و نقض آن می‌تواند به کاهش اعتماد عمومی و افزایش نابرابری‌ها منجر شود. برای مثال، جمع‌آوری داده‌های شخصی بدون رضایت کاربران می‌تواند به تبعیض هدفمند، مانند تبلیغات ناعادلانه یا پروفایل‌سازی نژادی، منجر شود. در جوامع دیجیتال، قوانین حریم خصوصی مانند قانون محافظت از داده‌های عمومی

---

1. Strengholt
2. Data Governance Models
3. International Business Machines
4. Digital Trust
5. Sarker
6. Privacy

به حفاظت از داده‌های شخصی کمک می‌کنند، اما چالش‌هایی مانند تفاوت‌های فرهنگی در درک حریم خصوصی همچنان باقی است. در برخی جوامع، آگاهی از حقوق حریم خصوصی پایین است که این امر می‌تواند به سوءاستفاده از داده‌ها منجر شود. آموزش عمومی و سیاست‌های شفاف می‌توانند این شکاف را کاهش دهند. حریم خصوصی همچنین بر مشارکت اجتماعی تأثیر می‌گذارد. زمانی که افراد احساس کنند داده‌هایشان امن نیست، ممکن است از خدمات دیجیتال، مانند برنامه‌های سلامت یا آموزش برخط، استفاده نکنند. این موضوع به ویژه در جوامع محروم که دسترسی به فناوری محدود است، تأثیرات منفی بیشتری دارد (اکیوستی و گارسکلاگ[1]، ۲۰۲۳).

اخلاق داده[2]

اخلاق داده به اصول و ارزش‌هایی اشاره دارد که استفاده مسئولانه از داده‌ها را هدایت می‌کنند. از منظر اجتماعی، اخلاق داده در جلوگیری از سوءاستفاده از اطلاعات و تضمین عدالت در تحلیل داده‌ها نقش دارد. برای مثال، استفاده غیراخلاقی از داده‌ها در الگوریتم‌های هوش مصنوعی می‌تواند به تبعیض علیه گروه‌های خاص، مانند اقلیت‌ها، منجر شود. چارچوب‌های اخلاقی می‌توانند با ترویج شفافیت و پاسخگویی، اعتماد اجتماعی را تقویت کنند. اخلاق داده همچنین به کاهش نابرابری‌های اجتماعی کمک می‌کند. در جوامعی که داده‌ها برای تصمیم‌گیری‌های کلان، مانند تخصیص منابع عمومی، استفاده می‌شوند، رعایت اصول اخلاقی می‌تواند از سوگیری‌های غیرمنصفانه جلوگیری کند. برای مثال، الگوریتم‌های استخدام که بدون توجه به اخلاق داده طراحی شده‌اند، ممکن است به تبعیض جنسیتی یا نژادی منجر شوند. چالش‌های اجتماعی در اخلاق داده شامل تفاوت‌های فرهنگی در درک ارزش‌های اخلاقی و کمبود آگاهی عمومی است. آموزش و تدوین دستورالعمل‌های جهانی می‌تواند به ترویج استفاده اخلاقی از داده‌ها کمک کند و از تأثیرات منفی بر جوامع جلوگیری کند (فلوریدی و تادو[3]، ۲۰۲۴).

بانکداری الکترونیکی و امنیت داده

در حوزه بانکداری الکترونیکی و امنیت سایبری، این اصطلاحات به فناوری‌ها، روش‌ها و فرایندهایی اشاره دارند که از داده‌ها، شبکه‌ها و برنامه‌های رایانه‌ای در برابر حملات سایبری محافظت می‌کنند. تهدید امنیت سایبری نوعی تروریسم مالی است که به طور فزاینده‌ای شایع شده است. چالش‌برانگیزترین جنبه بانکداری الکترونیکی مدرن، محافظت از اطلاعات شخصی مشتریان بوده است. امنیت سایبری راهبردی برای جلوگیری از حملات سایبری در فضای مجازی است. نقض هر سیستم امنیت سایبری منجر به ضررهای مالی و غیرمالی برای سازمان قربانی و مشتریان آن می‌شود، بنابراین امنیت سایبری به دنبال جلوگیری از این ضررها است (قلانی[4] و همکاران، ۲۰۲۲).

سرقت اطلاعات محرمانه و اطلاعات حساس مصرف‌کننده مانند شماره شناسایی و شماره‌حساب‌ها نمونه‌هایی از ضررهای غیرمالی هستند. جرایم سایبری مسئله‌ای جهانی با پیامدهای اقتصادی شدید برای جامعه آفریقای جنوبی است. محافظت از اطلاعات محرمانه نگرانی حیاتی در مورد امنیت سایبری و حریم خصوصی در حوزه بانکداری الکترونیکی است (پروج[5] و همکاران، ۲۰۲۱). با پیشرفت فناوری، بخش بانکداری تحول‌یافته و بانکداری اینترنتی به روشی مناسب‌تر برای انجام کسب‌وکار تبدیل شده است. بانک‌های آفریقای جنوبی به طور مرتب از پلتفرم‌های شخص ثالث مانند PayPal برای انجام معاملات بین‌المللی و داخلی استفاده می‌کنند. ازآنجایی‌که مدیریت این سیستم‌ها خارج از کنترل بانک‌ها است، وابستگی آنها به سیستم‌های شخص ثالث برای ارائه خدمات دیجیتالی به مشتریان، ریسک امنیتی شدیدی ایجاد می‌کند. همان‌طور که سیستم‌ها به هم متصل‌تر می‌شوند، وابستگی افزایش می‌یابد و خطر نقض یا حملات سایبری نیز افزایش می‌یابد. کنترل این تهدیدها

---

1. Acquisti & Grossklags
2. Data Ethics
3. Floridi & Taddeo
4. Ghelani
5. Perwej

مستلزم محدودکردن و کاهش‌دادن حملات قبل از وقوع آنها که به آن مدیریت ریسک گفته می‌شود (وینوس[1] و همکاران، ۲۰۲۲).

خدمات ارائه شده از امنیت داده در بانکداری الکترونیکی

- پایش سایبری[2]: یک راه‌حل مدیریت اطلاعات و رویدادهای امنیتی در زمان واقعی که ۲۴ ساعته و ۷ روزه تهدیدات را شناسایی، تحلیل، هشدار، گزارش و پاسخ می‌دهد.
- نظارت سایبری[3]: یک فید اطلاعات تهدید که دقیق و شخصی‌سازی شده است تا حملات بالقوه را قبل از وقوع شناسایی کند. اسکن مداوم آسیب‌پذیری‌ها و کنترل توسط نظارت سایبری ارائه می‌شود.
- پاسخ سایبری[4]: به رویدادهای سایبری پاسخ داده و سیستم‌ها و شبکه‌های سازمان را دفاع می‌کند. راهبردهای سنتی مدیریت ریسک بانک‌ها معمولاً بر اختلال در یک نقطه حمله متمرکز بودند. بااین‌حال، با تحول دنیای دیجیتال، حمله اکنون می‌تواند به طور هم‌زمان چندین سیستم و فرایند را هدف قرار دهد که منجر به عواقب مالی گسترده برای مؤسسه می‌شود.

بانکداری الکترونیکی به عنوان بخشی از اینترنت اشیا (IoT) اهمیت روزافزون پیدا می‌کند و این پلتفرم‌ها با نگرانی‌های امنیتی خاص خود همراه هستند. IoT به شبکه‌ای از اشیای فیزیکی اشاره دارد که می‌توانند داده‌ها را جمع‌آوری و به اشتراک بگذارند. این اشیا می‌توانند شامل دستگاه‌ها، ساختمان‌ها و سایر موارد باشند. با گسترش IoT در زندگی روزمره، نگرانی‌های مربوط به حریم خصوصی و امنیت افزایش می‌یابد. حملات سایبری خطری هستند که می‌توانند در محیط فناورانه امروز به دلیل کمبود آگاهی کاربران از امنیت سایبری رخ دهند. دنیای فیزیکی به یک سیستم اطلاعاتی گسترده به دلیل اینترنت اشیا تبدیل می‌شود، باهدف نهایی افزایش کیفیت زندگی و امکان ایجاد مدل‌های اقتصادی جدید. برای مقابله با حملات سایبری، از تدابیر امنیتی ارتباطات سنتی استفاده شده است که احراز هویت و کنترل دسترسی لایه اول دفاعی را ارائه می‌دهند. این راهبردها ناکارآمد بوده‌اند؛ زیرا باید با سایر تدابیر امنیتی مانند کنترل‌های رویه‌ای و امنیت فردی ترکیب شوند.

سیستم‌های اطلاعاتی (IS) اخیراً در عصر اینترنت در معرض محیط‌های در حال تغییر سریع قرار گرفته‌اند. برای مثال، فراوانی حملات با زمان (روزهای کاری و تعطیلات) و تخصص کاربران و هکرها تغییر می‌کند. در نتیجه، ریسک سیستم‌های اطلاعاتی برای همه مکان‌ها یکسان نیست. ممکن است یک اقدام ضد حمله در یک‌زمان مؤثر باشد؛ اما در زمان دیگر بی‌اثر باشد. دفاع از سیستم‌های اطلاعاتی در برابر خطرات بسیار هزینه‌بر است و نرخ شکست بالایی دارد. یک سیستم اطلاعاتی کارآمد باید الگوی حملات به سیستم اطلاعاتی را در طول زمان تحلیل کرده و اقدامات امنیتی متناسب با خطر فعلی را ارائه دهد تا به طور مؤثر و با هزینه کم از خود محافظت کند. در این شرایط، اتخاذ همه تصمیمات امنیتی در زمان طراحی کافی نیست؛ در عوض، اطلاعات امنیتی باید در زمان اجرا مدیریت شود.

مدیریت ریسک امنیتی فرایندی مبتنی بر دانش است که نیازمند پایش و ثبت داده‌های مهم است که به مدیران در اتخاذ بهترین تصمیم ممکن کمک می‌کند. در این مطالعه، یک پارادایم معنایی بهبودیافته برای مدیریت امنیت در طول چرخه عمر یک سیستم اطلاعاتی ارائه شده است. این مدل امکان جمع‌آوری مداوم رفتارهای تهدید شناسایی شده از سیستم تشخیص نفوذ، فیلتر و تحلیل تهدیدات در یک‌لحظه زمانی و بازنگری مجدد اقدامات امنیتی سیستم اطلاعاتی با ذی‌نفعان شامل مدیر امنیت، مدیران و سیستم مدیریت امنیت و اطلاعات را فراهم می‌کند. عامل پروب با استفاده از پایگاه دانش هدایت شده با هستی‌شناسی، ریسک‌های امنیتی شناسایی شده توسط سیستم تشخیص نفوذ را طبقه‌بندی می‌کند. در مقابل، احتمال فراوانی بلندمدت برای تعیین احتمال وقوع تهدیدات در زمان واقعی استفاده شده است. راه‌حل‌های امنیتی پیشنهادی بر اساس هستی‌شناسی تهدید

[1]. Vinoth
[2]. Cyber Monitor
[3]. Cyber Watch
[4]. Cyber Respond

موجود (CASE) است. بازبین مبتنی بر احتمال ادامه تهدیدات موفق است. این سیستم به مدیریت در انتخاب اقدامات کنترلی امنیتی کمک می‌کند تا بازده سرمایه‌گذاری امنیتی خود را افزایش دهند. یک سیستم بانکداری الکترونیکی رویکرد پیشنهادی جمع‌آوری – پروب – تحلیل – استدلال – بازنگری را نشان می‌دهد. در دنیای امروز، تجربه نشان داده است که تأمین امنیت داده دولتی در بخش بانکداری نقش حیاتی در حفاظت از امنیت ملی اوکراین، به ویژه جنبه اقتصادی آن (BNC) ایفا می‌کند. نظریه و عمل نقش کلیدی و سیستم‌ساز در فرایند توسعه سیستم ارائه اطلاعات بانکی (BIn) به عنوان بخشی از منابع اطلاعاتی ملی دولت ایفا می‌کنند که در آن مبنای علمی و روش‌شناختی به عنوان پایه‌ای برای اتخاذ تصمیمات مدیریتی آگاهانه و مؤثر توسط نهادهای ارائه‌دهنده بودجه دولتی در تمام سطوح خدمت می‌کند. تحولات انقلابی دهه گذشته در بخش بانکداری منجر به یکپارچه‌سازی شبکه‌های اطلاعاتی و رایانه‌ای در یک فضای اطلاعاتی و سایبرنتیکی واحد شده است که به ایجاد سیستم‌های بانکداری خودکار منجر شده است که دامنه خدمات الکترونیکی ارائه شده توسط بانک‌های دولتی و تجاری در سراسر جهان، از جمله در اوکراین، را به طور قابل‌توجهی گسترش داده است. در نتیجه، ریسک‌های مربوط به منبع اطلاعاتی ملی دولت، BIn، به‌شدت تغییر کرده است. تهدیدها شروع به ترکیب‌شدن کرده‌اند. به دلیل تأثیر هم‌زمان بر هدف حفاظت، هیبریدی شدن تهدیدات مانند امنیت داده (IS)، امنیت سایبری (CS) و امنیت داده (SI) شروع به ظهور کرده است.

جدول ۱. پیشینه داخلی و خارجی پژوهش

پیشینه داخلی				
ردیف	**نویسنده و سال**	**عنوان**	**روش**	**یافته‌ها**
۱	آزاد سنجری و چهارسوقی (۱۴۰۳)	نوآوری‌ها و توسعه امنیت سایبری در بانک‌های ایران: تحلیل SWOT و مقایسه فرصت‌ها	مدل SWOT	با توجه به گزارش‌های امنیتی، بدافزارهای بانکی و کلاه برداری‌های مالی طی چند دهه اخیر، رشد چشمگیری داشته است و با توجه به افزایش پیچیدگی حملات سایبری و سرعت بالای تهدیدات نوظهور، استفاده از استراتژی‌های امنیتی سنتی دیگر پاسخگوی نیازهای بانک‌های ایران نیستند.
۲	وجدانی (۱۴۰۳)	بررسی اثرگذاری حریم خصوصی و امنیت خدمات بانکداری الکترونیک بر وفاداری مشتریان بانکی با تأکید بر قابلیت اطمینان	روش معادلات ساختاری	با توجه به این مزیت‌ها است که در ساله‌ای اخیر، اقداماتی به‌منظور حرکت به‌سوی بانکداری الکترونیکی از سوی نظام بانکی کشور صورت‌گرفته است. در مقاله حاضر به موضوع بررسی اثرگذاری حریم خصوصی و امنیت خدمات بانکداری الکترونیکی بر وفاداری مشتریان بانکی با تأکید بر قابلیت اطمینان پرداخته شده است و نتایج حاصل نشان از تأیید فرضیه‌های مقاله در سطح اطمینان ۹۵ درصد داشته است.
۳	دروی و جمشیدی (۱۴۰۰)	بررسی سنجش مؤلفه‌های امنیت داده در دسترسی و استفاده از کتابخانه‌های دیجیتال	پیمایشی تحلیلی و جامعه پژوهش، کتابخانه‌های دیجیتال «شهرستان قم» اعم از عمومی و دانشگاهی (شامل ۵ کتابخانه)	توسعه سیستم‌های اطلاعاتی برای ارائه خدمات مؤثر در کتابخانه‌های دیجیتال نقشی مؤثر داشته است. همچنین، رابطه‌ای معنادار میان شاخص‌های مختلف امنیت داده در کتابخانه‌های دیجیتال «شهرستان قم» وجود دارد. در این پژوهش امنیت فیزیکی و محیطی به عنوان نقطه‌ضعف و مدیریت تداوم کسب‌وکار به عنوان نقطه قوت معرفی شده است. بهره‌گیری از پدافند غیرعامل، مشارکت گروه‌های امنیتی برای جلوگیری از فعالیت هکرها، شناسایی حفره‌های امنیتی، آموزش نیروهای متخصص و داشتن برنامه اجرایی امنیت داده از جمله پیشنهادهای این پژوهش است. در نهایت، باید بیان کرد که امنیت داده در کتابخانه‌های شهرستان قم از سطح بالایی برخوردار است.
۴	فراهانی و همکاران (۱۴۰۰)	بررسی ارائه مدل مفهومی مؤلفه‌ها و شاخص‌های سرمایه انسانی مؤثر بر امنیت داده سازمان‌ها	توصیفی هم‌بستگی و از نوع تحقیقات کاربردی	متغیرهای مدیریت و رهبری، آموزش کارکنان، فرهنگ امنیتی، تقویت سیاست‌های امنیتی، تجربیات و خودباوری افراد به عنوان شاخصه‌های سرمایه انسانی مؤثر بر امنیت داده سازمان‌ها معرفی شده‌اند.
۵	مغنی و همکاران (۱۳۹۸)	چگونگی تأثیر گسترش فناوری‌های مالی بر بهبود عملکرد خدمات مالی	آمیخته (کیفی – کمی)	سهولت خدمات و شخصی‌سازی خدمات و نوآوری خدمات بیشتری کمیت را داشته‌اند.

پیشینه خارجی				
۱	لی و همکاران (۲۰۲۱)	بررسی رضایت مشتری از خدمات بانک: نقش خدمات ابری، امنیت، آموزش الکترونیکی و کیفیت خدمات	معادلات ساختاری	نتایج نشان داده است که خدمات ابری، امنیت، آموزش الکترونیکی و کیفیت خدمات چهار عامل مهم تأثیرگذار بر رضایت مشتری در استفاده از خدمات بانکداری اینترنتی هستند.
۲	کیمیاگری و بائی (۲۰۲۱)	بررسی ارتقای استفاده واقعی بانکداری الکترونیک	آمیخته	نتایج نشان می‌دهد که مدل برازش وظیفه – فناوری و نوآوری خدمات فنی به عنوان زمینه فناوری به طور مثبت بر استفاده واقعی بانکداری الکترونیکی تأثیر می‌گذارد و ویژگی‌های وظیفه و فناوری به طور مثبت بر تناسب وظیفه – فناوری تأثیر می‌گذارد. ادغام کاربر و اندازه درک شده به عنوان زمینه‌سازمانی به ترتیب بر قصد رفتار و استفاده واقعی کاربران تأثیر مثبت می‌گذارد. علاوه بر این، مدل اعتماد اولیه به عنوان زمینه محیطی بر قصد رفتار کاربران تأثیر مثبت می‌گذارد. تضمین ساختاری به طور مثبت بر اعتماد اولیه تأثیر می‌گذارد، اما تأثیر اجتماعی و تأثیر شهرت بانک رد می‌شود. همچنین، تناسب فرهنگ–فناوری و حمایت دولت به عنوان زمینه محیطی بر استفاده واقعی بانکداری الکترونیکی تأثیر مثبت دارد.
۳	کیریلو[1] و همکاران (۲۰۲۱)	بررسی استفاده از فناوری‌های بیومتریک برای مدیریت امنیت تراکنش‌های بانکی در برابر پس‌زمینه تجربه بین‌المللی	فراترکیب	اجرای بیشتر بیومتریک در بخش بانکداری در اوکراین نیازمند یک رویکرد جامع و در نظر گرفتن بهترین شیوه‌های جهانی است. در مورد بانک اطلاعاتی در حال گسترش است.
۴	خروشچ[2] و همکاران (۲۰۲۰)	ارزیابی سطوح امنیت مالی بانک بر اساس یک شاخص جامع با استفاده از فناوری اطلاعات	الگوریتم محاسباتی	نتایج گروه‌بندی عموماً با نتایج رتبه‌بندی بانک‌ها بر اساس ارزیابی رتبه‌بندی ثبات آنها، ارائه شده در آمارهای رسمی، مطابقت داشت. این مقاله اجرای عملی روش محاسباتی پیشنهادی را ارائه می‌کند. برای خودکارسازی محاسبات و امکان مدل‌سازی سناریو، یک فرم الکترونیکی از یک صفحه گسترده با کمک کنترل‌های فرم ایجاد شد. نتایج به دست آمده این امکان را می‌دهد که تعداد سطوح امنیت مالی و مرزهای آنها شناسایی شود.
۵	اسچالز[3] و همکاران (۲۰۲۰)	گزینه‌هایی برای بهبود مدل عمومی مدیریت امنیت در بانک خصوصی با رعایت مقررات حفاظت از داده‌های عمومی	کیفی	این مقاله بینشی برای پرداختن به امنیت در بانک خصوصی ارائه می‌دهد که در حال حاضر معیارهای جدید تصویب شده از مقررات عمومی حفاظت از داده‌ها را برآورده می‌کند.

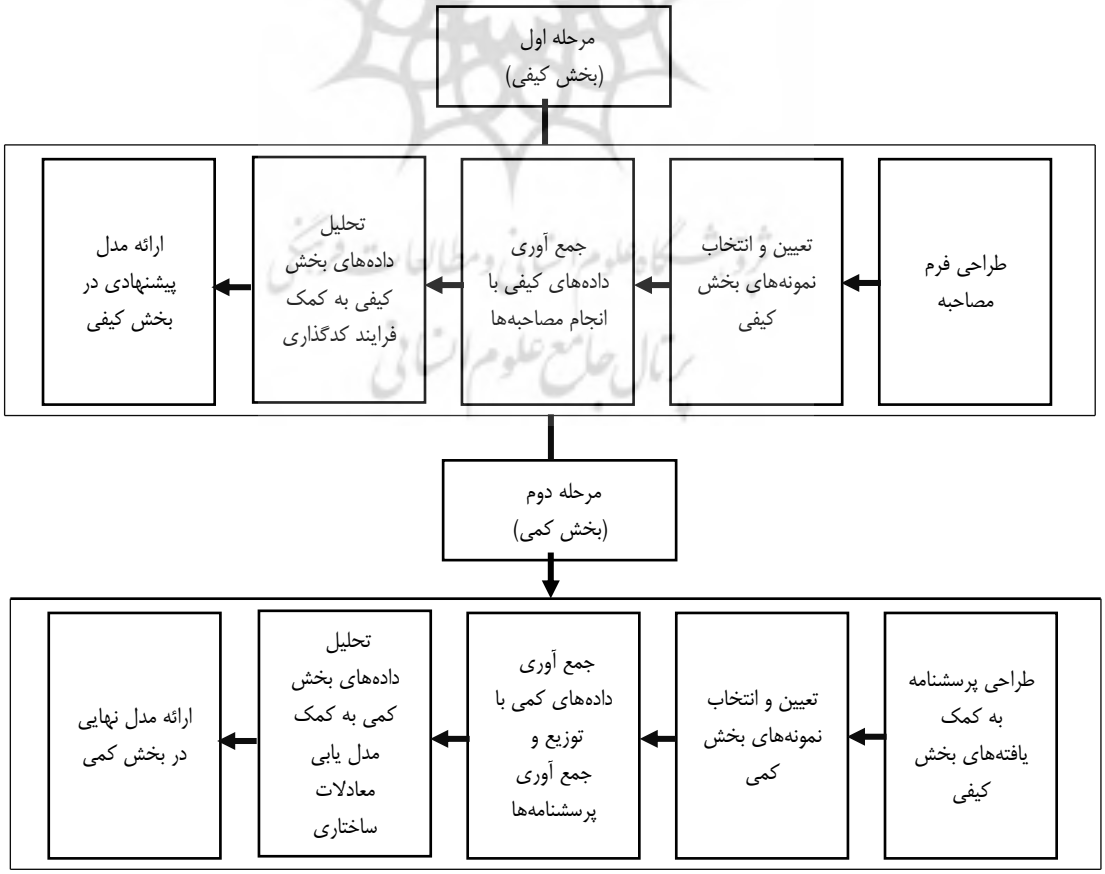
با توجه به آنچه ذکر شد، در پیشینه داخلی، از روش‌های مختلفی مانند مدل SWOT، معادلات ساختاری، پیمایشی و آمیخته استفاده شده است. این تنوع نشان‌دهندهٔ رویکردهای چندجانبه به موضوعات امنیت داده و بانکداری دیجیتال است. نیز با استفاده از روش‌های کیفی، کمی و فراترکیب به بررسی موضوعات مشابه پرداخته‌اند. این نشان‌دهندهٔ توجه به جنبه‌های مختلف موضوع و تلاش برای ایجاد یک چارچوب جامع‌تر است. در تحقیقات داخلی، به وضوح به رشد تهدیدات سایبری و ناکافی بودن استراتژی‌های امنیتی سنتی اشاره شده است. این نکته به ویژه در مقاله آزاد سنجری و چهارسوقی (۱۴۰۳) مشهود است. در کار وجدانی (۱۴۰۳)، تأثیر حریم خصوصی و امنیت بر وفاداری مشتریان به خوبی بررسی شده است، که نشان‌دهندهٔ اهمیت این عوامل در جذب و حفظ مشتریان است. پژوهش‌های مغنی و همکاران (۱۳۹۸) و کیمیاگری و بائی (۲۰۲۱) به تأثیر نوآوری در بهبود عملکرد خدمات مالی و استفاده از بانکداری الکترونیکی پرداخته‌اند. این نشان‌دهندهٔ اهمیت نوآوری در جذب مشتریان و بهبود خدمات است. در تحقیقات مختلف، مدل‌های مفهومی برای ارزیابی و بهبود امنیت داده پیشنهاد شده است. این مدل‌ها می‌توانند به عنوان ابزارهایی برای تحلیل و بهینه‌سازی فرایندهای امنیتی مورد استفاده قرار گیرند. تحقیقات انجام شده در زمینه امنیت داده نشان می‌دهد که با افزایش پیچیدگی حملات سایبری و ظهور تهدیدات نوین، بانک‌ها و مؤسسات مالی با چالش‌های جدی مواجه هستند. به ویژه، در مطالعات آزاد سنجری و چهار سوقی (۱۴۰۳) و وجدانی (۱۴۰۳)، به وضوح مشخص شده است

[1]. Kurylo
[2]. Khrushch
[3]. Schulz

که استراتژی‌های امنیتی سنتی دیگر قادر به پاسخگویی به نیازهای روز نیستند. این امر نه‌تنها به دلیل افزایش تعداد و تنوع حملات، بلکه به دلیل تغییرات سریع در انتظارات مشتریان و نیاز به خدمات سریع و امن است. بنابراین، بانک‌ها باید به‌سرعت به سمت نوآوری و به‌کارگیری فناوری‌های پیشرفته‌تر در زمینه امنیت داده حرکت کنند، تا بتوانند اعتماد مشتریان را جلب کرده و وفاداری آنها را حفظ کنند. با توجه به سرعت تغییرات فناوری و ظهور تهدیدات جدید، نیاز به رویکردهای نوآورانه در تحقیقات امنیت داده و بانکداری دیجیتال احساس می‌شود. پژوهش‌های خارجی، مانند کار کیمیاگری و بائی (۲۰۲۱)، به خوبی نشان می‌دهند که ادغام فناوری‌های جدید، مانند بیومتریک و خدمات ابری، می‌تواند به بهبود امنیت و رضایت مشتریان کمک کند. همچنین، همکاری بین پژوهشگران داخلی و خارجی می‌تواند به تبادل تجربیات و بهترین شیوه‌ها منجر شود و به توسعه مدل‌های جامع‌تری برای مدیریت امنیت داده کمک کند. در نهایت، این تلاش‌ها می‌تواند به ایجاد یک اکوسیستم امن و پایدار در بانکداری دیجیتال منجر شود که نه‌تنها به نفع بانک‌ها، بلکه به نفع مشتریان نیز خواهد بود. با توجه به تنوع و گستردگی موضوعات تحقیقاتی، نیاز به هم‌افزایی و همکاری بین پژوهشگران داخلی و خارجی احساس می‌شود. این همکاری می‌تواند به تبادل تجربیات و بهترین شیوه‌ها کمک کند. با توجه به سرعت تغییرات فناوری و تهدیدات نوظهور، استمرار تحقیقات در زمینه امنیت داده و بانکداری دیجیتال ضروری است. این تحقیقات باید به طور مداوم به‌روز شوند تا بتوانند نیازهای روز جامعه را برآورده کنند. در نهایت، پیشینه‌های داخلی و خارجی در زمینه امنیت داده و بانکداری دیجیتال به خوبی نشان‌دهندهٔ چالش‌ها، فرصت‌ها و نیاز به بهبود در این حوزه‌ها هستند.

روش‌شناسی

این پژوهش از نظر هدف کاربردی، از نظر ماهیت داده‌ها کیفی-کمی (آمیخته)، از نظر گردآوری داده‌ها توصیفی پیمایشی، با رویکرد مصاحبه و از نظر استراتژی میدانی است. با توجه به ماهیت اکتشافی موضوع تحقیق از طرح پژوهش آمیخته اکتشافی متوالی استفاده شد که در دوفاز کیفی و کمی به انجام رسید. در شکل ۱ نیز روند جمع‌آوری اطلاعات شرح داده شده است.



شکل ۱. مراحل روش تحقیق به کار گرفته شده

جامعه آماری در بخش کیفی متشکل از مدیران، مسئولان، مدیران کل و معاونان، خبرگان و کارشناسان بانک‌های کشور بودند که به صورت هدفمند این افراد جهت مصاحبه‌های کیفی در موضوع تحقیق نمونه‌گیری و انتخاب شدند؛ لازم به ذکر است پس از مصاحبه نفر بیست و یک به بعد، تکرار در اطلاعات دریافتی مشاهده گردید؛ اما برای اطمینان تا نفر بیست و چهارم ادامه یافت و از مصاحبه نفر بیستم به بعد داده‌ها کاملاً تکراری شد و به اشباع نظری صورت گرفت. جمع‌آوری اطلاعات از خرداد ۱۴۰۰ آغاز گردید. مصاحبه با طرح سؤال «عوامل مؤثر بر طراحی مدل جامع مدیریت امنیت داده در شبکه بانکی کشور کدامند ؟» آغاز شد (مصاحبه باز) و باقی پرسش‌ها براساس مبانی نظری و با رویکرد تئوری مطرح گردید و در نهایت، سؤالات نهایی بر اساس پاسخ‌های مصاحبه شونده طرح شد. مدت زمان هر مصاحبه از ۴۵ دقیقه تا ۲ ساعت (بسته به نظر فرد) بود و در بعضی موارد در دو جلسه انجام شد. تمامی مصاحبه‌ها ثبت گردید وبرای استخراج نکات کلیدی چندین بار مورد بررسی قرار گرفت.

جامعه و نمونه آماری پژوهش حاضر در بخش کمی شامل (رگولاتور، بانک‌های دولتی و خصوصی، تأمین‌کننده کسب‌وکارهای بانکداری متمرکز و جامع، کسب کارهای تأمین امنیت شبکه و داده در صنعت بانکی دارای مجوز و تأییدیه از مراجع ذی‌صلاح امنیتی، نهادهای حاکمیتی، نظارتی، تدوین‌کننده مقررات و دستورالعمل‌های امنیت داده بالادستی و مرتبط) شامل می‌شد که مجموعاً ۱۲۶ نفر را شامل شدند که به روش نمونه‌گیری تمام شمار، کل افراد در پژوهش حاضر شرکت داده شدند. برای گردآوری اطلاعات در بخش کیفی و کمی از جامعه آماری مدنظر از روش میدانی استفاده شد. ابزار گردآوری اطلاعات از پرسش‌نامه محقق ساخته و مصاحبه نیمه‌ساختاریافته استفاده گردید. پرسش‌نامه این پژوهش به همراه پایایی آن به شرح جدول ۲ بود. در این پرسشنامه از طیف پنج گزینه‌ای لیکرت استفاده گردیده است.

جدول ۲. مؤلفه‌های پرسشنامه

مؤلفه‌ها	تعداد سؤالات	ضریب آلفای کرونباخ
علل عمده حوادث امنیتی در بانک	۱-۹	۰/۸۳۸
موانع و نگرانی‌ها در اجرای انطباق امنیتی بهتر	۱۰-۱۳	۰/۷۹۷
استراتژی‌های امنیتی در شش ماه اخیر	۱۴-۱۸	۰/۸۷۲
اقدامات امنیت داده‌ها	۱۹-۲۲	۰/۸۷۵
چرخه امنیت داده‌ها	۲۳-۲۸	۰/۸۶۷
اقدامات امنیتی اضافی لازم برای بهبود امنیت داده‌ها (نحوه آمادگی امنیت داده‌ها)	۲۹-۳۳	۰/۷۶۷
مکانیسم‌های امنیت داده در خدمات بانکداری برخط	۳۴-۴۴	۰/۷۳۱
خدمات مالی تحت‌تأثیر مکانیسم‌های امنیت داده‌ها	۴۵-۴۸	۰/۷۸۱

ضریب آلفای کرونباخ به دست آمده نشان‌دهنده پایایی مطلوب پرسش‌نامه‌های پژوهش است. در نهایت در این تحقیق جهت تجزیه مصاحبه‌های نیمه‌ساختاریافته از دسته‌بندی‌ها استفاده شد. دسته‌بندی‌ها اغلب به صورت کدها یا کلمات کلیدی نام‌گذاری شده‌اند، اما به هر چیزی که نام‌گذاری شوند، همه آنها این قابلیت را دارند که داده‌ها را سازماندهی و نظام‌مند کنند، اغلب حتی به عنوان کدهای تحلیلی کار می‌کنند. کدهای تحلیلی نتیجه یک فرایند تحلیلی است که از تعیین یک موضوع فراتر می‌رود. کدگذاری اطلاعات نیز به کمک نرم‌افزار MAXQDA مورد تجزیه‌وتحلیل قرار گرفت. نرم‌افزار MAXQDA برای کدگذاری و تحلیل داده‌ها در رویکردهای مختلف پژوهش کیفی استفاده شد و برای تحلیل داده‌های به دست آمده از نمونه‌ها، از آماره‌های توصیفی شامل فراوانی، درصد، میانگین و انحراف معیار استفاده گردیده است. همچنین در بخش آمار استنباطی از روش مدل‌یابی معادلات ساختاری[1] استفاده شد. این تحلیل‌ها با استفاده از نرم‌افزار آماری SPSS نسخه ۲۷ و SmartPLS نسخه ۴ انجام گرفت.

یافته‌های پژوهش

در بخش کیفی، ابتدا به بررسی کدگذاری مصاحبه در محیط نرم‌افزاری MAXQDA پرداخته شده است. بر اساس کدهای باز، کد محوری و کد انتخابی استخراج شده است. لازم به ذکر است که این کدها بر اساس در نظر گرفتن ادبیات گذشته و بررسی استادان متخصص، به مؤلفه‌هایی کلی‌تر تبدیل شده است.

[1]. Structural Equation Modeling (SEM)

جدول ۳. یافته‌های کد انتخابی بر اساس کد محوری

تکرار	کد استخراجی (کدباز)	کد استخراجی (کد محوری)	کد استخراجی (کد انتخابی)
۵	نقص در آموزش کارکنان	بروز حوادث امنیتی در بانک‌ها	علل عمده حوادث امنیتی در بانک
۳	عدم به‌روزرسانی نرم‌افزارها		
۴	حملات فیشینگ		
۴	نفوذ بدافزارها		
۴	ضعف در احراز هویت		
۴	دسترسی غیرمجاز		
۳	خطای انسانی		
۳	کمبود نظارت امنیتی		
۳	استفاده از نرم‌افزارهای ناامن		
۳	ضعف در زیرساخت شبکه		
۲	حملات سایبری هدفمند		
۲	نقص در مدیریت رمز عبور		
۲	کمبود بودجه	موانع سازمانی، مالی و فناوری	موانع و نگرانی‌ها در اجرای انطباق امنیتی بهتر
۲	مقاومت کارکنان در برابر تغییرات		
۶	پیچیدگی‌های فناوری		
۶	فقدان استانداردهای یکپارچه		
۶	کمبود نیروی متخصص		
۳	نگرانی از نقض حریم خصوصی		
۵	عدم هماهنگی بین دپارتمان‌ها		
۳	زمان‌بر بودن فرایند انطباق		
۴	عدم آگاهی مدیران ارشد		
۴	نگرانی از هزینه‌های اضافی		
۴	عدم تطابق با قوانین محلی		
۴	مشکلات یکپارچه‌سازی سیستم‌ها		
۳	ترس از کاهش تجربه کاربری		
۳	پیاده‌سازی فایروال‌های پیشرفته	پیشگیری از تهدیدات امنیتی	استراتژی‌های امنیتی در شش ماه اخیر
۳	آموزش امنیت سایبری		
۳	استفاده از رمزنگاری پیشرفته		
۲	مانیتورینگ بلادرنگ		
۲	به‌روزرسانی پروتکل‌های امنیتی		
۲	اجرای تست نفوذ		
۲	استقرار سیستم‌های تشخیص نفوذ		
۶	تقویت احراز هویت چندمرحله‌ای		
۶	بازنگری سیاست‌های امنیتی		
۶	همکاری با شرکت‌های امنیتی		
۳	پیاده‌سازی استاندارد ISO 27001		
۵	تحلیل ریسک‌های امنیتی		
۳	رمزنگاری داده‌ها	فعالیت‌های عملی برای حفاظت از داده‌های بانکی	اقدامات امنیت داده‌ها
۴	پشتیبان‌گیری منظم		
۴	کنترل دسترسی کاربران		
۴	استفاده از VPN		
۴	نصب آنتی‌ویروس		
۳	رصد تراکنش‌ها		
۳	محدودکردن دسترسی به داده‌های حساس		

تکرار	کد استخراجی (کدباز)	کد استخراجی (کد محوری)	کد استخراجی (کد انتخابی)
۳	استفاده از امضای دیجیتال		
۳	پایش لاگ‌های سیستم		
۲	به‌روزرسانی سیستم‌عامل		
۲	اجرای پروتکل‌های SSL/TLS		
۲	مدیریت کلیدهای رمزنگاری		
۲	شناسایی دارایی‌های اطلاعاتی	فرایندهای چرخه‌ای برای مدیریت مستمر امنیت داده‌ها	چرخه امنیت داده‌ها
۶	ارزیابی ریسک		
۶	طراحی سیاست‌های امنیتی		
۶	پیاده‌سازی کنترل‌ها		
۳	نظارت مستمر		
۵	پاسخ به حوادث		
۳	بازنگری و بهبود		
۴	مستندسازی فرایندها		
۴	آموزش مستمر		
۴	تست و بازبینی سیستم‌ها		
۴	مدیریت تغییرات امنیتی		
۳	بازخورد از حوادث		
۳	تقویت آموزش‌های امنیتی	اقدامات پیشنهادی برای ارتقای سطح امنیت	اقدامات امنیتی اضافی لازم برای بهبود امنیت داده‌ها
۳	پیاده‌سازی هوش مصنوعی برای تشخیص تهدید		
۳	توسعه سیستم‌های پیش‌بینی حملات		
۲	افزایش بودجه امنیتی		
۲	استانداردسازی فرایندها		
۲	بهبود احراز هویت بیومتریک		
۲	توسعه تیم واکنش سریع		
۶	استفاده از بلاک‌چین		
۶	مانیتورینگ پیشرفته تهدیدات		
۶	تقویت همکاری‌های بین‌بانکی		
۳	بازنگری معماری شبکه		
۵	اجرای ممیزی‌های منظم		
۳	احراز هویت چندمرحله‌ای	مکانیسم‌های خاص برای حفاظت از خدمات برخط	مکانیسم‌های امنیت داده در خدمات بانکداری برخط
۴	رمزنگاری end-to-end		
۴	سیستم‌های تشخیص تقلب		
۴	محدودکردن دسترسی API		
۴	پایش تراکنش‌های برخط		
۳	استفاده از توکن‌های امنیتی		
۳	پروتکل‌های HTTPS		
۳	سیستم‌های تشخیص ناهنجاری		
۳	مدیریت نشست‌های کاربری		
۲	رمزنگاری پایگاه‌داده		
۲	محدودکردن دسترسی به سرورها		
۲	تست نفوذ برخط		
۲	تراکنش‌های برخط	خدمات تحت‌تأثیر مکانیسم‌های امنیتی	خدمات مالی تحت‌تأثیر مکانیسم‌های امنیت داده‌ها
۶	خدمات پرداخت موبایلی		
۶	وام‌های برخط		
۶	مدیریت حساب‌های دیجیتال		

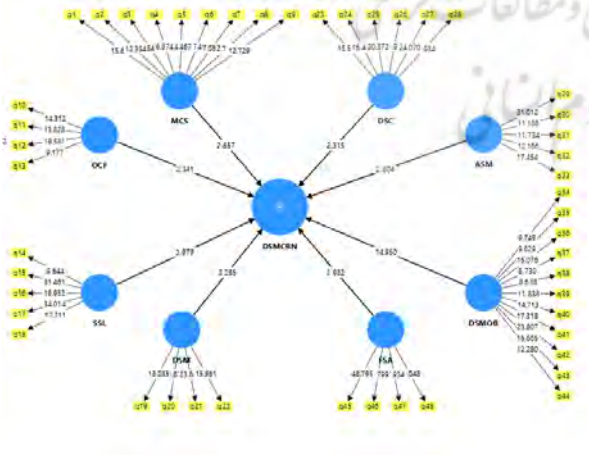
تکرار	کد استخراجی (کدباز)	کد استخراجی (کد محوری)	کد استخراجی (کد انتخابی)
۳	انتقال وجه بین‌بانکی		
۴	خدمات کارت اعتباری		
۴	پلتفرم‌های سرمایه‌گذاری		
۴	سیستم‌های مالی غیرمتمرکز		
۳	خدمات احراز هویت مشتری		
۳	مدیریت ریسک مالی		
۳	خدمات بانکداری باز		
۳	پلتفرم‌های تجارت الکترونیک		
۲	خدمات رمزنگاری شده مالی		
۲	خدمات مبتنی بر API		
۲	مدیریت تراکنش‌های بین‌المللی		

پس از استخراج کدهای مدنظر، به بخش کمی وارد شده و در این قسمت به جهت صحت روابط فرض شده از روش حداقل مربعات جزئی با استفاده از نرم‌افزار Smart PLS 4 استفاده گردید. پیش از ورود به بررسی متغیرها، مخفف متغیرهای پژوهش به شرح جدول ۴ است.

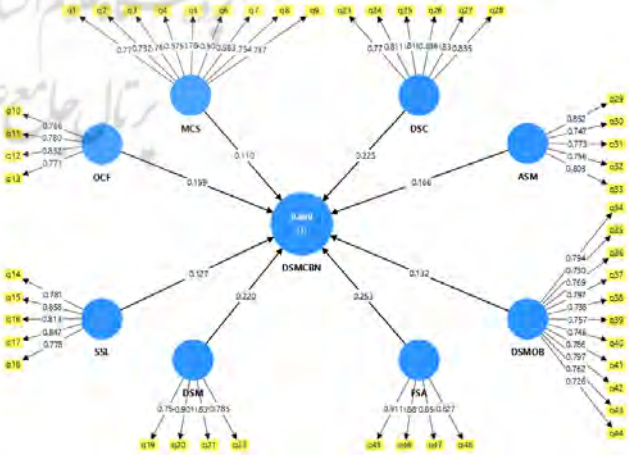
جدول ۴. مخفف متغیرهای پژوهش

ردیف	مؤلفه	مخفف
۱	علل عمده حوادث امنیتی در بانک	MCS
۲	موانع و نگرانی‌ها در اجرای انطباق امنیتی بهتر	OCF
۳	استراتژی‌های امنیتی در شش ماه اخیر	SSL
۴	اقدامات امنیت داده‌ها	DSM
۵	چرخه امنیت داده‌ها	DSC
۶	اقدامات امنیتی اضافی لازم برای بهبود امنیت داده‌ها (نحوه آمادگی امنیت داده‌ها)	ASM
۷	مکانیسم‌های امنیت داده در خدمات بانکداری برخط	DSMOB
۸	خدمات مالی تحت‌تأثیر مکانیسم‌های امنیت داده‌ها	FSA
۹	مدیریت امنیت داده در شبکه بانکی کشور	DSMCBN

در شکل ۱ و ۲ به بررسی مدل پژوهش پرداخته می‌شود.



شکل ۳ آزمون مدل (آماره تی)



شکل ۲ آزمون مدل (ضریب مسیر استاندارد)

پیش از ورود به بررسی شکل‌های ۲ و ۳ برخی از بررسی استانداردهای مدل و شاخص‌های برازش مدل مورد بررسی قرار گرفته است. پژوهشگران معتقدند که یک متغیر مکنون باید بخش قابل‌توجهی از پراکندگی هر معرف را توضیح دهد (معمولاً ۷۰ درصد). بنابراین، قدر مطلق همبستگی بین یک سازه و هر کدام از متغیرهای مشاهده شده آن یعنی قدر مطلق بارهای خروجی

استاندارد شده باید بیشتر از ۰/۷ باشد. به عبارت دیگر، هر معرف باید دارای بار عاملی بیشتر از ۰/۵ بر روی متغیر مربوط به خود باشد (موذن جمشیدی و خانی، ۲۰۱۳). جدول ۶ مقادیر بارهای عاملی و به عبارت دیگر، مقادیر وزن بارهای عاملی را نشان می‌دهد. همان‌طور که مشاهده می‌شود تمامی سؤالات بر روی متغیرهای خود دارای بار عاملی بزرگ‌تر از ۰/۷ هستند که نشان دهندهٔ مناسب بودن سؤالات به جهت تخمین متغیر مربوطه است. لازم به ذکر است پیش از ورود به بررسی متغیرها، مخفف متغیرهای پژوهش به شرح جدول ۵ است.

جدول ۵. مخفف متغیرهای پژوهش

ردیف	مؤلفه	مخفف
۱	علل عمده حوادث امنیتی در بانک	MCS
۲	موانع و نگرانی‌ها در اجرای انطباق امنیتی بهتر	OCF
۳	استراتژی‌های امنیتی در شش ماه اخیر	SSL
۴	اقدامات امنیت داده‌ها	DSM
۵	چرخه امنیت داده‌ها	DSC
۶	اقدامات امنیتی اضافی لازم برای بهبود امنیت داده‌ها (نحوه آمادگی امنیت داده‌ها)	ASM
۷	مکانیسم‌های امنیت داده در خدمات بانکداری برخط	DSMOB
۸	خدمات مالی تحت‌تأثیر مکانیسم‌های امنیت داده‌ها	FSA
۹	مدیریت امنیت داده در شبکه بانکی کشور	DSMCBN

جدول ۶. آزمون بارهای عاملی

مؤلفه‌ها	گویه	بارعاملی	AVE
MCS	۱Q	۰/۷۷۷	۰/۷۶۷
	۲Q	۰/۷۳۲	
	۳Q	۰/۷۴۶	
	۴Q	۰/۷۷۵	
	۵Q	۰/۷۸۴	
	۶Q	۰/۷۰۳	
	۷Q	۰/۷۸۳	
	۸Q	۰/۷۵۴	
	۹Q	۰/۷۳۷	
OCF	۱۰Q	۰/۷۶۶	۰/۶۲۱
	۱۱Q	۰/۷۸۰	
	۱۲Q	۰/۸۳۲	
	۱۳Q	۰/۷۷۱	
SSL	۱۴Q	۰/۷۸۱	۰/۶۳۷
	۱۵Q	۰/۸۵۸	
	۱۶Q	۰/۸۱۳	
	۱۷Q	۰/۸۴۷	
	۱۸Q	۰/۷۷۸	
DSM	۱۹Q	۰/۷۵۴	۰/۶۷۵
	۲۰Q	۰/۹۰۱	
	۲۱Q	۰/۸۳۹	
	۲۲Q	۰/۷۸۵	
DSC	۲۳Q	۰/۷۷۵	۰/۶۷۰
	۲۴Q	۰/۸۱۱	
	۲۵Q	۰/۸۱۶	
	۲۶Q	۰/۸۳۶	
	۲۷Q	۰/۸۳۵	
	۲۸Q	۰/۸۳۵	
ASM	۲۹Q	۰/۸۵۲	۰/۵۹۱

مؤلفه‌ها	گویه	بارعاملی	AVE
	۳۰Q	۰/۷۴۷	
	۳۱Q	۰/۷۷۳	
	۳۲Q	۰/۷۵۶	
	۳۳Q	۰/۸۰۳	
DSMOB	۳۴Q	۰/۷۹۴	۰/۵۲۰
	۳۵Q	۰/۷۳۰	
	۳۶Q	۰/۷۶۹	
	۳۷Q	۰/۷۹۷	
	۳۸Q	۰/۷۳۸	
	۳۹Q	۰/۷۵۷	
	۴۰Q	۰/۷۴۶	
	۴۱Q	۰/۷۸۶	
	۴۲Q	۰/۷۹۷	
	۴۳Q	۰/۷۶۲	
	۴۴Q	۰/۷۲۶	
FSA	۴۵Q	۰/۹۱۱	۰/۷۵۳
	۴۶Q	۰/۸۸۱	
	۴۷Q	۰/۸۵۰	
	۴۸Q	۰/۸۲۷	

همچنین در جدول ۶ روایی همگرا در ستون AVE استخراج شده است؛ به این معناست که آیا دو ابزاری را که مفهوم را اندازه‌گیری می‌کنند از همبستگی بالایی برخوردارند؟ به جهت بررسی روایی همگرا فورنل و لارکر (۱۹۸۱) متوسط واریانس استخراج شده AVE را به عنوان معیاری برای اعتبار همگرا پیشنهاد می‌کنند. حداقل مقدار AVE برابر با ۰/۵ بیانگر اعتبار همگرای کافی است، به این معنا که یک متغیر مکنون می‌تواند به طور میانگین بیش از نیمی از پراکندگی معرف‌هایش را تبیین کند (موذن جمشیدی و خانی، ۲۰۱۳). همان‌طور که در جدول مشاهده می‌شود کلیه مقادیر AVE برای تمام متغیرهای پژوهش بزرگ‌تر از ۰/۵ است. با توجه به مقادیر نشان داد شده می‌توان گفت که مدل از روایی همگرای مطلوبی برخوردار است. منظور از روایی واگرا این است که آیتم‌ها یا معرف‌های مربوط به یک متغیر فقط همان متغیر را بسنجد. در تحلیل PLS براساس نظر فورنل و لارکر (۱۹۸۱) جذر AVE یک متغیر باید از میزان همبستگی آن متغیر با سایر متغیرهای پژوهش بزرگ‌تر باشد. در این مرحله ابتدا جذر مقادیر AVE را محاسبه نموده و سپس مقادیر به دست آمده را بر روی قطر ماتریس (همبستگی) متغیر مکنون جایگزین می‌نماییم (موذن جمشیدی و خانی، ۲۰۱۳). در جدول همبستگی متغیرها با یکدیگر همان‌طور که مشاهده می‌گردد، مقادیر جذر AVE قرار گرفته بر روی قطر ماتریس همبستگی از مقادیر همبستگی آن متغیر با سایر متغیرها بزرگ‌تر است که نشان‌دهنده مناسب بودن روایی واگرای مدل اندازه گیری می‌باشد.

جدول ۷. میزان همبستگی بین متغیرها و جذر متوسط واریانس استخراج شده فورنل و لارکر

مؤلفه‌ها	ASM	DSC	DSM	DSMCBN	DSMOB	FSA	MCS	OCF	SSL
ASM	۰/۹۹۸								
DSC	۰/۹۹۲	۰/۹۸۸							
DSM	۰/۹۸۴	۰/۹۷۵	۰/۹۶۲						
DSMCBN	۰/۹۳۱	۰/۹۳۰	۰/۹۲۴	۰/۸۹۲					
DSMOB	۰/۹۲۶	۰/۹۲۱	۰/۹۱۱	۰/۸۸۴	۰/۸۸۱				
FSA	۰/۹۱۶	۰/۹۰۹	۰/۸۹۹	۰/۸۷۶	۰/۸۶۹	۰/۸۶۸			
MCS	۰/۹۰۹	۰/۹۰۲	۰/۸۹۱	۰/۸۶۴	۰/۸۶۱	۰/۸۵۰	۰/۷۸۳		
OCF	۰/۸۹۳	۰/۸۹۲	۰/۸۸۶	۰/۸۳۷	۰/۸۱۹	۰/۸۱۰	۰/۷۷۵	۰/۷۵۸	
SSL	۰/۸۹۰	۰/۸۸۹	۰/۸۸۰	۰/۸۳۱	۰/۸۱۲	۰/۷۹۳	۰/۷۴۷	۰/۷۲۸	۰/۷۱۱

حد مناسب شاخص HTMT برابر با ۰/۹ است. اگر اعداد موجود در ماتریس شاخص HTMT از ۰/۹ کمتر باشند، بیانگر این است که روایی واگرایی ابزار مناسب است (هایر و همکاران، ۲۰۱۷). در جدول ۸ تمامی مقادیر زیر ۰/۹ است؛ پس روایی واگرایی ابزار تایید شده است.

جدول ۸. میزان همبستگی بین متغیرها و جذر متوسط واریانس استخراج شده(HTMT)

مؤلفه‌ها	مدیریت امنیت داده در شبکه بانکی کشور
مدیریت امنیت داده در شبکه بانکی کشور	۰/۶۴۳

شاخص Q^2 مثبت و بزرگ، نشان از قابلیت بالای پیش‌بینی مدل دارد و مقادیر Q2 منفی بیانگر تخمین بسیار ضعیف متغیر پنهان است. با توجه به بررسی صورت گرفته مقادیر Q2 در جدول ۹ بالا و مثبت بوده است، پس، تخمین متغیر پنهان مطلوب است.

جدول ۹. شاخص‌های(Q2)

مؤلفه‌ها	Q^2
ASM	۰/۶۵۶
DSC	۰/۳۱۱
DSM	۰/۳۴۷
DSMOB	۰/۵۶۳
FSA	۰/۳۷۸
MCS	۰/۵۸۳
OCF	۰/۵۶۴
SSL	۰/۳۶۱

R2 معیاری است که برای متصل‌کردن بخش اندازه‌گیری و بخش ساختاری مدل‌سازی معادلات ساختاری بکار می‌رود و نشان از تأثیری دارد که یک متغیر برون‌زا بر یک متغیر درون‌زا می‌گذارد که بر اساس شکل ۲، مقدار R2 برای متغیر وابسته ۰/۸۸۰ گزارش گردید که مطلوب است. برای اثر در مدل مسیری می‌توان اندازه اثر را با استفاده از f square کوهن ارزیابی کرد. اندازه اثر f2 به صورت نسبتی از تغییرات هر R2به روی بخشی از واریانس متغیر مکنون درونزا است که به صورت تبیین نشده در مدل باقی می‌ماند. طبق نظر کوهن مقادیر ۰/۰۲، ۰/۱۵ و ۰/۳۵برای f2به ترتیب بیانگر اثر کوچک، متوسط و بزرگ است.

جدول ۱۰. شاخص‌های(F2)

مؤلفه‌ها			F^2
ASM	<--	مدیریت امنیت داده در شبکه بانکی کشور (DSMCBN)	۰/۰۶۴
DSC			۰/۸۰۲
DSM			۰/۳۰۱
DSMOB			۱/۸۰۲
FSA			۰/۰۷۰
MCS			۰/۰۳۷
OCF			۰/۰۸۳
SSL			۰/۰۵۱

با توجه به مقادری گزارش شده از جدول ۱۰ می‌توان اظهار اثر متغیرهای مکنون درون‌زا بزرگ است. معیار GOF نیز محقق می‌تواند پس از بررسی برازش بخش اندازه‌گیری و بخش ساختاری مدل کلی پژوهش خود، برازش بخش کلی را نیز کنترل نماید. با توجه به این که سه مقدار ۰/۱، ۰/۲۵ و ۰/۳۶ به عنوان مقادیر حاکی از برازش مناسب ضعیف، متوسط و قوی معرفی

شده‌اند (وتزلس و همکاران، ۲۰۰۹)، حصول مقدار مدل حاضر برابر با ۰/۷۶۴ است که نشان از برازش مناسب مدل کلی پژوهش است. شاخص ریشه میانگین مربعات باقیمانده[1] به معنای ریشه میانگین مجذور باقیمانده با استفاده از فرمول $\sqrt{R2\text{-}1}$ محاسبه می‌شود. هرچه این معیار به صفر نزدیک‌تر باشد نیکوئی برازش مدل‌بالاتر است. شاخص ریشه میانگین مربعات باقیمانده استانداردشده SRMR در مطالعات جدیدتر پیشنهاد گردید. اگر مقدار این شاخص کمتر از ۰/۰۸ باشد مناسب است (هنسلر و سارستد، ۲۰۱۳)، همان‌طور که در جدول زیر مشاهده می‌شود این مقدار کمتر از ۰/۰۸ بوده و موردتأیید است و شاخص NFI[2] که شاخص بنتلر–بونت[3] هم نامیده می‌شود برای مقادیر بالای ۰/۹ قابل‌قبول و نشانه برازندگی مدل است. همان‌طور که در جدول ۱۱ مشاهده می‌شود این مقدار بیش از ۰/۹ بوده و موردتأیید است.

جدول ۱۱مقادیر SRMR وNFI

شاخص‌ها	مقادیر
SRMR	۰/۰۷۳
NFI	۱/۲۳۸

برای بررسی فرض‌های ایجاد شده، روابط بین متغیر وابسته و متغیرهای مستقل در مدل موردبررسی قرار گرفت. همان‌طور که در جدول ۱۲ مشاهده می‌شود.

جدول ۱۲. بررسی فرض‌های پژوهش

فرضیه			ضریب مسیر استاندارد	آماره t	سطح معناداری	نتیجه
علل عمده حوادث امنیتی در بانک	مدیریت امنیت داده در شبکه بانکی کشور	<--	۰/۱۱۰	۲/۵۸۷	P<۰/۰۵	تأیید
موانع و نگرانی‌ها در اجرای انطباق امنیتی بهتر			۰/۱۵۹	۲/۳۴۱	P<۰/۰۵	تأیید
استراتژی‌های امنیتی در شش ماه اخیر			۰/۱۲۷	۲/۹۷۹	P<۰/۰۵	تأیید
داده‌ها امنیت اقدامات			۰/۲۲۰	۲/۲۸۵	P<۰/۰۵	تأیید
چرخه امنیت داده‌ها			۰/۲۲۵	۲/۳۱۵	P<۰/۰۵	تأیید
اقدامات امنیتی اضافی لازم برای بهبود امنیت داده‌ها			۰/۱۶۶	۲/۸۰۴	P<۰/۰۵	تأیید
برخط بانکداری خدمات در داده امنیت مکانیسم‌های			۰/۱۳۲	۱۴/۵۵۰	P<۰/۰۵	تأیید
داده‌ها امنیت مکانیسم‌های تحت‌تأثیر مالی خدمات			۰/۲۵۳	۲/۹۸۲	P<۰/۰۵	تایید

بحث و نتیجه‌گیری

نتایج این مطالعه با یافته‌های پژوهشگرانی نظیر آزاد سنجری و چهارسوقی (۱۴۰۳)، وجدانی (۱۴۰۳)، دروی و جمشیدی (۱۴۰۰)، لی و همکاران (۲۰۲۱)، کیمیاگری و بائی (۲۰۲۱)، کیریلو و همکاران (۲۰۲۱)، خروشچ و همکاران (۲۰۲۰)، و اسچالز و همکاران (۲۰۲۰) هم‌خوانی دارد. این هم‌راستایی نشان‌دهنده وجود الگوهای مشترک در ضعف‌های امنیتی سیستم‌های فناوری اطلاعات در شبکه‌های بانکی است.

حوادث امنیتی در شبکه بانکی اغلب از ضعف‌های مشترک مانند نرم‌افزارهای قدیمی، پیکربندی نادرست، و عدم به‌روزرسانی‌های امنیتی ناشی می‌شوند. این ضعف‌ها، به دلیل استفاده بانک‌ها از فناوری‌ها و پروتکل‌های مشابه، می‌توانند به کل شبکه تسری یابند. حملات سایبری نظیر فیشینگ، باج‌افزارها و نفوذ به سیستم‌ها، نشان‌دهنده تکامل تهدیدات سایبری هستند که اعتماد مشتریان به نظام بانکی را کاهش داده و ضرورت بازنگری سیاست‌های امنیتی را برجسته می‌کنند. یک حادثه امنیتی در یک بانک می‌تواند به عنوان نقطه ورود برای حملات به سایر بانک‌ها عمل کرده و کل شبکه را در معرض خطر قرار دهد. مدیریت یکپارچه امنیت داده‌ها در شبکه بانکی نیازمند هماهنگی بین‌بانکی و اجرای استانداردهای امنیتی سخت‌گیرانه‌تر، مانند ISO 27001 و PCI DSS، است. نهادهای نظارتی، از جمله بانک مرکزی، با وضع مقررات جدید، بانک‌ها را به بهبود فرایندهای

[1]. Root Mean Square Residual
[2]. Normed Fit Index
[3]. Bentler-Bonett

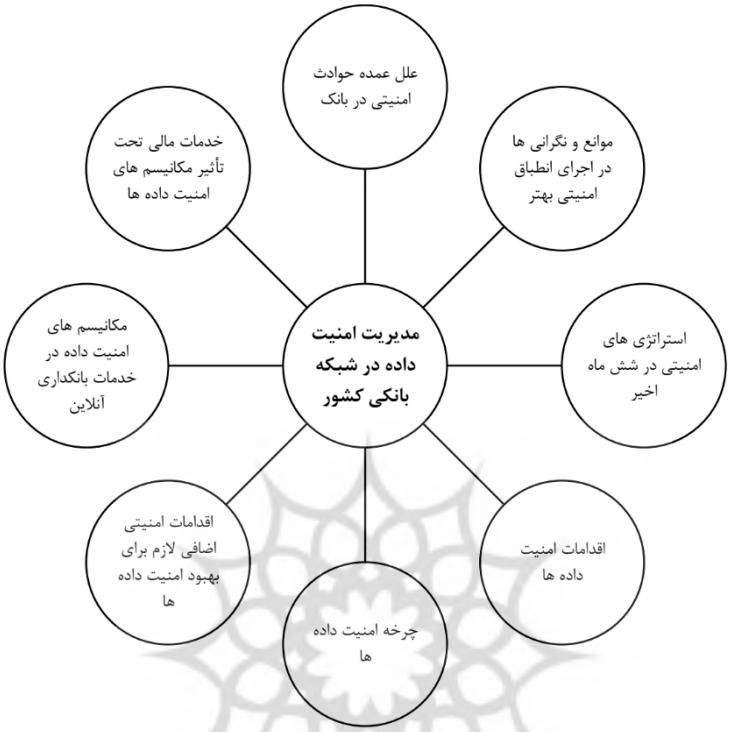
امنیتی ملزم می‌کنند. همکاری بین بانک‌ها برای اشتراک‌گذاری اطلاعات تهدیدات و راهکارهای امنیتی، به کاهش نقاط ضعف مشترک و تقویت مدیریت امنیت داده‌ها کمک می‌کند. اجرای سیاست‌های امنیتی یکپارچه با چالش‌هایی مواجه است، از جمله: (محدودیت‌های مالی (کمبود بودجه برای سرمایه‌گذاری در فناوری‌های جدید و به‌روزرسانی زیرساخت‌ها)، ناسازگاری زیرساختی (ناهمخوانی زیرساخت‌های قدیمی با استانداردهای امنیتی مدرن)، مقاومت سازمانی (عدم آگاهی یا مقاومت کارکنان و مدیران در برابر تغییرات)، ناهمگونی بانک‌ها (تفاوت در سطوح فناوری و منابع بانک‌ها، که هماهنگی را دشوار می‌کند)، تداخل با قوانین حریم خصوصی (پیچیدگی‌های ناشی از انطباق با مقررات محلی و بین‌المللی)). این موانع می‌توانند اعتماد بین بانک‌ها و نهادهای نظارتی را کاهش داده و همکاری لازم برای مدیریت امنیت داده‌ها را تضعیف کنند.

در شش ماه گذشته، تهدیدات سایبری مانند باج‌افزارها و فیشینگ پیشرفته‌تر شده‌اند. استراتژی‌های جدید، از جمله استفاده از هوش مصنوعی برای تشخیص تهدیدات، رمزنگاری پیشرفته، فایروال‌های مدرن، و سیستم‌های تشخیص نفوذ، به بهبود امنیت داده‌ها کمک کرده‌اند. این استراتژی‌ها بر هماهنگی بین‌بانکی، آموزش کارکنان، و انطباق با مقررات جدید تأکید دارند. به‌روزرسانی زیرساخت‌ها و اجرای برنامه‌های آموزشی برای کاهش خطاهای انسانی، به استانداردسازی و کارآمدی مدیریت امنیت داده‌ها در شبکه بانکی منجر شده است. این اقدامات، با افزایش اعتماد مشتریان و کاهش نقاط ضعف، شبکه بانکی را در برابر تهدیدات آینده مقاوم‌تر می‌کنند. از سویی اقدامات کلیدی برای بهبود مدیریت امنیت داده‌ها می‌توانند شامل (فناوری‌های پیشرفته (پیاده‌سازی رمزنگاری end-to-end، احراز هویت چندمرحله‌ای (MFA) و سیستم‌های تشخیص تقلب مبتنی بر هوش مصنوعی)، آموزش و سیاست‌های دسترسی (آموزش مستمر کارکنان و اجرای سیاست‌های دسترسی محدود برای کاهش خطاهای انسانی)، اشتراک‌گذاری اطلاعات (تبادل اطلاعات تهدیدات و بهترین روش‌ها بین بانک‌ها برای پیشگیری از حوادث)، انطباق با استانداردها (تطبیق با مقررات داخلی و بین‌المللی برای استانداردسازی فرایندهای امنیتی)، به‌روزرسانی زیرساخت‌ها (ارتقای سیستم‌ها برای مقابله با تهدیدات نوظهور)؛ این اقدامات با کاهش ریسک نقض داده‌ها، اعتماد مشتریان و شرکای تجاری را تقویت کرده و مدیریت امنیت داده‌ها را به اولویت استراتژیک شبکه بانکی تبدیل می‌کنند. چرخه امنیت داده‌ها در پنج مرحله کلیدی (شناسایی داده‌های حساس و دارایی‌های بحرانی برای هدف‌گذاری دقیق‌تر سیاست‌های امنیتی؛ استفاده از رمزنگاری، کنترل دسترسی، و به‌روزرسانی سیستم‌ها برای کاهش ریسک نقض داده‌ها؛ بهره‌گیری از سیستم‌های نظارتی و تحلیل داده برای شناسایی زودهنگام تهدیدات؛ اجرای پروتکل‌های مدیریت حوادث برای محدودسازی آسیب‌ها و هماهنگی بین‌بانکی؛ بازسازی سیستم‌ها پس از حوادث و یادگیری از تجربیات برای بهبود سیاست‌های امنیتی) باشد. این چرخه با ارائه چارچوبی ساختاریافته، همکاری و انطباق با مقررات را تسهیل کرده و مدیریت امنیت داده‌ها را کارآمدتر می‌کند.

خدمات بانکداری برخط و مالی، به دلیل حساسیت داده‌های تراکنش‌ها، هدف اصلی حملات سایبری هستند. مکانیسم‌های امنیتی مانند رمزنگاری end-to-end، احراز هویت چندمرحله‌ای، پروتکل‌های امن (مانند HTTPS)، و سیستم‌های تشخیص تقلب مبتنی بر هوش مصنوعی، از داده‌های مشتریان محافظت می‌کنند. این مکانیسم‌ها، با استانداردسازی امنیت در تبادل داده‌ها و انطباق با مقررات (مانند PCI DSS)، مدیریت یکپارچه امنیت داده‌ها را تقویت می‌کنند. نظارت بلادرنگ و تحلیل رفتار کاربران، تهدیدات نوظهور را خنثی کرده و اعتماد مشتریان را افزایش می‌دهد. این اقدامات، با کاهش خسارات ناشی از نقض داده‌ها و کلاهبرداری، انگیزه بانک‌ها برای سرمایه‌گذاری در امنیت داده‌ها را تقویت می‌کنند. برای مقابله با تهدیدات پیشرفته مانند حملات صفر – روز و بدافزارهای پیچیده، اقدامات تکمیلی نظیر تست نفوذ منظم، به‌روزرسانی زیرساخت‌های قدیمی، و پیاده‌سازی استانداردهای جدید (مانند GDPR) ضروری است. این اقدامات، همراه با پروتکل‌های مشترک برای اشتراک‌گذاری اطلاعات تهدیدات و شبیه‌سازی حملات سایبری، آمادگی بانک‌ها را برای مدیریت بحران‌ها افزایش داده و ریسک‌های عملیاتی را کاهش می‌دهند. این تلاش‌ها، با تقویت هماهنگی و انطباق با مقررات، مدیریت امنیت داده‌ها را در شبکه بانکی یکپارچه‌تر و مؤثرتر می‌کنند.

در نهایت مدیریت مؤثر امنیت داده‌ها در شبکه بانکی نیازمند رویکردی یکپارچه، هماهنگ و پویاست. رفع موانع مالی، فنی، و سازمانی، همراه با سرمایه‌گذاری در فناوری‌های نوین، آموزش کارکنان، و انطباق با استانداردهای بین‌المللی، برای ایجاد

اکوسیستم بانکی امن و پایدار ضروری است. چرخه امنیت داده‌ها، استراتژی‌های نوین، و مکانیسم‌های پیشرفته در خدمات مالی و بانکداری برخط، با کاهش ریسک‌ها، افزایش اعتماد، و تقویت همکاری بین‌بانکی، شبکه بانکی را در برابر تهدیدات سایبری مقاوم‌تر می‌کنند. این اقدامات، با تثبیت مدیریت امنیت داده‌ها به عنوان اولویت استراتژیک، به پایداری و اعتبار نظام بانکی کشور کمک می‌کنند. با توجه به یافته‌ها مدل نهایی پژوهش حاضر به شرح شکل ۴ است.



شکل ۴. طراحی مدل جامع مدیریت امنیت داده در شبکه بانکی کشور

در نهایت برای هر یک از مؤلفه‌های ارائه‌شده از یافته‌های پژوهشی حاضر در طراحی مدل جامع مدیریت امنیت داده در شبکه بانکی کشور، پیشنهاد کاربردی ارائه شده است. این پیشنهادات باهدف تقویت مدیریت امنیت داده، عملی و قابل‌اجرا در شبکه بانکی کشور طراحی شده‌اند که عبارت‌اند از:

- پیاده‌سازی برنامه‌های آموزشی منظم: برگزاری دوره‌های آموزشی مداوم برای کارکنان بانک‌ها در مورد شناسایی حملات فیشینگ، مدیریت رمزهای عبور قوی و رعایت پروتکل‌های امنیتی برای کاهش خطاهای انسانی که یکی از علل اصلی حوادث امنیتی است.
- انجام تست‌های نفوذ دوره‌ای: اجرای تست‌های نفوذ سالیانه برای شناسایی نقاط ضعف زیرساختی و نرم‌افزاری در سیستم‌های بانکی، با تمرکز بر نرم‌افزارهای قدیمی و پیکربندی‌های نادرست.
- استقرار سیستم‌های نظارت بلادرنگ: استفاده از ابزارهای نظارتی مبتنی بر هوش مصنوعی برای تشخیص زودهنگام فعالیت‌های مشکوک و جلوگیری از گسترش حوادث امنیتی در شبکه بانکی.
- تخصیص بودجه هدفمند: ایجاد برنامه‌های مالی برای تأمین منابع موردنیاز جهت به‌روزرسانی زیرساخت‌ها و انطباق با استانداردهای امنیتی، با همکاری نهادهای نظارتی مانند بانک مرکزی.
- تشکیل کمیته‌های هماهنگی بین‌بانکی: راه‌اندازی کمیته‌های مشترک برای تبادل تجربیات و راهکارهای غلبه بر موانع فنی و سازمانی در اجرای انطباق امنیتی.
- آموزش و فرهنگ‌سازی سازمانی: برگزاری کارگاه‌های آگاهی‌بخشی برای مدیران و کارکنان به‌منظور کاهش مقاومت در برابر تغییرات و پذیرش سیاست‌های جدید امنیتی.

- توسعه پروتکل‌های اشتراک‌گذاری تهدیدات: ایجاد یک پلتفرم مشترک برای به‌اشتراک‌گذاری اطلاعات تهدیدات سایبری بین بانک‌ها به‌منظور واکنش سریع‌تر به حملات جدید.
- به‌روزرسانی زیرساخت‌های امنیتی: سرمایه‌گذاری در فایروال‌های نسل جدید و سیستم‌های تشخیص نفوذ برای تقویت دفاع در برابر تهدیدات سایبری نوظهور.
- اجرای برنامه‌های شبیه‌سازی حمله: برگزاری تمرین‌های منظم شبیه‌سازی حملات سایبری برای ارزیابی اثربخشی استراتژی‌های امنیتی و بهبود آمادگی شبکه بانکی.
- پیاده‌سازی احراز هویت بیومتریک: استفاده از فناوری‌های بیومتریک مانند تشخیص اثر انگشت یا چهره برای افزایش امنیت ورود به سیستم‌های بانکداری برخط.
- نظارت بلادرنگ تراکنش‌ها: استقرار سیستم‌های تحلیل رفتار کاربر برای شناسایی تراکنش‌های مشکوک در بانکداری برخط و جلوگیری از کلاهبرداری.
- آموزش مشتریان: ارائه راهنماهای ساده و ویدئوهای آموزشی به مشتریان برای آگاهی از روش‌های ایمن استفاده از خدمات بانکداری برخط و جلوگیری از فیشینگ.
- استقرار پروتکل‌های امن پرداخت: استفاده از استانداردهای امن مانند D-Secure۳ برای تراکنش‌های برخط به‌منظور کاهش ریسک کلاهبرداری در خدمات مالی.
- توسعه سیستم‌های تشخیص تقلب: پیاده‌سازی ابزارهای مبتنی بر یادگیری ماشین برای شناسایی الگوهای غیرعادی در تراکنش‌های خدمات مالی، مانند وام‌ها یا پرداخت‌های بین‌بانکی.
- ایجاد درگاه‌های امن API: طراحی APIهای امن با پروتکل‌های OAuth 2.0 برای تبادل داده بین خدمات مالی بانک‌ها، باهدف افزایش امنیت و هماهنگی در شبکه بانکی.

ملاحظات اخلاقی

پیروی از اصول اخلاق پژوهش

نویسندگان اصول اخلاقی را در انجام و انتشار این پژوهش علمی رعایت نموده‌اند و این موضوع مورد تأیید همه آنهاست.

مشارکت نویسندگان

نویسنده اول: تهیه و آماده‌سازی طرح اولیه تحقیق، انجام تحقیق و گردآوری داده‌ها، تجزیه و تحلیل آماری داده‌ها، تحلیل و تفسیر اطلاعات و نتایج، تهیه پیشنویس مقاله

نویسنده دوم: استاد راهنمای پایان‌نامه، طراحی پژوهش، نظارت بر مراحل انجام پژوهش، بررسی و کنترل نتایج، اصلاح، بازبینی و نهایی‌سازی مقاله.

تعارض منافع

بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

حامی مالی

مقاله حاضر با حمایت مالی معاونت پژوهشی دانشگاه تهران انجام شد.

سپاسگزاری

از مشارکت‌کنندگان در پژوهش تشکر و قدردانی می‌شود.

منابع

آزاد سنجری، سمیرا، و چهارسوقی، سیدکمال (۱۴۰۳). نوآوری‌ها و توسعه امنیت سایبری در بانک‌های ایران: تحلیل SWOT و مقایسه فرصت‌ها. *دومین کنفرانس مهندسی و مدیریت فرایندهای سازمانی*. تهران، ایران.

احمدی، سعید (۱۴۰۲). تهدیدات سایبری در شبکه‌های هوشمند: مطالعه موردی اینترنت اشیا و رایانش ابری. *کنفرانس بین‌المللی امنیت سایبری* (صص ۱۱۲–۱۲۵). تهران، ایران.

درودی، فریبرز، و جمشیدی، زینب (۱۴۰۰). سنجش مؤلفه‌های امنیت اطلاعات در دسترسی و استفاده از کتابخانه‌های دیجیتال. پژوهشنامه پردازش و مدیریت اطلاعات، ۳۷(۱)، ۱۱۷–۱۳۴. https://doi.org/10.52547/jipm.37.1.117

رضوانی، شهلا (۱۳۹۷). طراحی الگوی مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی. *پژوهشنامه کتابداری و اطلاع‌رسانی (مطالعات تربیتی و روان‌شناسی)*، ۸(۱، پیاپی ۱۵)، ۳۳۷–۳۵۶. https://doi.org/10.22067/riis.v0i0.61486

عزیزی سرخانی، محمد جواد، کردلوئی، حمیدرضا (۱۳۹۵). بررسی ابزارهای امنیتی بانکداری الکترونیک در بخش بانکداری دولتی بانک‌های هند با مروری بر جهانی‌شدن. *دانش سرمایه‌گذاری*، ۵(۱۸)، ۲۵۳–۲۶۲. http://www.jik-ifea.ir/article_8630.html

مغنی، حیدر؛ ناصحی‌فر، وحید، و ناطق، تهمینه (۱۳۹۸). چگونگی تأثیر گسترش فناوری‌های مالی بر بهبود عملکرد خدمات مالی. *اقتصاد مالی*، ۱۳(۴۹)، ۱۸۳–۲۱۲.

نوده فراهانی، ساناز؛ جباری، حسین، و پناهیان، حسین (۱۴۰۰). ارائه مدل مفهومی مؤلفه‌ها و شاخص‌های سرمایه انسانی مؤثر بر امنیت اطلاعات سازمان‌ها. *فصلنامه پژوهش‌های حفاظتی و امنیتی*، ۶(۹)، ۱۴۷–۱۷۰.

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*.

References

Acquisti, A., & Grossklags, J. (2023). Privacy in the digital age: A social perspective. *Journal of Privacy and Confidentiality*. *MIS Quarterly*, *35*(4), 1017-1041. https://doi.org/10.2307/41409971

Ahmadi, S. (2014). Cyber threats in smart grids: A case study of internet of things and cloud computing. *International Conference on Cyber Security* (pp. 112–125). Tehran, Iran. (in Persian)

Azad Sanjari, S., and Chaharsouki, K. (2014). Innovations and development of cybersecurity in Iranian banks: SWOT analysis and comparison of opportunities. Second Conference on *Organizational Process Engineering and Management*. Tehran, Iran. (in Persian)

Azizi Sorkhani, M.J., & Kordloui, H. (2016). A study of electronic banking security tools in the public banking sector of Indian banks with a review of globalization. *Investment Knowledge*, 5(18), 253–262. (in Persian)

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, 92, 101747.

Doroudi, F. , & Jamshidi,Z. (2021). Assessing the components of information security in accessing & use of digital libraries. *Iranian Journal of Information Processing and Management*, *37*(1), 117-134. https://doi.org/10.52547/jipm.37.1.117 (in Persian)

Floridi, L., & Taddeo, M. (2024). Data ethics: A framework for responsible data use. *Ethics and Information Technology*.

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. *Authorea Preprints*.

Kalyan, M. (2023). Data lifecycle management: Understanding stages and best practices. Solix. https://www.solix.com/fa/blog/data-lifecycle-management-understanding-stages-best-practices/

Khrushch, N., Hryhoruk, P., Hovorushchenko, T., Lysenko, S., Prystupa, L., & Vahanova, L. (2020). Assessment of bank's financial security levels based on a comprehensive index using information technology. *In M3E2-mlPEED* (pp. 239–260).

Kimiagari, S., & Baei, F. (2021). Promoting e-banking actual usage: Mix of technology acceptance model and technology-organisation-environment framework. *Enterprise Information Systems*, *16*(8-9), 1894356.

Kurylo, M. P., Klochko, A. M., Volchenko, N. V., Klietsova, N. V., & Bolotina, A. O. (2021). *The use of biometric technologies for bank transaction security management against the background of the international experience: Evidence from Ukraine.*

Li, F., Lu, H., Hou, M., Cui, K., & Darbandi, M. (2021). Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. *Technology in Society*, 64, 101487.

Mousavi, S. H., Nabiollahi, A., & Khani, N. (2023). *Systematic literature review on data governance*. In Seventh National Conference on Enterprise Architecture Progress.

Mughni, H., Nasehifar, V., & Nateg, T. (2019). How the expansion of financial technologies affects the improvement of financial services performance. *Financial Economics*, *13*(49), 183–212. (in Persian)

Nodeh Farahani, S., Jabbari, H., & Panahian, H. (2019). Presenting a conceptual model of human capital components and indicators affecting information security of organizations. *Journal of Security and Protection Research*, 6(9), 147–170.(in Persian)

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jalswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of Scientific Research and Management*, 9(12), 669–710.

Rezvani, S. (2018). Designing an information security management model in digital libraries. *Library and Information Science Research*, *8*(1), 337-356. https://doi.org/10.22067/riis.v0i0.61486 (in Persian)

Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics*, *9*(2), 107–118. https://doi.org/10.1016/j.aci.2011.05.002

Sarker, S., & Hossain, M. (2024). Building digital trust in the age of data breaches. *Journal of Information Systems Security*.

Schulz, K., Karovič, V., & Veselý, P. (2021). Options to improve the general model of security management in private bank with GDPR compliance. *In Developments in Information & Knowledge Management for Business Applications* (pp. 343–370). Cham, Switzerland: Springer.

Sharma, A., Rana, N. P., & Nunkoo, R. (2021). Fifty years of information management research: A conceptual structure analysis using structural topic modeling. *International Journal of Information Management*, 58, 102316.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215–225.

Strengholt, P. (2023). *Data management at scale*. Sebastopol, CA: O'Reilly Media.

Vinoth, S., Vemula, H. L., Haralayya, B., Mamgaln, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today: Proceedings*, 51, 2172–2175.

Vojdani, B. (2020). Investigating 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 the Humanities*. (in Persian)