Scientometrics Research Journal

Scientific Bi-Quarterly of Shahed University
Vol. 11, No. 2, Autumn & Winter 2025-26 (Serial 22)

Research Article

DOI: 10.22070/rsci.2025.20186.1790

From Information Security to Artificial Intelligence: A Scientometrics Analysis of Research Trends in Cybersecurity within the Banking Industry

Sepideh Fahimifar [1*]

Amirhossein Momenzadeh [2]

1. Associate Professor, Department of Information Science and Knowledge Management, Faculty of Public Administration and organizational Science, College of Management, University of Tehran, Tehran, Iran, (Corresponding Author).

2. Computer Science Engineering, Data Security and Splunk Expert in SITS Company-Mellat Bank.
Email: a.momenzadeh@sits-co.com

Email: sfahimifar@ut.ac.ir

Received:
22/02/2025

Revised:
31/05/2025

Accepted:
31/05/2025

Early online access:
31/05/2025

Published:
01/10/2025

Abstract

Purpose: Today, cybersecurity and confidentiality in cyberspace are more important than ever. This is especially critical in financial environments such as banks, due to the presence of individuals' confidential information and their financial accounts. Therefore, cybersecurity has emerged as one of the key thematic trends, and information security-related jobs are considered among the most important professions of the future. Consequently, policy-makers, managers, and banking specialists—given the sensitivity of the data stored in their environments—need to stay informed about the latest research in this field. However, due to the vast number of studies published annually in this area, it is not feasible for experts to review all of them. In this regard, scientometric and bibliometric approaches, indicators, and tools assist specialists in identifying the most important thematic areas of cybersecurity within the banking sector. Therefore, this study aims to explore the co-occurrence network, thematic evolution, trend topics, and thematic map using the authors' keywords.

Methodology: The study adopts a scientometric approach and employs methods such as co-word analysis, as well as centrality and density indicators for clustering. The research population comprises scientific outputs in cybersecurity indexed in the Web of Science database, with no time limitations. To conduct co-word analysis and form clusters, a thesaurus of terms and a list of stop terms were created. Additionally, the Walktrap algorithm was used to generate thematic maps of clusters. The software tools utilized for this study included the Biblioshiny package and VOSviewer.

Findings: From 2004 to 2024, the number of publications in this field has grown exponentially. Since 2020, the number of articles has increased from 259 to 438 in 2024, indicating the growing importance of security in the digital banking environment. The results of the co-occurrence keyword network showed that the keywords risk management (456 occurrences), machine learning (113 occurrences), credit risk (117 occurrences), and fraud detection (104 occurrences) had the highest frequency. These were followed by banking, fintech, bank, G21, deep learning, and fraud. The thematic map

Scientometrics Research Journal

Scientific Bi-Quarterly of Shahed University
Vol. 11, No. 2, Autumn & Winter 2025-26 (Serial 22)

Research Article

DOI: 10.22070/rsci.2025.20186.1790

Sepideh Fahimifar [1*]

Amirhossein Momenzadeh [2]

Received:
22/02/2025

Revised:
31/05/2025

Accepted:
31/05/2025

Early online access:
31/05/2025

Published:
01/10/2025

visualization revealed that topics such as machine learning, deep learning, fintech, artificial intelligence, cybersecurity, data models, fraud detection, and credit card have been prominent in recent years. In 2024, trending topics included fraud, data models, federated learning, and digital transformation. In 2023, the trending topics were machine learning, fintech, credit card fraud, and blockchain. In 2022, fraud detection, cybersecurity, Islamic banking, deep learning, and artificial intelligence were among the most frequently addressed subjects. In 2021, research peaked around topics such as bank, credit risk, corporate governance, systemic risk, and information security. Finally, in 2020, the most attention was given to topics such as risk, operational risk, capital, banking regulations, and credit scoring.

The machine learning cluster is positioned in the motor quadrant, indicating it is a driving theme. The fintech cluster falls into the basic quadrant, representing a fundamental theme. The maximum financial loss cluster is located in the emerging or declining quadrant, while the risk cluster is situated in the niche quadrant, indicating a specialized area.

To examine the historical trend of topics, four time periods were selected based on the publication dates of the articles. The first period (2004–2008) focused on topics such as deposit insurance, information security, data mining, risk, model risk, credit scoring, and capital. The second period (2009–2013) included themes such as fraud detection, credit risk, risk hedging, operational risk, credit risk management, risk, authentication, deposit insurance, financial crisis, financial risk management, cyber-attack, systemic risk, pervasive banking, and financial stability. The third period (2014–2018) addressed subjects like liquidity risk, operational risk, fraud detection, authentication, risk, financial crisis, information security, cybersecurity, and phishing. Finally, the fourth period (2019–2024) highlighted key topics such as credit risk, fintech, machine learning, and risk.

Conclusion: A logical analysis of the evolution of research in the field of cybersecurity in banks over the past two decades reveals a significant conceptual shift—from traditional topics such as financial risk and information security toward more advanced themes like machine learning, federated learning, and intelligent fraud detection. Emerging technologies such as federated learning, artificial intelligence, and financial technology have become key players, playing a central role in redefining security paradigms in the banking environment. Findings derived from co-word analysis, topic trends, and conceptual clustering indicate that traditional topics are no longer represented as independent clusters. Instead, they have either merged with newer themes to form interdisciplinary clusters or have lost prominence in comparison to emerging research frontiers. These transformations highlight a broader shift in cybersecurity research in the banking sector—from a linear, centralized perspective to a more complex, networked, and technology-driven approach.

Keywords: Cybersecurity, Banking, Scientometrics, Biblioshiny, VOSviewer, Thematic analysis.

پژوهش‌نامه علم‌سنجی
دوفصلنامه علمی دانشگاه شاهد/ دوره ۱۱/ شماره ۲/ پاییز و زمستان ۱۴۰۴ (پیاپی ۲۲)

مقاله پژوهشی

DOI: 10.22070/rsci.2025.20186.1790

گذار از امنیت اطلاعات به هوش مصنوعی: تحلیل روندهای پژوهشی در امنیت سایبری صنعت بانکداری با رویکرد علم‌سنجی

سپیده فهیمی فر [1*]

امیرحسین مؤمن زاده [2]

۱. دانشیار گروه علم اطلاعات و مدیریت دانش، دانشکده مدیریت دولتی و علوم سازمانی، دانشکدگان مدیریت، دانشگاه تهران، تهران، ایران، (نویسنده مسئول).

۲. مهندس رایانه، متخصص امنیت داده و اسپلانک شرکت زیرساخت امن خدمات تراکنشی- بانک ملت.

Email: sfahimifar@ut.ac.ir

Email: a.momenzadeh@sits-co.com

چکیده

هدف: افزایش جرائم سایبری در سال‌های اخیر و افزایش هزینه‌های ناشی از خسارت‌های وارده در این حوزه موجب شده است که مدیران، سیاست‌گذاران و دولتمردان بیش‌ازپیش به امنیت سایبری توجه نشان دهند. بااین‌حال، درصد کمی از متخصصان دید جامعی نسبت به موضوع‌های مهم این حوزه دارند. این پژوهش باهدف شناسایی موضوع‌های محرک، تخصصی، ضروری و پایه‌ای حوزه امنیت سایبری و همچنین بررسی روندهای موضوعی در سال‌های مختلف انجام‌شده است. علاوه بر این، شناسایی موضوع‌های نوظهور و روند تاریخی ظهور و افول موضوع‌ها در دوره‌های زمانی مختلف از دیگر اهداف این پژوهش است.

روش‌شناسی: رویکرد مطالعه، علم‌سنجی است و از روش تحلیل هم‌رخدادی، تحلیل شبکه‌های اجتماعی و شاخص‌های مرکزیت و چگالی استفاده‌شده است. جامعهٔ آماری پژوهش، کلیهٔ مقاله‌های منتشرشده (تعداد ۲۷۲۰ مقاله) در حوزهٔ امنیت سایبری در پایگاه وب‌آوساینس از سال ۲۰۰۴ تا ۲۰۲۴ است. به‌منظور تحلیل هم‌واژگانی و تشکیل خوشه‌ها، فهرست لغات یکپارچه و بازدارنده ساخته شد و برای تحلیل داده‌ها از نرم‌افزار ووس ویور و افزونهٔ تحت وب بیبلیوشاینی استفاده گردید.

یافته‌ها: شبکه هم‌رخدادی واژه‌ها نشان داد که موضوع‌های مدیریت ریسک و یادگیری ماشین بیشترین رخداد را در پژوهش‌ها به خود اختصاص داده‌اند و دارای بیشترین قدرت ارتباطی با سایر موضوع‌ها هستند. موضوع‌های کلاهبرداری، مدل‌های داده‌ای، یادگیری یکپارچه و تحول دیجیتال ازجمله مهم‌ترین موضوع‌های سال ۲۰۲۴ بوده است. خوشهٔ یادگیری ماشین دارای بیشترین مرکزیت و تراکم است.

نتیجه‌گیری: تحلیل منطقی روند تحولات پژوهشی در حوزه امنیت سایبری در بانک‌ها طی دو دهه گذشته حاکی از گذار مفهومی از موضوع‌های سنتی همچون «ریسک سرمایه» و «امنیت اطلاعات» به سمت مفاهیم نوینی مانند «یادگیری ماشین»، «یادگیری یکپارچه» و «کشف هوشمند کلاهبرداری» است. بازیگران اصلی در این حوزه فناوری‌های نوظهور مانند «یادگیری یکپارچه»، «هوش مصنوعی» و «فناوری مالی» هستند که نقشی کلیدی در بازتعریف الگوهای امنیتی ایفا می‌کنند.

واژگان کلیدی: امنیت سایبری، بانکداری، علم‌سنجی، بیبلیوشاینی، ووس ویور، تحلیل موضوعی.

صفحه ۳۲۶-۲۹۹

دریافت: ۱۴۰۳/۱۲/۰۴

بازنگری: ۱۴۰۴/۰۳/۱۰

پذیرش: ۱۴۰۴/۰۳/۱۰

زودآیند: ۱۴۰۴/۰۳/۱۰

انتشار: ۱۴۰۴/۰۷/۰۹

مقدمه و بیان مسئله

آمارهای متعددی از سراسر جهان منتشرشده‌اند که نشان می‌دهند بسیاری از افراد در طول زندگی خود با چالش‌هایی درزمینهٔ خدشه‌دار شدن امنیت در فضای اینترنت و شبکه‌ها مواجه بوده‌اند. جرائم سایبری نظیر سرقت هویت، زورگویی اینترنتی، مزاحمت سایبری، ازجمله مهم‌ترین معضلات جهانی محسوب می‌شوند که نه‌تنها امنیت فردی، بلکه امنیت شرکت‌های بین‌المللی، بانک‌ها و دولت‌ها را نیز تهدید می‌کنند (Loan et al., 2022). با توجه به حساسیت بالای امنیت سایبری در محیط بانک‌ها، ارزیابی مداوم و اصلاح استراتژی‌های امنیت سایبری، ضرورتی انکارناپذیر است. این مهم نیازمند همکاری مستمر با شرکت‌های فعال در حوزه امنیت سایبری است. در این میان، بهره‌گیری از هوش مصنوعی در کنار دانش تخصصی انسانی می‌تواند بر بهبود این وضع کمک قابل‌توجهی انجام دهد. بر اساس گزارش پترویسان (Petrosyan, 2025) تعداد شکایت‌های مرتبط با جرائم اینترنتی به ۸۸۰ هزار مورد و شمار قربانیان فیشینگ در آمریکا در سال ۲۰۲۳، به ۲۹۹ هزار نفر رسید. همچنین، نتایج یک نظرسنجی در استرالیا نشان داد که ۲۷ درصد از شرکت‌کنندگان قربانی سوءاستفاده آنلاین، ۲۲ درصد هدف بدافزارها، ۲۰ درصد دچار سرقت هویت و ۸ درصد قربانی کلاهبرداری شده‌اند. علاوه بر این ٤٧ درصد از افراد موردبررسی این مطالعه، در طول ۱۲ ماه پیش از شرکت در پژوهش، حداقل یک جرم سایبری را تجربه کرده‌اند و نیمی از این گروه با بیش از یک جرم سایبری مواجه بوده‌اند (Voce & Morgan, 2023).

هزینه‌های جهانی ناشی از خسارت جرائم سایبری نیز به‌شدت بالاست؛ شرکت سایبرسکیوریتی وِنچر که شرکت پژوهشی معتبری در زمینه اقتصاد جهانی سایبری است در گزارش منتشر شده خود خسارات ناشی از جرائم سایبری را در سال ۲۰۲۵، ۱۰.۵ تریلیون دلار پیش بینی کرده است که تا سال ۲۰۳۱ به ۱۲.۲ تریلیون دلار خواهد رسید. این رقم رشد چشمگیری نسبت به سال ۲۰۱۵ (۳ تریلیون دلار) داشته است (Cybersecurity Ventures, 2025) . در سال‌های اخیر هزینه نشت داده‌ها[1] بسیار افزایش‌یافته است به‌طوری‌که بر پایه گزارش شرکت امنیتی «آی‌بی‌ام»، میانگین هزینه نشت اطلاعاتی به ٤.٣٥ میلیون دلار افزایش‌یافته است (Kuzior et al., 2022). به‌علاوه هزینه جرائم سایبری در سرتاسر جهان در سال ۲۰۲٤ معادل ۹.۲۲ تریلیون دلار بوده است. همچنین پیش‌بینی‌شده در فاصله سال‌های ۲۰۲٤ تا ۲۰۲۹ شاخص جهانی «هزینهٔ تخمینی جرائم سایبری» به‌طور پیوسته افزایش یابد که رشد ٦٩ درصدی را نشان می‌دهد و در سال ۲۰۲۹ به رقم ۱۵.٦۳ تریلیون آمریکا خواهد رسید. در نتیجه، سازمان‌ها بیش از گذشته به مخاطرات ناشی از حملات سایبری آگاه شده‌اند و تقویت تاب‌آوری سایبری در گروه‌های امنیت اطلاعات به یکی از اولویت‌های اصلی هزینه‌کرد شرکت‌های جهانی در سال ۲۰۲۳ تبدیل‌شده است (Petrosyan, 2025).

بر اساس گزارش آینده شغلی در سال ۲۰۲۳، مشاغلی نظیر متخصص یادگیری ماشین و هوش مصنوعی، متخصصان توسعه پایدار، تحلیل‌گر هوش تجاری، تحلیل‌گر امنیت اطلاعات، مهندسان فناوری مالی و نظایر آن به وجود آمده و یا در آینده پیشرفت خواهند کرد. اغلب شغل‌هایی که در آینده پیشرفت بسیار زیادی خواهند کرد مرتبط با فناوری هستند و در مقابل اکثر شغل‌هایی که تعداد آن‌ها کاهش خواهد یافت، مرتبط با دفتری یا منشی‌گری، متصدیان بانک و کارکنان مرتبط، کارمندان خدمات پستی و کارمندان مربوط به تهیه بلیت خواهند بود (Aldasoro et al., 2024). بنابراین، بحث امنیت اطلاعات، به‌ویژه در حوزه‌های مالی، ازجمله مهم‌ترین حوزه‌های موردتوجه در سال‌های پیش‌رو است. بااین‌حال، تنها درصد کمی از متخصصان این حوزه، دید جامعی از ابعاد و موضوع‌های مهم و

1 . data breaches

همهٔ جنبه‌های آن دارند (Alqurashi & Ahmad, 2024). بدیهی است که امنیت سایبری موضوع موردتوجه و علاقه طیف وسیعی از ذی‌نفعان است چراکه تمرکز بر آن می‌تواند از حمله‌های سایبری، سرقت‌های اطلاعاتی و نشت داده‌ها جلوگیری کرده و به مدیریت ریسک کمک کند. این مفهوم، یکی از موضوعات در حال رشد با تأثیر و نتایجی بسیار گسترده است (Solms & Solms, 2018). بنابراین روش‌ها و فعالیت‌های مرتبط با امنیت سایبری باهدف حفاظت از داده‌ها، اطلاعات و شبکه‌های شخصی و سازمانی در برابر تمام تهدیدات ممکن، چه داخلی و چه خارجی، طراحی‌شده‌اند (Akintoye et al., 2022). در حال حاضر پژوهش‌های مرتبط با امنیت سایبری در اوج شکوفایی قرار دارند. در این میان، بهره‌گیری از روش‌های علم‌سنجی می‌تواند به‌ویژه ازنظر کمی و کیفی، برای ارزیابی روندها و تحلیل ساختار این حوزه بسیار سودمند واقع شود (Loan et al., 2022).

آگاهی از موضوعات و ایده‌های مهم یک حوزهٔ علمی به‌صورت سنتی با پرسش از متخصصان و بر اساس شیوه‌های نوین‌تر از طریق تحلیل واژگان منابع اطلاعاتی آن حوزه انجام می‌شود (Lee, 2008). پژوهش‌های علم‌سنجی مرتبط با حوزهٔ امنیت سایبری را می‌توان به دو دستهٔ کلی تقسیم کرد: دسته اول، مطالعاتی هستند که به بررسی کارآمدترین نویسندگان، کشورها، سازمان‌ها، منابع منتشرکننده و نظایر آن پرداخته‌اند(Dhawan et al., 2021; Olijnyk, 2015; Rai et al., 2019). دسته دوم پژوهش‌هایی هستند که به شناسایی موضوع‌های پرکاربرد، خوشه‌های موضوعی و تحلیل‌های هم‌استنادی پرداخته‌اند که در کنار دید کمی، تحلیل کیفی این پژوهش‌ها نسبت به پژوهش‌های نخست به‌منظور آگاهی از روندهای موضوعی گذشته و شناسایی موضوعات آینده مهم‌تر است(Elango et al., 2023; Omote et al., 2024; Pourmadadkar et al., 2024; Shevchuk & Martsenyuk, 2024). بااین‌حال، بررسی مطالعات گذشته نشان می‌دهد که طیف منابع گردآوری‌شده منطبق باهدف پژوهش نبوده است؛ چراکه مهم‌ترین بخش تحلیل داده‌ها در علم‌سنجی بحث گردآوری منابع است. در اغلب پژوهش‌های پیشین، تنها از مجموعه محدودی از کلیدواژه‌ها برای بازیابی منابع مرتبط استفاده‌شده است و به نظر می‌رسد نیاز به تحلیل موضوع‌های مقاله‌ها به‌صورت جامع وجود دارد. از سوی دیگر، تعداد معدودی از پژوهش‌های گذشته به بررسی موضوع‌های نوظهور، تخصصی، محرک یا پیشران این حوزه پرداخته‌اند. همچنین، تحلیل روندهای تاریخی موضوع‌ها در بازه‌های زمانی مختلف و روند تحول آن‌ها در کم‌تر پژوهشی بررسی‌شده است.

پژوهش‌های جدید همواره مبنای تصمیم‌گیری‌ها و پژوهش‌های آینده هستند و از همه مهم‌تر می‌توانند موجب دستاوردهای عملی در محیط واقعی باشند. روش‌هایی نظیر فراترکیب، مرور سامانمند و علم‌سنجی می‌توانند شمای کلی از میزان پیشرفت‌ها، همکاری‌ها، موضوع‌های موردتوجه و نظایر آن را در اختیار پژوهشگران قرار دهند. بنابراین، آگاهی از روند پژوهش‌ها، همکاری‌های موجود و مهم‌تر از همه خوشه‌های پژوهشی اصلی و حوزه‌های موضوعی نوظهور یا رو به افول می‌تواند پژوهشگران این حوزه را با آخرین پیشرفت‌ها در این حوزه آشنا سازد. با توجه به اهمیت موضوع امنیت سایبری، به‌ویژه در سال‌های اخیر و کافی نبودن دانش متخصصان این حوزه درزمینهٔ طیف‌های موضوعی گستردهٔ حوزهٔ مورداشاره و نیز اهمیت حفظ داده‌های مشتریان و محرمانه بودن داده‌ها در محیط‌های مالی به‌خصوص بانک‌ها، نیاز به آگاهی از روندهای موضوعی این حوزه احساس می‌شود. این پژوهش باهدف شناسایی حوزه‌های موضوعی با شبکه هم‌رخدادی[1] واژگان، پیگیری تحول مفاهیم،[2] کشف موضوع‌های نوظهور، روندهای

1 . Co-occurrence network
2 . Thematic evolution

موضوعی[1] و نقشه‌های موضوعی[2] با تحلیل تماتیک چهار بخشی است. ازاین‌رو، این پژوهش درصدد پاسخگویی به این پرسش است که موضوعات اصلی و تحول‌یافته حوزهٔ امنیت سایبری در محیط بانکداری چه موضوعاتی هستند و روند تحول آن‌ها در دوره‌های زمانی مختلف چگونه بوده است؟

پرسش‌های پژوهش

پرسش‌هایی که این پژوهش قصد پاسخگویی به آن‌ها را دارد عبارت‌اند از:

۱. روند انتشارات و استنادات پژوهش‌های انجام‌شده در حوزهٔ امنیت سایبری در بانک‌ها چگونه بوده است؟

۲. شبکه هم‌رخدادی واژگان در حوزهٔ امنیت سایبری در بانک‌ها چگونه است؟

۳. تحول موضوع‌های پرتکرار در دوره‌های زمانی مختلف چگونه است؟

٤. در نقشه موضوعی حوزهٔ امنیت سایبری در بانک‌ها موضوع‌های محرک، تخصصی، ضروری و نوظهور چه موضوع‌هایی هستند؟

۵. روندهای موضوعی مهم و پرتکرار و موضوع های محرک، تخصصی، ضروری و نوظهور یا رو به افول در دوره های زمانی مختلف چه موضوع‌هایی بوده‌اند؟

چارچوب نظری

امنیت سایبری مجموعه‌ای جامع از همه روش‌ها و فناوری‌هایی است که مسئول دفاع از شبکه‌ها، نرم‌افزارها و داده‌ها در برابر حملات سایبری احتمالی هستند (Shaukat et al., 2020). با افزایش ارتباط بینابینی احتمال وقوع حملات سایبری افزایش می‌یابد (Deora & Chudasama, 2021). این امر، به‌ویژه بعد از دورهٔ همه‌گیری کرونا با توجه به افزایش ارتباطات در سطح مجازی اهمیت ویژه‌ای یافت. اتحادیه اروپا و دولت‌های عضو آن نیز در آن دوره و بعدازآن با تهدیدها و فعالیت‌های سایبری مخربی روبرو بوده‌اند (Borrell, 2020). در سطح جهانی تهدیدهای محیط سایبری شامل سرقت هویت، حملات بدافزار، فیشینگ و ویژینگ، ویروس‌ها و تروجان‌ها، کلاهبرداری با کارت‌های ای تی اِم، دبیت، اعتباری، باج‌افزار، تهدیدات داخلی، جعل هویت، محروم‌سازی از خدمات، مهندسی اجتماعی، تروریسم سایبری، هک رایانه و سرقت اطلاعات، داده‌های رمزنگاری نشده، خدمات شخص ثالث غیرقابل‌اعتماد، حملات دسترسی مستقیم، مهندسی معکوس و ایمیل‌های اسپم بیش از گذشته دارای اهمیت شدند (Cele & Kwenda, 2024).

صنعت بانکداری برای حفاظت همیشگی از داده‌های مهم نیاز به انطباق با فناوری‌های نوین دارد. بانکداری دیجیتالی با حذف محیط فیزیکی و تبدیل آن به محیط الکترونیکی و حضور مشتری به‌واسطه کلیک در محیط اینترنت بیش‌ازپیش محبوب شده است (Nesakumar et al., 2022). بااین‌حال حفاظت و امنیت داده‌های مشتریان و رکوردهای تراکنش‌ها اهمیت ویژه‌ای دارد. درنتیجه سنجه‌های امنیت سایبری قوی به‌منظور محافظت از تخلف‌ها و کلاهبرداری‌ها ضروری است.

حوزهٔ پژوهشی امنیت سایبری طیف گسترده‌ای از زمینه‌ها است، از شبکه، نرم‌افزار و سخت‌افزار گرفته تا رمزنگاری، احراز هویت و مقابله با حملات سایبری (Omote et al., 2024). سالانه حجم قابل‌توجهی از پژوهش‌ها

1 . Trend Topics
2 . Thematic Map

در حوزه امنیت سایبری در محیط بانکی انجام می‌شود تا از تهدیدهای فضای سایبری جلوگیری و استراتژی‌های مقابله با ریسک‌های احتمالی توسعه یابد (Cele & Kwenda, 2024). امروزه، اغلب بانک‌های مرکزی ابزارهای هوش مصنوعی مولد را برای کشف سریع تهدیدهای سایبری و کاهش زمان پاسخگویی به این تهدیدها پذیرفته‌اند. بااین‌حال، ظهور هوش مصنوعی مولد خطراتی نظیر حملات مهندسی اجتماعی و افشای غیرمجاز داده‌ها را افزایش داده است. بنابراین، نیاز به سرمایه‌گذاری در حوزهٔ نیروی انسانی کارآمد، متخصص در امنیت سایبری و برنامه‌نویسی هوش مصنوعی، از سوی بانک‌های مرکزی به‌شدت احساس می‌شود (Aldasoro et al., 2024).

مدیران و سیاست‌گذاران، از اهمیت راهبردی علم و فناوری در ایجاد ارزش و مزیت رقابتی برای سازمان‌ها، شبکه‌های صنعتی، مناطق و کشورها آگاه هستند. این مسائل با افزایش هزینه، پیچیدگی و نرخ افزایش تغییر فناوری و همچنین جهانی‌شدن رقابت و منابع فناوری، اهمیت بیش‌تری پیدا کرده‌اند. هم مدیران و هم سیاست‌گذاران (مانند نهادهای تأمین مالی) باید درباره این‌که در کدام حوزه‌های فناورانه سرمایه‌گذاری کرده و کدام گزینه‌های راهبردی را دنبال کنند، تصمیم‌گیری کنند. این تصمیم‌گیری‌ها چالش‌برانگیز است، زیرا تحولات بازار، فناوری و صنعت، پیچیده و پویا هستند و کمبود اطلاعات و عدم قطعیت در پیش‌بینی‌ها نیز بر دشواری آن می‌افزاید (Phaal et al., 2011). برای بنیادهای پژوهشی و سیاست‌گذاران، شناسایی به‌موقع موضوع‌های نوظهور[1] پژوهشی بسیار اهمیت دارد، چراکه به توسعهٔ حوزه‌های پژوهشی نویدبخش، کمک می‌کند.

فناوری‌های نوظهور موضوع بحث‌های فراوان در پژوهش‌های دانشگاهی و موضوع‌های مرکزی در سیاست‌گذاری بوده و ابتکاری برای تحرک بخشیدن به نوآوری‌ها هستند. افزایش تعداد انتشارات مرتبط با علم و فناوری و همچنین افزایش اخبار مربوط به فناوری‌های نوظهور و پروژه‌های پژوهشی، نشان‌دهندهٔ توجه روزافزون به این فناوری‌ها و موضوعات مرتبط با آن‌هاست. پروژه‌های متعددی که توسط شورای تحقیقات اروپا[2] برای شناسایی حوزه‌های نوظهور اجراشده است، نمونه‌ای از علاقهٔ فزاینده به این موضوعات هستند (Xu et al., 2021).

بهترین نمایهٔ یک رشته علمی، منابعی است که جامعهٔ علمی آن رشته منتشر می‌کنند (Martín-Martín et al., 2016) هرساله تقریباً یک میلیون مقاله علمی در حال انتشار است؛ آیا می‌توانیم تمامی این پیشرفت‌ها را دنبال کنیم و از الگوهای پنهان آن‌ها مطلع شویم (Van Raan, 2014)؟ بیشتر مرورهای ادبیات موجود، بر اساس تجربه پژوهشگران صورت می‌گیرد و ممکن است تحت تأثیر محدودیت‌های زمانی و توانایی شناختی آن‌ها در حوزه موردنظر قرار گیرد. بنابراین، ممکن است برخی مقاله‌ها در مرور آن پژوهشگر وارد نشوند (Raghuram et al., 2010).

کلیدواژه‌های مقاله‌های علمی چه به‌صورت دستی (توصیفگرهای موضوعی و کلیدواژه‌های نویسندگان) و چه به‌صورت خودکار تولیدشده باشند؛ نماینده‌ای از پیشرفت‌ها، ساختار و موضوع‌های یک حوزه علمی به‌واسطه تحلیل واژگان هستند (Callon et al., 1983). برخلاف روش‌های کتاب‌سنجی نظیر تحلیل هم‌استنادی و تحلیل هم‌نویسندگی، تحلیل هم‌واژگانی روش محتوا–مداری است که به‌واسطه آن مفاهیم موضوعی تفسیر می‌شوند. فراوانی اصطلاح به‌عنوان تعداد رخداد آن اصطلاح در مجموعه‌ای مشخص تعریف می‌شود و اغلب به‌منظور توصیف تم‌های موضوعی مهم یک حوزه به شمار می‌آیند (Khasseh et al., 2017). اگرچه رخداد یک کلمه می‌تواند تم‌های مهم هر حوزه موضوعی را نشان دهد، اما این سنجه روابط هم‌رخدادی در میان کلیدواژه‌ها را نادیده می‌گیرد که این مهم در

1 . emerging research topics (ERTs)
2 . European Research Council (ERC)

شبکه‌های هم‌واژگانی پیاده‌سازی شده است. ساختار شبکه‌های هم‌واژگانی ماورای رخداد کلمه هستند و می‌توانند اهمیت کلیدواژه را موردسنجش قرار دهند (Wanying et al., 2018). برای تحلیل واژگان اصطلاحات اغلب از عناوین، متن کامل اثر، چکیده‌ها، اصطلاحات موضوعی و کلیدواژه‌های نویسندگان استفاده می‌شود (Wanying et al., 2018).

پیشینهٔ پژوهش

پژوهش‌های متعددی تاکنون به بررسی مبحث امنیت سایبری در محیط بانکی از ابعاد مختلف پرداخته‌اند. بااین‌حال، نگاه به این حوزه از دیدگاه علم‌سنجی نادیده گرفته‌شده است. عسکریان کاخ و همکاران (۱۴۰۲) به بررسی مقالات مجلات و کنفرانس‌های منتشرشده در حوزه موضوعی سیاست‌های پولی در بانک اطلاعاتی وب‌آوساینس پرداختند. آن‌ها از نرم‌افزار راور پریمپ، ووس ویور[1] و اکسل استفاده کردند. پرکارترین نویسندگان، پربسامدترین کلیدواژه‌ها و مجلات هسته، پراستنادترین مقالات در اثر پژوهشی آن‌ها شناسایی‌شده است. عسگری مهر و مقصودلو (۱۴۰۲) به ارائه مدلی برای مدیریت ریسک امنیت سایبری با تأکید بر یکی از بانک‌های ایران پرداختند. آن‌ها برای استخراج شاخص‌ها از مطالعه کتابخانه‌ای و برای ارزیابی و بهینه‌سازی شاخص‌ها، از گروهی از متخصصان موضوعی استفاده کردند. درنهایت، شاخص‌ها از سوی تعدادی از متخصصان مورد ارزیابی قرار گرفت و مدل مفهومی نهایی بر اساس معادلات ساختاری استخراج و بر مبنای روش تحلیل عاملی تأییدی تفسیر شد. آن‌ها به این نتیجه رسیدند که بیمه سایبری، استراتژی‌های سازمانی، راهبری فناوری در سازمان، مشتری، کارمندان، قوانین کشوری بر مدیریت ریسک امنیت سایبری تأثیرگذار است. حاجیان و زرجینی (۱۴۰۲) با رویکرد علم‌سنجی و استفاده از نرم‌افزار ووس ویور، به بررسی مقالات منتشرشده در بانک اطلاعاتی وب‌آوساینس در حوزه موضوعی بیمه پرداختند. آن‌ها شبکه هم‌رخدادی واژگان در حوزه موضوعی داده‌کاوی و بیمه، کشف تخلفات بیمه، ریسک و مدیریت آن را ترسیم کردند. افزون بر این، به شناسایی مجلات مهم و کشورهای منتشرکننده مقالات نیز پرداختند.

آزاد سنجری و چارسوقی (۱۴۰۳) به بررسی نوآوری‌ها و توسعه امنیت سایبری در بانک‌های ایران با استفاده از کارت امتیازی متوازن پرداختند. آن‌ها رشد روزافزون آگاهی عمومی نسبت به امنیت اطلاعات، همکاری با شرکت‌های داخلی در رابطه با امنیت سایبری، افزایش نیاز به خدمات بانکداری اینترنتی را به‌عنوان فرصت، ایجاد روابط نزدیک با نهادهای نظارتی، سیاست‌ها و استانداردهای سخت‌گیرانه داخلی را به‌عنوان نقاط قوت، حملات سایبری از سوی دولت‌ها، ضعف قوانین حفاظت از داده‌ها، سرعت‌پایین تطابق با تغییرات فناورانه را به‌عنوان تهدید و عدم انطباق ساختار سازمانی مطابق با استانداردهای امنیتی، کمبود نیروی انسانی متخصص، ضعف در آموزش و آگاهی کارکنان را به‌عنوان ضعف شناسایی کردند.

در حوزه‌های مرتبط با امنیت سایبری تاکنون پژوهش‌هایی با رویکرد کتاب‌سنجی و علم‌سنجی به زبان‌های غیرفارسی انجام‌شده است. نخستین پژوهش در حوزه امنیت اطلاعات، از سوی لی (Lee, 2008) صورت گرفته که از داده‌های نمایه استنادی علوم استفاده کرد و به تحلیل هم‌واژگانی به‌منظور تعیین موضوع‌های مهم این حوزه پرداخت. اُلیجنیک (Olijnyk, 2015) به تحلیل مقاله‌های منتشرشده در مجله‌ها و کنفرانس‌ها در حوزه امنیت اطلاعات در پایگاه اسکوپوس از سال ۱۹۶۵ تا ۲۰۱۵ پرداخت و از کلیدواژه‌هایی مانند امنیت اطلاعات، تضمین اطلاعات، امنیت سایبری و تنوع نگارش آن، امنیت رایانه، امنیت ارتباطات، امنیت داده و امنیت شبکه برای جستجوی منابع مرتبط

1 .VOSviewer

استفاده کرد. به‌علاوه با استفاده از نرم‌افزار ووس ویـور بـه تحلیـل واژگـان پرداخـت. رمزنگـاری و مـدیریت امنیـت اطلاعات به‌عنوان موضوع موردتوجه چندین دهـه و موضـوع‌هـایی نظیـر شناسـایی نفـوذ، امنیـت داده‌هـای پزشـکی، نهان‌نگاری و امنیت بی‌سیم به‌عنوان موضوع‌های نوظهور مطرح شدند. پژوهشی مشابه نیـز، باهـدف بررسـی تولیـدات علمی در حوزه امنیت اطلاعات و امنیت سایبری با رویکرد علم‌سنجی و ترسیم نقشـه‌هـای دانشـی از سـال ۱۹۹۵ تـا ۲۰۱۵ در نمایه استنادی علوم اجتماعی و نمایه استنادی هنر و علوم انسانی انجام‌شده است. درمجموع، ۱۷۵۰ مقالـه در بارهٔ امنیت اطلاعات و ۵۳۸ مقاله در حوزه امنیت سایبری با بهره‌گیری از نرم‌افزار سایت اسپیس مورد تحلیل قرار گرفتند.

رایانش ابری جدیدترین اصطلاحی است که از سال ۲۰۱۱ به بعد موردتوجه بوده است. مقاله‌هـایی کـه بـه هـر دو موضوع امنیت اطلاعات و امنیت سایبری مرتبط بودند، به موضوع انرژی برق بسیار توجه داشـته‌انـد کـه نشـان‌دهنـدهٔ مسئله آسیب‌پذیری زیرساخت‌های کنترل متصل به اینترنـت اسـت (Chang, 2016). ارزیـابی داده‌هـای پژوهشـی در حوزه امنیت سایبری، در بانک اطلاعاتی اسکوپوس از سال ۲۰۰۱ تا ۲۰۱۸ موضوع پژوهش دیگری بوده اسـت. رای و همکاران (Rai et al., 2019) به تحلیل نویسندگان، مؤسسات، همکاری‌ها و بودجه‌های پژوهشـی پرداختنـد. در ایـن مطالعه، تنها از واژه امنیت سایبری برای گردآوری داده‌ها در قسمت جستجوی عنوان بانک اطلاعاتی، استفاده‌شده است.

دافی و دافی (Duffy & Duffy, 2020) به‌مرور سامانمند و شناسایی موضوع‌های نوظهور عوامل مـرتبط انسـانی در امنیت سایبری با استفاده از تحلیل محتوا و روش‌های علم‌سنجی تا سال ۲۰۲۰ در دو پایگاه وب‌آوساینس و گوگـل اسکالر پرداخته‌اند. آن‌ها از ابزارهایی نظیر ووس ویور، مکس کیودا[1]، هارزیگ[2]، اوتـورمپر[3] بـرای تحلیـل پـژوهش‌هـا استفاده کردند. کلیدواژه‌های مورد جستجو برای گردآوری منابع تنها محدود به امنیت سـایبری و عامـل انسـانی[4] بـوده است. عوامل انسانی و ارگونومی کاربردی[5] مهم‌ترین موضوع پرتکرار در پژوهش‌های این حوزه بوده اسـت. مشـابه بـا پژوهش لی (Lee, 2008)، لون و همکاران (Loan et al., 2022) در مطالعه‌ای به تحلیل مجموعه مقالـه‌هـای نمایـه شده در مجموعه هستهٔ وب‌آوساینس از سال ۲۰۱۱ تا ۲۰۲۰ در حوزه‌های امنیت سایبری، امنیت وب، امنیت اطلاعـات و امنیت رایانه پرداختند. مجموعهٔ داده‌ها در قالـب فایـل‌هـای اکسـل ذخیـره شـد و بـا اسـتفاده از افزونـه تحـت وب بیبلیوشاینی[6] و نرم‌افزار ووس ویور، تحلیل داده‌ها انجام گرفت. تنوع کلیدواژه‌هـای مـورد جسـتجو در ایـن پـژوهش، گردآوری داده‌ها نسبت به پژوهش حاضر، کم‌تر بود. نتایج نشان داد که متـداول‌تـرین کلیـدواژه‌هـا امنیـت سـایبری و پس‌ازآن تنوع نگارشی این کلیدواژه‌ها به‌صورت ترکیب دو کلیدواژه امنیت و سایبر با فاصله و بعـدازآن بـا خـط تیـره بوده است. کلیدواژه‌های امنیت، امنیت رایانه‌ای و امنیت اطلاعات، حفظ محرمانگی، یـادگیری ماشـین، اینترنـت اشـیا، تشخیص نفوذ، رمزنگاری، شبکه هوشمند برق در رتبه‌های بعد قرار دارند.

برخی پژوهش‌ها تولیدات علمی با موضوع امنیت سایبری خاص یک کشور را بررسی کـرده‌انـد. بـه‌عنـوان نمونـه تولیدات علمی مربوط به امنیت سایبری در کشور مکزیک، ازجمله پژوهش‌های اخیر در این حوزه به شمار می‌رود که با رویکرد کتاب‌سنجی و باهدف بررسـی تعـداد مقـالات سـالانه، تعـداد مقـالات در هـر نشـریه، سـهم مؤسسـات و نویسندگان و محتوای موضوعی مقالات انجام‌شده است (Matilde-Espino & Valencia-Pérez, 2022).

1 . MAXQDA
2 . Harzing
3 . AuthorMapper
4 . cybersecurity AND human factors
5 . Applied Human Factors and Ergonomics(AHFE)
6 . Biblioshiny

اِلانگو و همکارن (Elango et al., 2023) ازنظر جنبه‌های انسانی نیز به مسئله امنیت سایبری با رویکرد علم‌سنجی نیز توجه کرد و با استفاده از نرم‌افزارهای اکسل، پکیج بیبلیومتریکس آر، ووس ویور و یوسی‌نِت به کشف ساختارهای اجتماعی و مفهومی منابع منتشرشده از سوی پژوهشگران هندی پرداخت و درمجموع ۹۸۹ مدرک مورد تحلیل قرار گرفت. پژوهشگران هندی توجه خود را از موضوعات مرتبط با داده به موضوع‌های یادگیری ماشین، فناوری‌های مرتبط با هوش مصنوعی و رایانش ابری سوق داده‌اند. موضوع مقاله‌ها از امنیت شبکه در سال ۲۰۱٤ به شبکه‌های هوشمند در سال ۲۰۱۵، سپس محاسبه ابری در سال ۲۰۱۷ تغییریافته است. سپس در بازهٔ ۲۰۱۸ تا ۲۰۲۰ از کنترل نظارتی و جمع‌آوری داده‌ها[1] در سال ۲۰۱۸ به یادگیری عمیق در سال ۲۰۲۰ تغییریافته است.

پورمددکار و همکاران (Pourmadadkar et al., 2024) به تحلیل کتاب‌سنجی منابع منتشرشده در پایگاه وب‌آوساینس و اسکوپوس در حوزه امنیت سایبری در سیستم‌های سایبری-فیزیکی[2] (درمجموع ۱٦٤۹ مدرک) پرداختند. آن‌ها از تحلیل هم‌رخدادی واژگان باهدف شناسایی خوشه‌های موضوعی استفاده کردند که درمجموع ۷ خوشه شناسایی شد. توسعه دانش در این حوزه به ٤ دورهٔ زمانی امنیت داده‌ها در سیستم‌های کنترل نظارتی و گردآوری داده‌ها[3]، امنیت زیرساخت‌های حیاتی[4]، امنیت سایبری سیستم‌های کنترل صنعتی[5] و امنیت سایبری سیستم‌های سایبر-فیزیکی[6] تقسیم‌شده است.

اُمُت و همکاران (Omote et al., 2024) به شناخت انواع حوزه‌های موضوعی امنیت سایبری با بررسی پژوهش‌های ده درصد برتر در فاصله سال‌های ۲۰۱۰ تا ۲۰۱۹ که حتماً دو سال از زمان انتشار آن‌ها گذشته باشد، پرداختند. یافته‌ها نشان داد که این حوزه به چهار حوزه اصلی حملات سایبری، رمزنگاری، احراز هویت و بلاکچین مربوط است که بیش‌ترین تعداد پژوهش‌ها را تاکنون به خود اختصاص داده‌اند. پژوهش دیگری در حوزه به‌کارگیری شبکه‌های عصبی در امنیت سایبری به‌واسطه تحلیل علم‌سنجی و به‌کارگیری نرم‌افزار سایت اسپیس انجام‌شده است. جامعهٔ پژوهش انواع منابع منتشرشده در این حوزه از سال ۲۰۰۳ تا ۲۰۲۳ در پایگاه مجموعه هسته وب‌آوساینس بوده است. به‌علاوه منابع گردآوری‌شده با جستجوی کلیدواژه امنیت سایبری با دو مدل نگاش پیوسته دو کلمه و جدا از هم به همراه کلیدواژه شبکه عصبی در بخش موضوعی این پایگاه (درمجموع ۲۰۱۸ منبع) جمع‌آوری‌شده است. حوزه یادگیری عمیق، یادگیری ماشین و تشخیص نفوذ، امنیت سایبری، شبکه های عصبی، اینترنت، الگوریتم، بهینه‌سازی، داده‌های بزرگ و اینترنت اشیاء به ترتیب از مهم‌ترین موضوعاتی بوده‌اند که فراوانی بالاتری نسبت به سایر کلیدواژه‌ها داشته‌اند. به‌علاوه کلیدواژه‌های امنیت سایبری، داده‌کاوی و شبکه عصبی به ترتیب بیش‌ترین میزان استناد را در بازه‌های مختلف با توجه به دورهٔ زمانی موردبررسی به خود اختصاص داده‌اند (Shevchuk & Martsenyuk, 2024).

در حوزهٔ آموزش عالی نیز به امنیت سایبری با رویکرد کتاب‌سنجی و با استفاده از نرم‌افزارهایی مانند دیتارَپِر[7]، ووس ویور و بیبلیومتریکس توجه شده و مطالعه‌ای بر منابع منتشرشده در پایگاه اسکوپوس انجام گرفته که درمجموع ۱۱۸ اثر را در بر می‌گیرد. در این حوزه، بیشتر پژوهش‌ها به مسائلی چون امنیت سایبری، تهدیدات سایبری، آگاهی از امنیت سایبری، نقض امنیت سایبری، امنیت اطلاعات، و مقررات عمومی حفاظت از داده‌ها پرداخته‌اند (Orosco-Fabian, 2024).

1 . SCADA
2 . Cyber–physical systems (CPSs)
3 . Supervisory Control and Data Acquisition
4 .critical infrastructures
5 . industrial control systems
6 .Cyber–physical systems (CPSs)
7 . Datawrapper

نگاهی به پژوهش‌های گذشته نشان می‌دهد که تحلیل مطالعات حوزه امنیت سایبری و امنیت اطلاعات به‌عنوان مسائل مهم، به‌صورت کلی یا با توجه به جنبه‌های خاص آن موردبررسی قرارگرفته است. بنابراین، پرداختن به حوزه امنیت سایبری به‌صورت مطالعات کلان محور یا موضوع محور بوده است. موضوع امنیت سایبری در ارتباط با عامل انسانی، آموزش، سیستم‌های سایبری-فیزیکی، شبکه‌های عصبی به‌صورت خاص در پژوهش‌ها بررسی‌شده و در سایر تحقیقات، موضوع امنیت سایبری و امنیت اطلاعات به‌صورت کلی ارزیابی‌شده است.

ازنظر موضوعی، هیچ پژوهشی به بررسی حوزه‌های موضوعی امنیت سایبری در محیط بانکداری نپرداخته است. این در حالی است که حوزه بانکداری به‌عنوان حیاتی‌ترین زیرساخت اقتصادی می‌تواند با چالش‌های مهم، اساسی و منحصربه‌فردی به‌صورت روزانه مواجه باشد. هدف عمده پژوهش‌های گذشته، شناسایی روندها و بازیگران کلیدی این حوزه بوده است. بااین‌حال، تحلیل روندهای موضوعی، شناسایی موضوع‌های مهم در دوره‌های زمانی مختلف و تحول آن‌ها، شناخت موضوع‌های محرک، ضروری و نوظهور و بررسی روندهای پررنگ و کم‌رنگ شدن موضوعات در تحقیقات موردتوجه نبوده است؛ ازاین‌رو پژوهش حاضر سعی دارد تمامی این جنبه‌ها را پوشش دهد. درنتیجه، این پژوهش، دید جامع‌تر و دقیق‌تری از روندهای موضوعی مهم در حوزهٔ امنیت سایبری در بانک‌ها ارائه می‌دهد.

در این پژوهش توجه اصلی به حوزه‌های موضوعی بوده است و سعی شده مباحث مربوطه جایگزین مباحث کمی علم‌سنجی نظیر پرکارترین نویسنده، پراستنادترین نویسنده، سازمان، کشور و نظایر آن گردد. اغلب پژوهش‌های قبلی از پایگاه وب‌آوساینس و اسکوپوس برای جمع‌آوری داده‌ها استفاده کرده‌اند. دورهٔ زمانی، انواع منابع موردبررسی، دامنه موضوعی و نرم‌افزار مورداستفاده در پژوهش‌ها متنوع بوده است. بااین‌حال، نرم‌افزار ووس ویور به‌عنوان یکی از شاخص‌ترین نرم‌افزارها، در کنار سایر نرم‌افزارها برای تحلیل هم‌رخدادی به کار گرفته‌شده است. تنوع کلیدواژه‌ها برای جستجو و گردآوری منابع در تعداد زیادی از پژوهش‌ها محدود بوده است. به‌علاوه در اغلب پژوهش‌ها از فهرست لغات و یا فهرست لغات بازدارنده استفاده‌نشده است. در این مطالعه، برای ایجاد یکدستی، تنوع نگارش کلمات، جمع یا مفرد بودن آن‌ها، اختصارات و نظایر آن، فهرست لغات اصطلاح‌نامه در نظر گرفته شد و فهرست واژگان بازدارنده نیز تهیه و در افزونه تحت وب بیبلیوشاینی مورداستفاده قرار گرفت.

روش‌شناسی پژوهش

با توجه به هدف پژوهش که شناخت حوزه‌های موضوعی و گرایش‌های نوظهور، محرک، ضروری و سیر تحول موضوع‌ها در حوزه امنیت سایبری در حیطهٔ تخصصی بانکداری است، با رویکرد علم‌سنجی به تحلیل کلیدواژه‌های مقاله‌ها پرداخته شد. برای این منظور، از تحلیل هم‌رخدادی، تحلیل شبکه اجتماعی و شاخص‌های مرکزیت و چگالی استفاده گردید.

جامعه پژوهش شامل کلیه مقاله‌های منتشرشده در حوزه امنیت سایبری در بانک‌ها در پایگاه اطلاعاتی وب‌آوساینس از سال ۲۰۰٤ تا ۲۰۲٤ است و با توجه به این‌که شروع نمایه شدن این مقاله‌ها در پایگاه مورداشاره از سال ۲۰۰٤ بود، این بازهٔ زمانی برای پژوهش انتخاب شد. جستجو در تاریخ ۲۸ اسفند ۱٤۰۳ انجام و داده‌ها گردآوری شدند. دلیل انتخاب این پایگاه وجود مقالات با کیفیت جهانی و مقالات آی‌اِس‌آی در آن است که به‌عنوان مقالات هسته شناخته می‌شوند. با جستجو در فیلد Topic این پایگاه و با استفاده از کلیدواژه‌های مترادف و با نگارش‌های متفاوت، کلیه مدارک مرتبط بازیابی شدند. همچنین، با توجه به حساسیت و اهمیت کلیدواژه‌های جستجو و با

مشورت متخصصان حوزه امنیت سایبری کلیه کلیدواژه‌های مرتبط در نظر گرفته شدند. از میان منابع بازیابی شده، تنها مقاله‌های انگلیسی‌زبان و در تمامی سال‌های مورد بررسی، به‌جز سال ۲۰۲۵ در جستجو مدنظر قرار گرفتند. دلیل عدم انتخاب مقاله‌های سال ۲۰۲۵ این است که تنها دو ماه از شروع این سال سپری‌شده است و این مقاله‌ها در این مدت کوتاه چه ازنظر کمیت و چه ازنظر استنادی، قابل‌مقایسه با دیگر مقالات نیستند. راهبرد جستجو در بخش جستجوی پیشرفته پایگاه عبارت است از:

TS=("Cybersecurity" OR "cyber security" OR "Cyber-security" OR "information security" OR "data security" OR "data-security" OR "network security" OR "financial cybersecurity" OR "cyber attack" OR "cyber threat" OR "fraud detection" OR "phishing" OR "ransomware" OR "identity theft" OR "data breach" OR "risk management") AND TS=("bank" OR "banks" OR "banking sector" OR "financial institutions" OR "digital banking" OR "online banking" OR "fintech" OR "financial institution" OR "digital payment" OR "online banking") and English (Languages) and Article (Document Types) and 2025 (Exclude – Publication Years) and Retracted Publication or Proceeding Paper or Early Access or Book Chapters (Exclude – Document Types)

درمجموع ۲۷۷۰ مدرک بازیابی شد که برخی از آن‌ها به دلیل تکراری بودن حذف گردیدند. تعدادی از مدارک نیز تاریخ نشر آن‌ها مربوط به سال ۲۰۲۵ بود که آن‌ها نیز از مجموعه مدارک حذف شدند و تعداد نهایی مدارک مورد تحلیل به ۲۷۲۰ رسید.

به دلیل اینکه پژوهشگران به اطلاعات کامل هر یک از مدارک بازیابی شده نیاز داشتند، کل اطلاعات مرتبط با هر رکورد به همراه منابع و مأخذ آن‌ها با فرمت txt. دانلود شدند. سپس به‌منظور تحلیل داده‌ها از افزونه تحت وب بیبلیوشاینی و نرم‌افزار ووس ویور استفاده شد. با توجه به اینکه بیبلیوشاینی کل داده‌ها را در یک فایل می‌پذیرد، داده‌های جمع‌آوری‌شده در یک فایل تجمیع شدند. افزونه تحت وب بیبلیوشاینی به‌واسطه نصب و اجرای نرم‌افزار آر در مرورگر قابل فراخوانی خواهد بود. به‌منظور استفاده از آن باید متناسب با سیستم‌عامل خود و نسخه نرم‌افزار آر کدهایی را در برنامه آر اجرا کرد تا امکان استفاده از این افزونه مهیا شود. بیبلیوشاینی می‌تواند به‌عنوان جایگزین برخی نرم‌افزارهای حوزه علم‌سنجی استفاده شود، زیرا ترسیم بسیاری از نقشه‌ها و محاسبه شاخص‌ها را می‌توان به‌واسطه این نرم‌افزار انجام داد.

درنهایت، پژوهشگران اقدام به ساخت فهرست لغات به‌منظور یکدستی و فهرست لغات بازدارنده به‌صورت جداگانه کردند تا در بستر بیبلیوشاینی مورداستفاده قرار گیرد. با توجه به این‌که فهرست کلیدواژه‌های بازدارنده و مترادف از قبل مشخص نیست و چنین فهرستی در هر حوزه موضوعی ممکن است متفاوت باشد، ابتدا تمام کلیدواژه‌ها با استفاده از نرم‌افزار ووس ویور استخراج و سپس از فرمت txt. به xlsx. تبدیل شدند. این اصطلاح‌نامه شامل تبدیل اختصارات به نوع کامل کلمه، تبدیل کلیدواژه‌های جمع به مفرد و نیز کلیدواژه‌هایی که چند شکل نگارش دارند به یک نوع نگارش و نظایر آن بود.

یافته‌های پژوهش

پاسخ به پرسش اول پژوهش. روند انتشارات و استنادات پژوهش‌های انجام‌شده در حوزهٔ امنیت سایبری در بانک‌ها چگونه بوده است؟

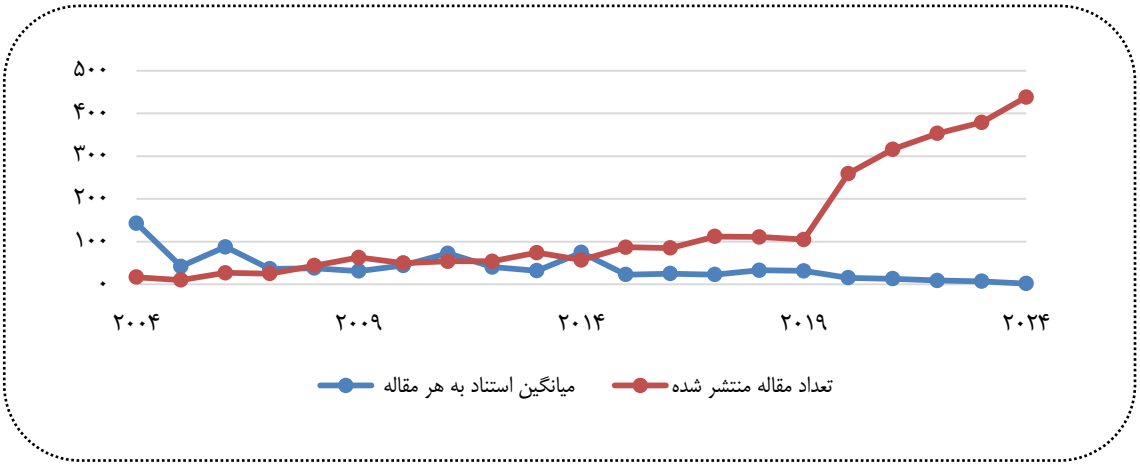
کلیات مدارک موردبررسی نشان می دهد که ۲۷۲۰ مقاله منتشرشده در این حوزه در ۱۰۳۳ مجله منتشرشده است. نزدیک به ۳۰ درصد از این آثار با همکاری نویسندگان بین‌المللی نگارش یافته‌اند. علاوه بر این، تعداد زیادی از

پژوهش‌های حوزۀ امنیت سایبری در محیط بانکی با مشارکت گروهی از پژوهشگران انجام‌شده است. همچنین، هر مدرک به‌طور متوسط ۱۹ استناد دریافت کرده است. با توجه به نرخ رشد سالانه مقاله‌ها، می‌توان نتیجه گرفت که این حوزه ازجمله موضوع‌های مهم و پژوهشی محسوب می‌شود.

شکل ۱. توصیف مجموع مقاله‌های حوزه امنیت سایبری در بانک

نمودار ۱، تعداد مقاله‌های منتشرشده در هرسال (رنگ نارنجی) و متوسط میزان استناد به مقاله‌ها (رنگ آبی) را در هرسال نشان می‌دهد. از سال ۲۰۰٤ تا ۲۰۲٤ تعداد مقاله‌ها در این حوزه رشد تصاعدی داشته است. از سال ۲۰۲۰ به بعد تعداد مقاله‌ها از ۲۵۹ به ٤۳۸ مقاله در سال ۲۰۰٤ رسیده که نشان می‌دهد اهمیت امنیت در فضای دیجیتالی در محیط بانک‌ها روزبه‌روز بیش‌تر شده است.

همچنین نگاهی به روند استنادات در سال‌های مختلف نشان می‌دهد که میانگین استناد به ازای هر مقاله در سال ۲۰۰٤ بیش از دیگر سال‌ها (۱٤۳) بوده است. میانگین استناد به ازای هر مقاله روند افزایشی و کاهشی داشته است. بعدازآن، سال ۲۰۰٦ و سال ۲۰۱٤ بیش‌ترین میانگین استناد به ازای هر مقاله را به خود اختصاص داده‌اند.



نمودار ۱. روند انتشارات و متوسط میزان استناد به مقاله‌ها در حوزه امنیت سایبری در بانک‌ها

به‌منظور تعدیل تأثیر سال انتشار مقاله بر میزان دریافت استناد از شاخص میانگین استناد سالانه بـه ازای هـر مقالـه استفاده شد. فرمول محاسبه این میانگین به شرح زیر است:

تعداد کل استنادها/(تعداد مقاله‌ها× تعداد سال‌های سپری‌شده از زمان انتشار)

با توجه به جدول ۱، سال‌های ۲۰۰٤، ۲۰۱٤، ۲۰۱۱ و ۲۰۱۹ بالاترین میانگین استناد سالانه به ازای هر مقالـه را بـه خود اختصاص داده‌اند. در میان مقاله‌های موردبررسی، مقالهٔ مربوط به *توپولوژی شبکه تجزیه واریانس‌ها: اندازه‌گیـری میزان اتصال شرکت‌های مالی*[1] از سوی دیبولد و ییلماز[2] (۲۰۱٤) دارای بیشترین استناد (۲٦۰۵ استناد) اسـت. بعـدازآن مقاله‌ای با عنوان *ارزش در معرض ریسک خود رگرسیونی شرطی با استفاده از رگرسیون چارکی*[3] به نویسـندگی اِنگِـل و منگلنیس[4] (۲۰۰٤) توانسته ۱۲۲٦ استناد دریافت کند.

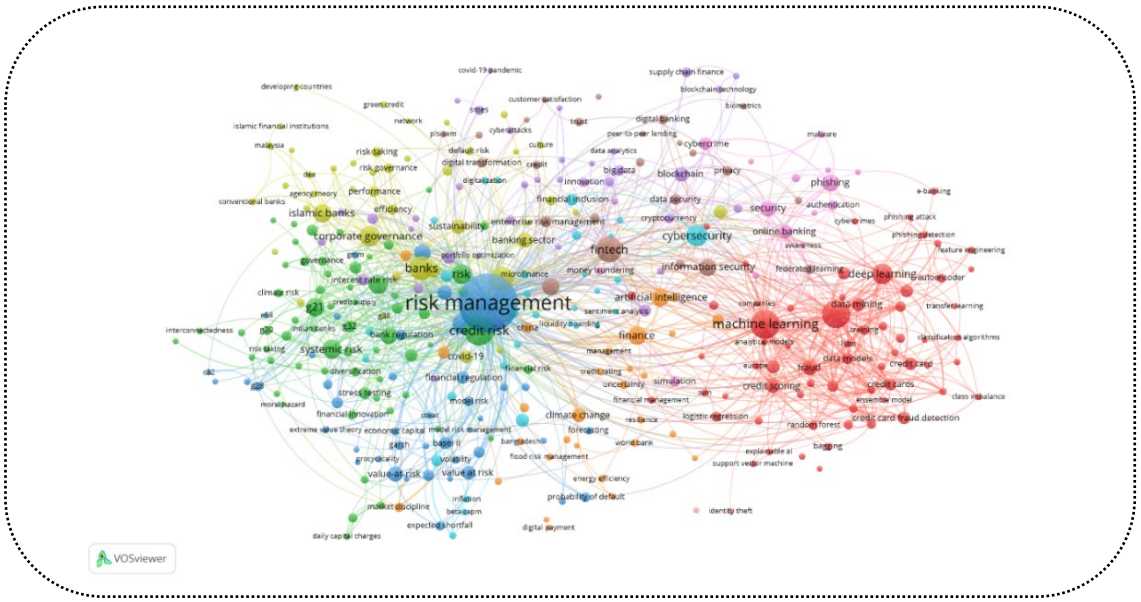
جدول ۱. میانگین استناد سالانه به مقاله‌ها

سال انتشار	تعداد سال‌های قابل استناد	میانگین استناد سالانه به ازای هر مقاله
۲۰۰٤	۲۲	٦.۵۱
۲۰۰۵	۲۱	۲
۲۰۰٦	۲۰	٤.۳۸
۲۰۰۷	۱۹	۱.۹۱
۲۰۰۸	۱۸	۲.۱۰
۲۰۰۹	۱۷	۱.۸۳
۲۰۱۰	۱٦	۲.۷۷
۲۰۱۱	۱۵	٤.۸٦
۲۰۱۲	۱٤	۲.۸۹
۲۰۱۳	۱۳	۲.٤۵
۲۰۱٤	۱۲	٦.۲۱
۲۰۱۵	۱۱	۲.۱
۲۰۱٦	۱۰	۲.۵۱
۲۰۱۷	۹	۲.۵۵
۲۰۱۸	۸	٤.۱۲
۲۰۱۹	۷	٤.۵۱
۲۰۲۰	٦	۲.۵۵
۲۰۲۱	۵	۲.٦۵
۲۰۲۲	٤	۲.۲٦
۲۰۲۳	۳	۲.۳۸
۲۰۲٤	۲	۰.۹٤

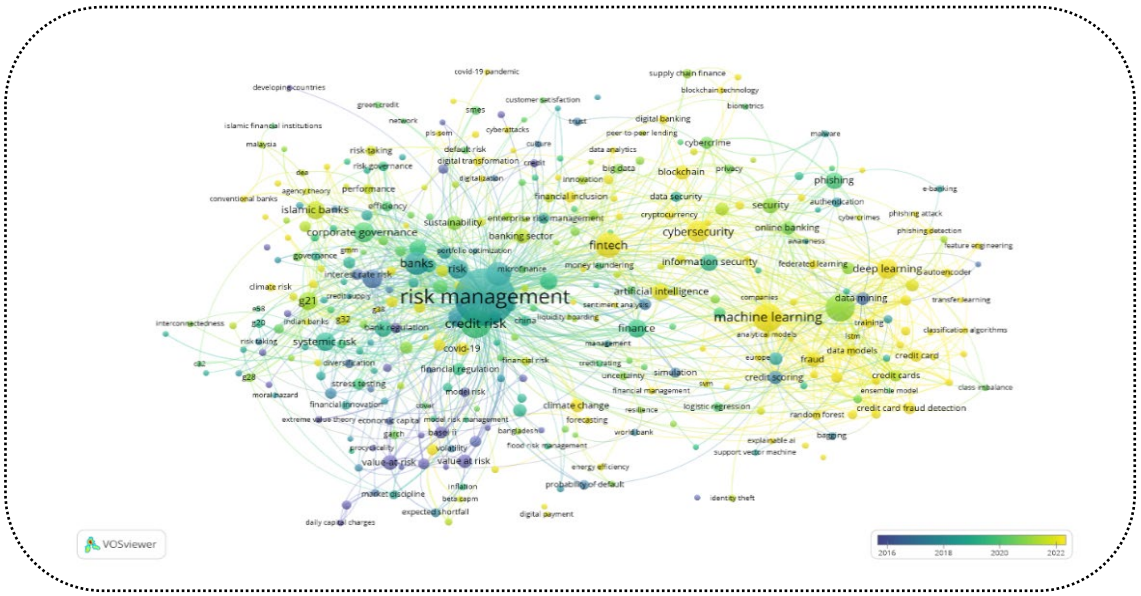
1 .On The Network Topology of Variance Decompositions: Measuring the Connectedness of Financial Firms
2. Diebold and Yilmaz
3 .CAVIAR: Conditional Autoregressive Value at Risk by Regression Quantiles
4 . Engle & Manganellis

پاسخ به پرسش دوم پژوهش. شبکه هم‌رخدادی واژگان در حوزهٔ امنیت سایبری در بانک‌ها چگونه است؟

شبکه هم‌رخدادی واژه‌ها با استفاده از کلیدواژه‌های نویسندگان ترسیم شد. شرط ورود به شبکه حداقل پنج رخداد در نظر گرفته شد و درمجموع ۳۵۲ کلیدواژه وارد نقشه شدند. بر اساس تعداد فراوانی در مقاله‌ها، کلیدواژه مدیریت ریسک (٤٥٦ رخداد)، یادگیری ماشین (۱۱۳ رخداد)، ریسک اعتباری (۱۱۷ رخداد)، کشف کلاهبرداری (۱۰٤ رخداد) بیش‌ترین تعداد رخداد را به خود اختصاص داده‌اند. بعدازآن، واژه‌های بانکداری، فناوری مالی، بانک، جی ۲۱، یادگیری عمیق و کلاهبرداری قرار دارند. بررسی قدرت ارتباطی پیوندها نیز نشان می‌دهد که موضوع‌های بیان شده به همان ترتیب دارای بیش‌ترین قدرت ارتباطی هستند (شکل ۲).



شکل ۲. شبکه هم‌رخدادی واژه‌ها در حوزه امنیت سایبری در بانک‌ها



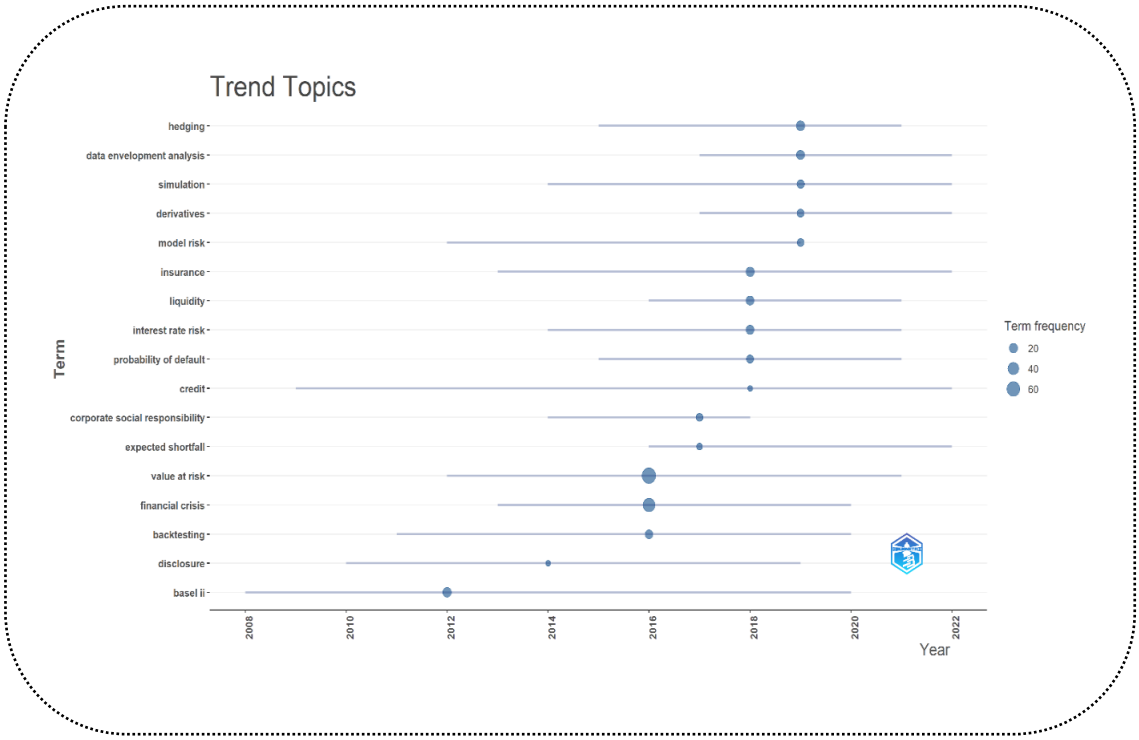
شکل ۳. نقشه مصورسازی پوششی حوزه امنیت سایبری در بانک‌ها

پاسخ به پرسش سوم پژوهش. تحول موضوع‌های پرتکرار در دوره‌های زمانی مختلف چگونه است؟

به‌منظور آگاهی از مهم‌ترین موضوعات پرکاربرد در دوره‌های زمانی مختلف و سیر تحول آن‌ها نمودار روندهای موضوعی ترسیم شد. برای نشان دادن موضوعات مهم و پرتکرار دو بازهٔ زمانی در نظر گرفته شد. نخست موضوعاتی که از ابتدای سال ۲۰۰٤ تا سال ۲۰۱۹ (شکل ٤) ازجمله موضوعات پرتکرار بوده‌اند و دورهٔ دوم، تحولات سال‌های اخیر از سال ۲۰۲۰ تا ۲۰۲٤ (شکل ٥) در نظر گرفته شد. دلیل آن‌که نمودار نخست از سال ۲۰۰۸ شروع‌شده آن است که با توجه به اهمیت تکرار کلیدواژه‌ها برای ورود به نمودار در فاصله سال‌های ۲۰۰٤ تا ۲۰۰۸ موضوعاتی به‌عنوان نقطه اوج یا محبوب وجود نداشته است.

خط افقی نقطه شروع زمانی استفاده از کلیدواژه در مقاله‌ها تا نقطهٔ پایانی استفاده از آن کلیدواژه پرتکرار را نشان می‌دهد. دایره‌های روی خط افقی اوج محبوبیت آن کلیدواژه را نشان می‌دهند. هر چه اندازه دایره بزرگ‌تر باشد، محبوبیت آن کلیدواژه بر اساس فراوانی تکرار آن از سوی پژوهشگران بیش‌تر بوده است.

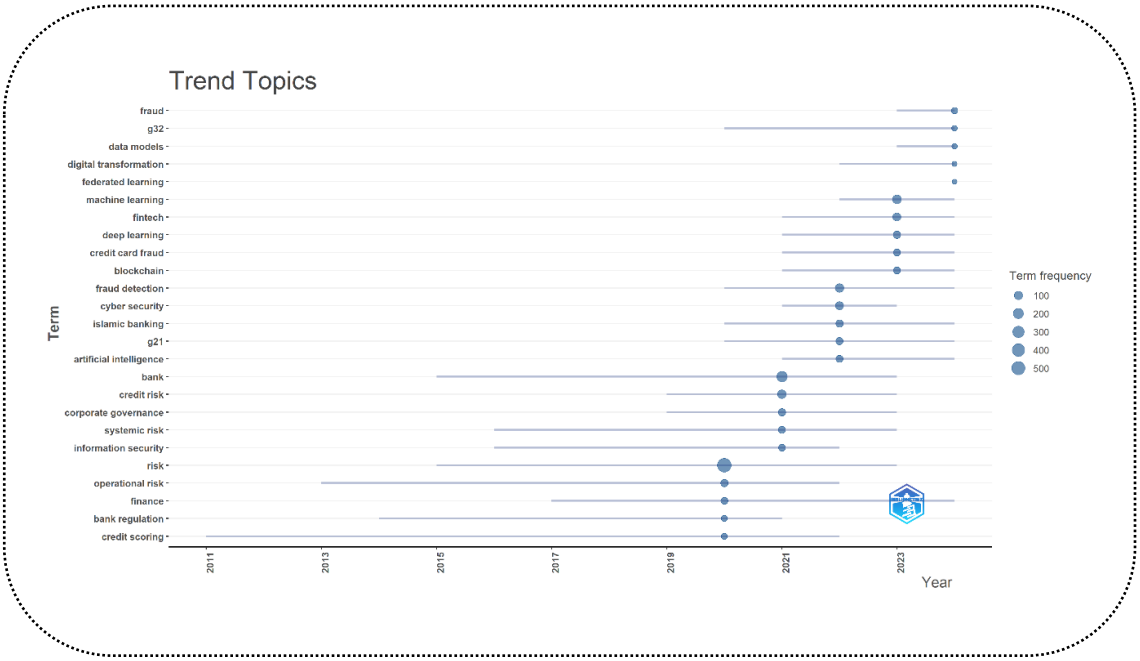
دو موضوع حداکثر زیان احتمالی[1] با ۷۲ مورد تکرار در مقالات و بحران مالی با ٤۹ مورد تکرار در مقالات، ازجمله روندهای موضوعی محبوب مقاله‌های این حوزه در سال ۲۰۱٦ بوده است. شروع توجه به موضوع حداکثر زیان احتمالی از سال ۲۰۱۲ بوده و تا پایان سال ۲۰۱۹ نیز ادامه داشته است. موضوع بحران مالی از سوی پژوهشگران از سال ۲۰۱۳ موردتوجه قرار گرفت. موضوع مقررات و چارچوب‌های بین‌المللی برای اندازه‌گیری و مدیریت ریسک در بانک‌ها از سال ۲۰۰۸ نیز موردتوجه بوده است، اما اوج محبوبیت آن در سال ۲۰۱٦ رخ‌داده است. اقدامات مالی برای کاهش ریسک نیز با فراوانی ۲۱ از سال ۲۰۱٥ به آن پرداخته‌شده و دارای بیشترین محبوبیت در سال ۲۰۱۹ است.



شکل ٤. حوزه‌های موضوعی محبوب از سال ۲۰۰٤ تا ۲۰۱۹

1. Value at Risk (VaR)

موضوعات کلاهبرداری، مدل‌های داده‌ای، یادگیری یکپارچه و تحول دیجیتال ازجمله روندهای موضوعی در سال ۲۰۲٤ بوده‌اند. در سال ۲۰۲۳ روندهای موضوعی به یادگیری ماشین، فناوری مالی، کلاهبرداری کارت اعتباری و بلاک چین مربوط است. در سال ۲۰۲۲ کشف کلاهبرداری، امنیت سایبری، بانکداری اسلامی، یادگیری عمیق و هوش مصنوعی، ازجمله موضوعات پرتکرار پژوهشگران بوده‌اند. سال ۲۰۲۱ موضوع‌های بانک، ریسک اعتباری، حکمرانی مشارکتی، ریسک نظام‌مند و امنیت اطلاعات به اوج محبوبیت در پژوهش‌ها رسیدند. درنهایت، در سال ۲۰۲۰ موضوع‌های ریسک، ریسک عملیاتی، سرمایه، قوانین بانکی و امتیازدهی اعتباری در نقطه اوج توجه قرار داشتند (شکل ۵).



شکل ۵. حوزه‌های موضوعی محبوب از سال ۲۰۲۰ تا ۲۰۲٤

پاسخ به پرسش چهارم پژوهش. در نقشه موضوعی حوزهٔ امنیت سایبری در بانک‌ها موضوع‌های محرک، تخصصی، ضروری و نوظهور چه موضوع‌هایی هستند؟

این نمودار دارای دو محور چگالی و مرکزیت است. چگالی نشان‌دهندهٔ قدرت ارتباط بین نتایج پژوهشی موضوعات (تم‌ها) منفرد است. هر چه چگالی بیشتر باشد، آن موضوع به بلوغ بیشتری رسیده است. مرکزیت میزان قدرت ارتباط بین پژوهش‌ها را نشان می‌دهد. هر چه میزان مرکزیت بیشتر باشد، احتمال این‌که آن موضوع موردتوجه بیشتری در پژوهش‌ها قرار گیرد بیشتر است؛ یعنی ارتباط بین موضوعات یک خوشه با خوشه دیگر بیشتر است و در کانون توجه قرار دارد (Zhang, 2024).

با استفاده از الگوریتم واک ترپ[1] برای خوشه‌بندی کلیدواژه‌ها، چهار خوشهٔ اصلی شناسایی شد که عبارت‌اند از: خوشهٔ ریسک، خوشهٔ یادگیری ماشین، خوشهٔ فناوری مالی و درنهایت خوشهٔ حداکثر زیان مالی.

نمودار به چهار بخش اصلی تقسیم‌شده که عبارت‌اند از:

1 .Walktrap

۱. ناحیه محرک و پیشران[1] بالا-راست

این ناحیه در سمت راست‌بالا قرار دارد و نشانگر موضوعاتی است که تأثیرگذاری و تراکم بالایی دارند. موضوعات این ناحیه به‌عنوان هسته و محرک اصلی پژوهش شناخته می‌شوند و ازنظر ساختار و ارتباطات داخلی بین موضوعی و ارتباط با سایر موضوع‌ها غنی هستند. همچنین، این موضوعات به‌شدت تأثیرگذارند. این خوشه با عنوان خوشهٔ یادگیری ماشین شامل موضوعاتی نظیر تشخیص کلاهبرداری، یادگیری عمیق، کلاهبرداری کارت اعتباری، فیشینگ است. خوشه‌هایی که با موضوعات بسیاری در این حوزه دارای ارتباطات داخلی و غنی هستند و نیز جز موضوعات پراستناد این حوزه به شمار می‌روند.

۲. ناحیه ضروری[2] پایین-راست

این ناحیه در سمت راست پایین قرار دارد و شامل موضوعاتی است که تأثیرگذاری بالا اما تراکم یا توسعه‌یافتگی پایینی دارند. این موضوعات پراستناد و مهم‌اند، اما ارتباطات داخلی کمتری دارند و بیشتر به‌عنوان پایه‌های اصلی پژوهش شناخته می‌شوند. موضوعات مربوط به این چارک نمودار، معمولاً ازجمله موضوعات داغ یا روندهای پژوهشی به شمار می‌آیند (Zhang, 2024). خوشه‌ی فناوری مالی شامل موضوعات فناوری مالی، امنیت سایبری، هوش مصنوعی، سرمایه و امنیت اطلاعات است. این موضوعات بلوغ و پختگی کمی دارند، اما در حوزه بسیار مهم هستند.

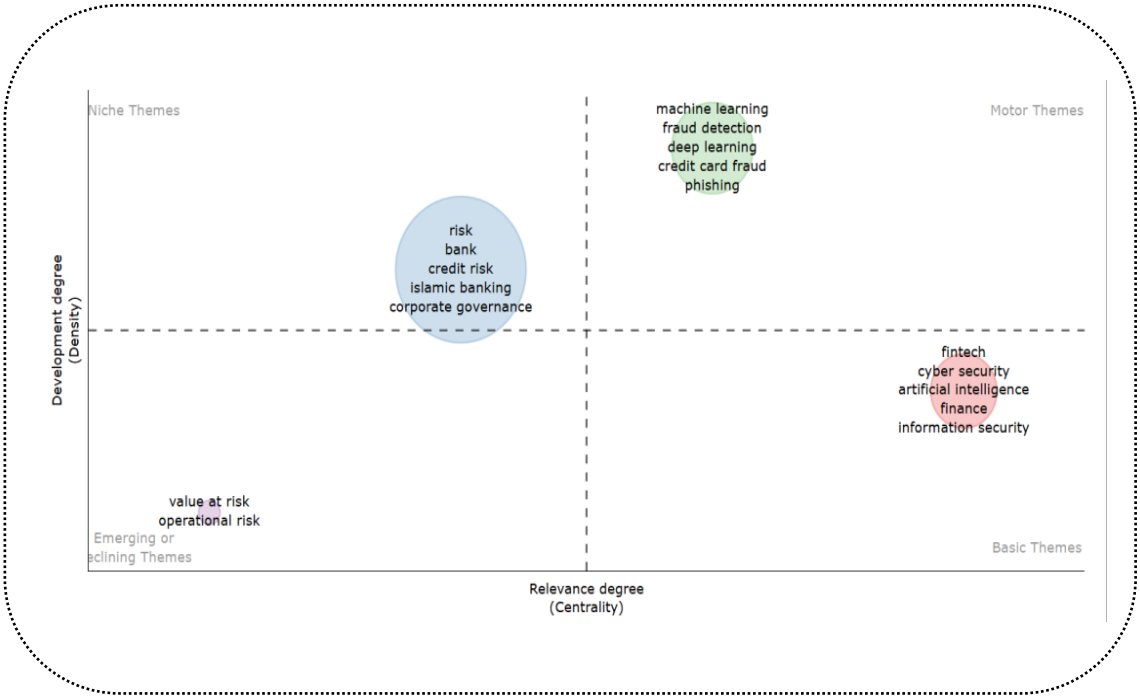
۳. ناحیه نوظهور یا رو به افول[3] پایین- چپ

این ناحیه در سمت چپ پایین قرارگرفته و شامل موضوعاتی است که تأثیرگذاری و تراکم پایینی دارند. خوشه‌های مربوط به این قسمت به دو بخش قابل‌تقسیم‌اند: موضوعاتی که به‌تازگی مطرح‌شده‌اند و پژوهش‌های کمی در باره آن‌ها انجام‌شده است یا موضوعاتی که در حال فراموشی هستند و در آن حوزه موضوعی قابل‌طرح نیستند. ازاین‌رو، این موضوعات بیشتر در حال رشد یا در مرحله گذار هستند و ممکن است به‌مرورزمان به ناحیه موتور انتقال یابند یا از اهمیت‌شان کاسته شود. برای نمونه، خوشهٔ حداکثر زیان مالی که در حوزهٔ بانکداری قرار دارد شامل موضوعاتی نظیر حداکثر زیان مالی و ریسک عملیاتی است. با توجه به این خوشه و نیز نقشهٔ مصورسازی پوششی می‌توان استنباط کرد که خوشه حداکثر زیان مالی در مرحله کاهش توجه قرار داد.

٤. ناحیه تخصصی و خاص[4] بالا- چپ:

این ناحیه در سمت چپ بالا قرار دارد و شامل موضوعاتی با تراکم بالا اما تأثیرگذاری پایین است. این موضوعات معمولاً پژوهش‌های خاص و تخصصی هستند که ممکن است تنها برای گروه خاصی از پژوهشگران اهمیت داشته باشند. خوشهٔ ریسک شامل موضوعات ریسک، بانک، ریسک اعتباری، بانکداری اسلامی و حکمرانی مشارکتی، نشان‌دهندهٔ موضوعات خاص حوزه امنیت سایبری در بانک‌ها است. موضوعات مرتبط با این خوشه موضوعاتی هستند که طیف زیادی از پژوهش‌ها را به خود اختصاص داده‌اند و گروه خاصی از پژوهشگران به پژوهش در این حوزه‌ها مشغول‌اند (شکل ٦).

1 . Motor Themes
2 . Basic Themes
3 . Emerging or Declining Themes
4. Niche Themes



شکل ٦. خوشه‌های موضوعی محرک، ضروری، تخصصی، نوظهور یا رو به افول

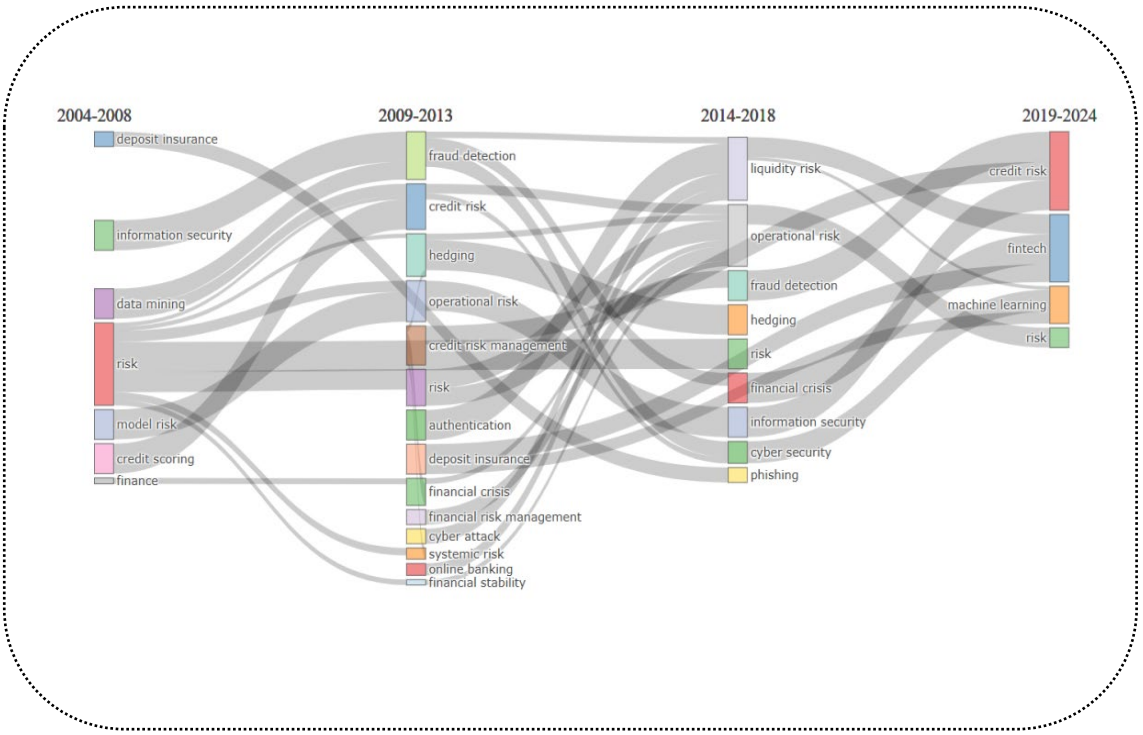
پاسخ به پرسش پنجم پژوهش. روندهای موضوعی مهم و پرتکرار و موضوع‌های محرک، تخصصی، ضروری و نوظهور یا رو به افول در دوره‌های زمانی مختلف چه موضوع‌هایی بوده‌اند؟

برای بررسی روند تاریخی موضوعات، چهار دورهٔ زمانی بر اساس تاریخ نشر مقالات انتخاب شد (شکل ۷). دورهٔ اول مربوط به سال‌های ۲۰۰٤ تا ۲۰۰۸ است و موضوعات اصلی شامل بیمه سپرده‌ها، امنیت اطلاعات، داده‌کاوی، ریسک، ریسک مدلی، امتیازدهی اعتباری و سرمایه بود. دورهٔ دوم از سال ۲۰۰۹ تا ۲۰۱۳، شامل موضوعات کشف کلاهبرداری، ریسک اعتباری، پوشش ریسک، ریسک عملیاتی، مدیریت ریسک اعتباری، ریسک، احراز هویت، بیمه سپرده‌ها، بحران مالی، مدیریت ریسک مالی، حمله سایبری، ریسک نظام‌مند، بانکداری پیوسته و ثبات مالی بودند. دورهٔ سوم از سال ۲۰۱٤ تا ۲۰۱۸ به موضوعات ریسک نقدینگی، ریسک عملیاتی، کشف کلاهبرداری، احراز هویت، ریسک، بحران مالی، امنیت اطلاعاتی، امنیت سایبری و فیشینگ پرداخته و درنهایت دورهٔ چهارم از سال ۲۰۱۹ تا ۲۰۲٤ موضوعات اصلی به سمت ریسک اعتباری، فناوری مالی، یادگیری ماشین و ریسک گرایش یافته است.

در اوایل شکل‌گیری پژوهش‌های امنیت سایبری در بانک‌ها، مسئله کلیدی عمدتاً مربوط به ریسک کلی بود که در سال‌های بعد این موضوع جزئی‌تر شده است. موضوع اصلی پژوهش در فاصله سال‌های ۲۰۰۹ تا ۲۰۱۳ موضوع کشف کلاهبرداری بوده است. این امر نشان می‌دهد که در سال‌های موردبررسی، مسئله فعالیت‌های مشکوک، فریبنده و دسترسی‌های غیرمجاز ازجمله دغدغه‌های اصلی آن دوره بوده است. این موضوع در دورهٔ بعد (۲۰۱٤ تا ۲۰۱۸) به موضوعات تخصصی‌تر نظیر ریسک نقدینگی، بحران مالی و امنیت سایبری تبدیل‌شده است. در فاصله سال‌های ۲۰۰۹ تا ۲۰۱۳ نسبت به سال‌های قبل و بعد آن شاهد ظهور موضوعات تخصصی‌تر بیشتری هستیم. در این دوره مفهوم بانکداری پیوسته موردتوجه قرار گرفت و مفاهیمی که به‌صورت خاص به انواع ریسک‌ها در محیط بانکی می‌پردازند نظیر ریسک اعتباری، ریسک عملیاتی، مدیریت ریسک و نظایر آن به‌صورت جزئی‌تر موردتوجه قرار گرفتند.

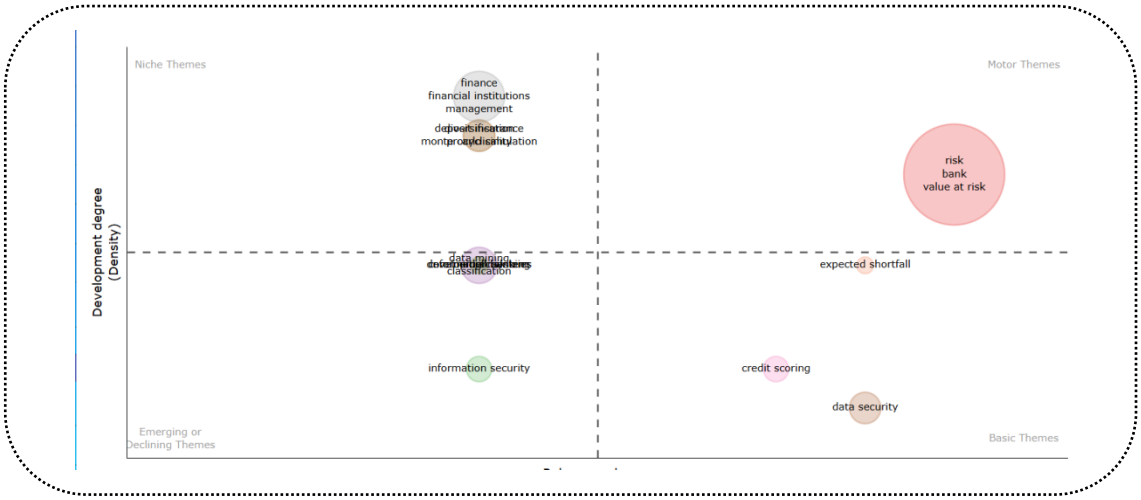
در فاصله سال‌های ۲۰۱٤ تا ۲۰۱۸، ریسک نقدینگی به‌عنوان مهم‌ترین موضوع معرفی شد که از سه مفهوم احراز هویت، حمله سایبری و بانکداری پیوسته در سال‌های ۲۰۰۹ تا ۲۰۱۳ نشأت گرفته است. می‌توان این‌طور نتیجه گرفت که چنانچه احراز هویت مشتریان بانک‌ها دچار اختلال گردد یا به‌واسطهٔ حمله سایبری هکرها به اطلاعات مشتریان دسترسی پیدا کنند، احتمال ریسک نقدینگی وجود دارد و این امر باوجود اهمیت بانکداری پیوسته، روزبه‌روز بیشتر خواهد شد. به‌علاوه در این دوره شاهد اهمیت موضوع امنیت در فضای دیجیتالی در بانکداری هستیم.

در دورهٔ چهارم، در سال‌های ۲۰۱۹ تا ۲۰۲٤، مفاهیم اصلی بیشتر به سمت فناوری تمایل یافته و مفهوم یادگیری ماشین به‌عنوان یک مفهوم جدید در این سال‌ها ظهور کرده است. بااین‌حال، هنوز ریسک اعتباری به‌عنوان موضوع اصلی در این حوزه مطرح است. در این دوره شاهد حضور فناوری‌های هوشمند و نوین در حوزهٔ بانک و بانکداری هستیم.



شکل ۷. روندهای موضوعی مهم و پرتکرار در بازه‌های زمانی مختلف و تحول آن‌ها

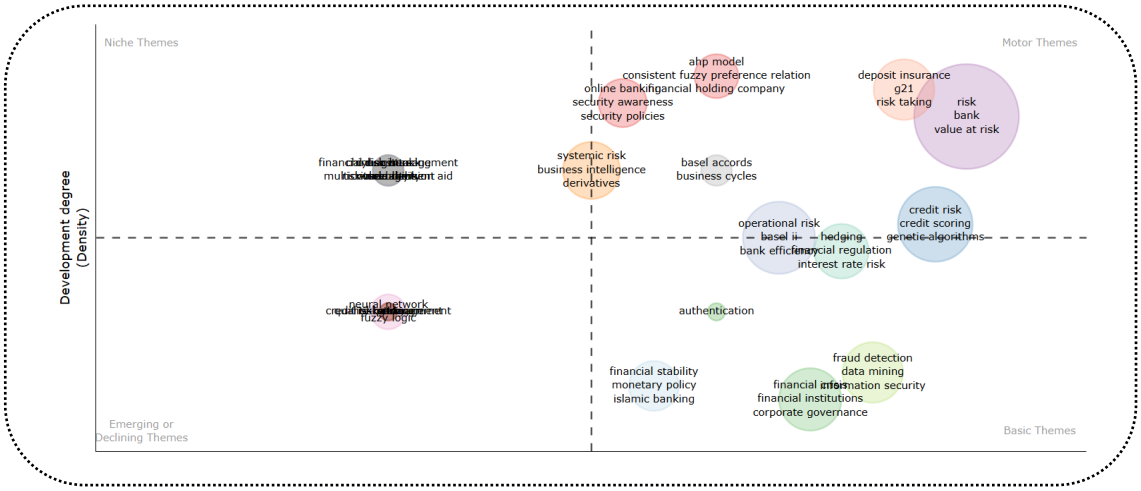
در سال‌های ۲۰۰٤ تا ۲۰۰۸ خوشهٔ داده‌کاوی، بانکداری تجاری و امنیت اطلاعات، ازجمله موضوعات نوظهور در حوزه امنیت سایبری در بانک‌ها هستند. خوشهٔ امنیت داده، امتیازدهی اعتباری و متوسط ضرر دهی بانک‌ها، ازجمله موضوعات کاربردی و ضروری دورهٔ مذکور محسوب می‌شدند. این موضوعات، ازجمله موضوعات اساسی این دوره به شمار می‌آیند، اما هنوز توسعه‌نیافته‌اند. خوشهٔ ریسک و موضوعات مرتبط با آن، به‌عنوان خوشه پیشران و محرک در این سال‌ها محسوب می‌شود. خوشهٔ سرمایه شامل موضوعاتی مانند مؤسسه‌های سرمایه‌ای، مدیریت و خوشه تنوع‌بخشی است که به‌عنوان موضوعات تخصصی از سوی برخی پژوهشگران موردتوجه قرارگرفته است. این موضوعات در سال‌های ابتدایی خود دارای ارتباط قوی با سایر خوشه‌های موضوعی نیستند، اما به آن‌ها به‌صورت عمیق‌تر پرداخته‌شده است (شکل ۸).



شکل ۸. روند تحول موضوعات در فاصله سال‌های ۲۰۰۴ تا ۲۰۰۸

تنوع و تعدد خوشه‌ها در سال‌های ۲۰۰۹ تا ۲۰۱۳ قابل‌توجه است، این امر به‌ویژه در حوزه‌های ضروری و محرک (پیشران) نمود بیشتری دارد. خوشه‌های موضوعی شبکه عصبی و خوشهٔ مدیریت ریسک اعتباری به‌عنوان خوشه‌های نوظهور در این دوره، در پژوهش‌های حوزه امنیت سایبری در محیط بانکی ظاهر می‌شوند. در این دوره مشاهده می‌شود که انواع ریسک‌ها نظیر ریسک اعتباری، ریسک سیستمی و ریسک عملیاتی، به‌عنوان خوشه‌های مجزا مطرح‌شده‌اند.

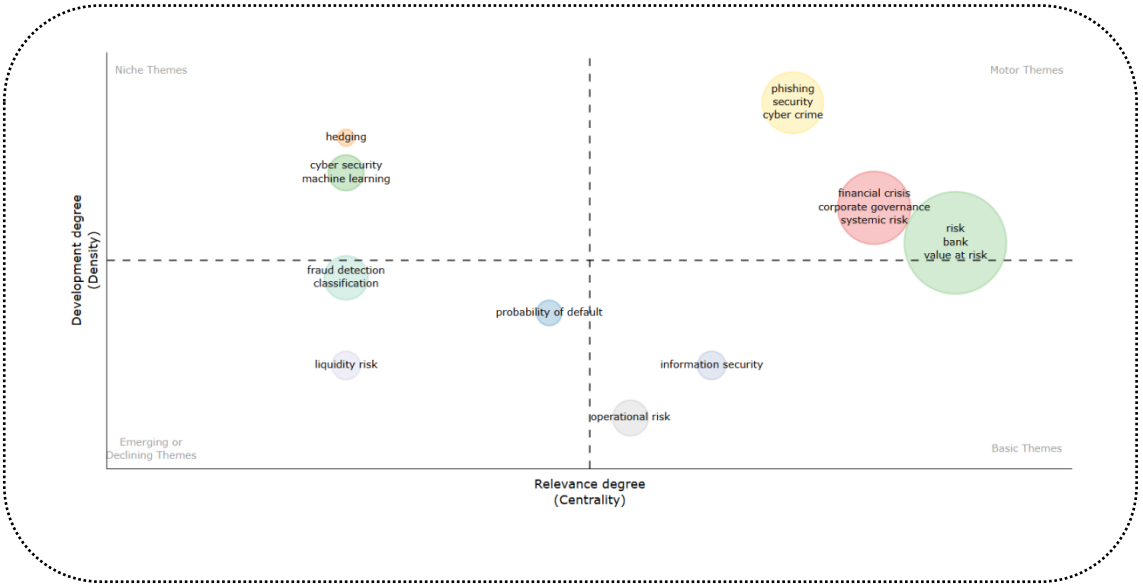
افزون بر این، خوشه‌های جدیدی به‌عنوان خوشه‌های محرک مطرح شدند، ازجمله: خوشهٔ بانکداری پیوسته، خوشهٔ احراز هویت، خوشهٔ بیمه سپرده‌گذاری، خوشهٔ مدل سلسله مراتبی، خوشهٔ توافق‌نامه‌های بازل (مقررات بین‌المللی برای مدیریت ریسک در بانک‌ها)، خوشهٔ پوشش ریسک.[1] این خوشه‌ها ازجمله خوشه‌های اصلی این دوره به‌عنوان موضوع‌های پیشران مطرح بودند. همچنین، خوشه‌هایی مانند پایداری سرمایه، بحران سرمایه، تشخیص کلاهبرداری و احراز هویت نیز در این زمان، به‌عنوان موضوعات ضروری و پایه‌ای مطرح شدند؛ موضوعاتی که میزان ارتباط آن‌ها با سایر خوشه‌ها بیشتر است (شکل ۹).



شکل ۹. روند تحول موضوعات در فاصله سال‌های ۲۰۰۹ تا ۲۰۱۳

1 . hedging

موضوع ریسک نقدینگی، ازجمله خوشه‌های نوظهور در دورهٔ سوم (۲۰۱٤ تا ۲۰۱۸) است. در این دوره، خوشهٔ کشف کلاهبرداری به ناحیهٔ موضوعی رو به افول وارد شد؛ به این معنا که این خوشهٔ در سال‌های موردبررسی، دیگر به‌عنوان یک موضوع پژوهشی مهم موردتوجه نبود. از سوی دیگر، خوشهٔ فیشینگ به‌عنوان یک خوشه جدید، پیشران و محرک، موردتوجه پژوهشگران قرارگرفته است (شکل ۱۰).



شکل ۱۰. روند تحول موضوعات در فاصله سال‌های ۲۰۱٤ تا ۲۰۱۸

تنوع موضوعی در سال‌های ۲۰۱۹–۲۰۲٤ نسبت به دو دوره قبل از آن کمتر شده است. خوشهٔ یادگیری ماشین و موضوعات آن به‌عنوان موضوع محرک و پیشران، خوشهٔ ریسک اعتباری به‌عنوان موضوع تخصصی، خوشهٔ ریسک به‌عنوان خوشهٔ رو به افول و خوشهٔ فناوری مالی به‌عنوان خوشهٔ ضروری مطرح است (شکل ۱۱).

شکل ۱۱. روند تحول موضوعات در فاصله سال‌های ۲۰۱۹ تا ۲۰۲٤

بحث و نتیجه‌گیری

اهمیت امنیت سایبری در بانک‌ها با توجه به حجم بالای داده‌های با ارزش و همچنین حفظ حریم شخصی افراد و اطلاعات آن‌ها در این مراکز، روزبه‌روز افزایش می‌یابد. اکثر پژوهش‌های حوزه امنیت سایبری و امنیت اطلاعات حاصل تعامل و همکاری گروهی است (Loan et al., 2022). نتایج این پژوهش نیز نشان داد درصد قابل‌توجهی از آثار منتشرشده در این حوزه به‌صورت گروهی نگارش یافته‌اند.

بررسی نقشهٔ مصورسازی پوششی با استفاده از نرم‌افزار ووس ویور گویای آن است که در سال‌های اخیر، اهمیت موضوعاتی مانند یادگیری ماشین، یادگیری عمیق، فناوری مالی و هوش مصنوعی در میان پژوهشگران افزایش‌یافته است. نتایج پژوهش‌های لون و همکاران (Loan et al., 2022) و شفچوک و مارتسنیوک (Shevchuk & Martsenyuk, 2024) در مورد یادگیری ماشین، با نتایج این پژوهش تطابق دارد. بااین‌حال، تفاوت‌هایی نیز با نتایج پژوهش‌های پورمددکار و همکاران (Pourmadadkar et al., 2024) و امت و همکاران (Omote et al., 2024) مشاهده می‌شود. این تفاوت‌ها می‌تواند به دلایلی مانند تمرکز بر موضوعات خاص‌تر در حوزهٔ امنیت سایبری (مانند سیستم‌های سایبری فیزیکی) در پژوهش پورمددکار و تفاوت سال‌های مطالعه (۲۰۱۰ تا ۲۰۱۹) در پژوهش امت و همکاران (Omote et al., 2024) باشد.

موضوع حداکثر زیان احتمالی و بحران مالی که ازجمله موضوع‌های محبوب در سال ۲۰۱٦ بوده‌اند، محبوبیت خود را بعدازآن سال‌ها ازدست‌داده‌اند. نگاهی به نقشهٔ مصورسازی پوششی کلیدواژه‌ها نیز این مسئله را تائید می‌کند.

ازجمله مهم‌ترین روندهای پژوهشی در سال ۲۰۲٤ در حوزه امنیت سایبری در بانک‌ها که به اوج محبوبیت خود رسیدند، می‌توان به موضوع کلاهبرداری اشاره کرد که با توجه به اهمیت روزافزون بانکداری اینترنتی و اپلیکیشن‌های تلفن همراه، این موضوع بیش‌ازپیش موردتوجه قرارگرفته است. همچنین، موضوع یادگیری یکپارچه در سال ۲۰۲٤ مطرح شد و در همان سال به اوج محبوبیت رسید. این نوع یادگیری یکی از تازه‌ترین و پیچیده‌ترین روش‌های یادگیری ماشین است که بدون ارسال داده، مدل‌ها آموزش می‌بینند. بحث یادگیری ماشین در سال ۲۰۲۳ نیز از موضوع‌های مهم بوده است. نتایج پژوهش شفچوک و مارتسنیوک (Shevchuk & Martsenyuk, 2024) در حوزه شبکهٔ عصبی و امنیت سایبری، منطبق با پژوهش حاضر است. آن‌ها نیز یادگیری ماشین را به‌عنوان پرطرفدارترین موضوع موردبررسی پژوهشگران معرفی کرده‌اند.

در سال‌های اولیه پژوهش در این حوزه (۲۰۰٤ تا ۲۰۰۸)، خوشه‌های امنیت اطلاعات، داده‌کاوی و بانکداری تجاری به‌عنوان مفاهیم اولیه و مهم پژوهش مطرح شدند. در دورهٔ دوم (۲۰۰۹ تا ۲۰۱۳) این خوشه‌ها وارد خوشه بزرگ‌تری مانند تشخیص کلاهبرداری شدند و از موضوعات نوظهور، به موضوعات ضروری پژوهش در این حوزه تبدیل شدند. ارتباط موضوعی خوشه‌هایی مانند داده‌کاوی، امنیت اطلاعات و تشخیص کلاهبرداری، با توجه به افزایش تمرکز بر این حوزه‌ها در محیط بانکداری، بیشتر شد. در دورهٔ سوم (۲۰۰۹ تا ۲۰۱۳)، خوشهٔ امنیت اطلاعات همچنان اهمیت خود را حفظ کرد، اما به‌عنوان هستهٔ اصلی مستقل و مهم در حوزه امنیت سایبری باقی ماند. نتایج پژوهش لون و همکاران (Loan et al., 2022) نیز نشان دادند که امنیت اطلاعات متداول‌ترین حوزه موضوعی موردبررسی در فاصله سال‌های ۲۰۱۱ تا ۲۰۲۰ در کنار سایر موضوعات نظیر امنیت، امنیت رایانه‌ای، حفظ محرمانگی و نظایر آن بوده است.

خوشهٔ امتیازدهی اعتباری که در بازهٔ زمانی ۲۰۰٤ تا ۲۰۰۸ ازجمله موضوعات ناحیهٔ ضروری محسوب می‌شد، در

فاصله سال‌های ۲۰۰۹ تا ۲۰۱۳ وارد خوشهٔ ریسک اعتباری گردید و در مرز بین ناحیهٔ ضروری و ناحیهٔ محرک قرار گرفت. این بدان معنی است که این موضوع، همراه با موضوعات مربوط به خوشه خود در این دورهٔ زمانی ازجمله موضوعات پویا و پیش‌رونده پژوهشی محسوب می‌شود. همچنین، این خوشه در عین ارتباط قوی با موضوعات داخل خوشهٔ خود، با خوشه‌های دیگر نیز در حال برقراری ارتباطات موضوعی مناسبی است. این امر نشان‌دهندهٔ آن است که ارتباط بین‌حوزه‌ای موضوعات در این خوشه‌ها با خوشه‌های دیگر در همین ناحیه افزایش‌یافته و احتمال شکل‌گیری موضوعات جدیدتر با ترکیب خوشه‌ها وجود دارد. خوشهٔ ریسک که شامل انواع ریسک‌ها مانند ریسک عملیاتی، بازار و اعتباری است، به‌عنوان خوشه محرک در دو دورهٔ زمانی ۲۰۰٤ تا ۲۰۰۸ و ۲۰۰۹ تا ۲۰۱۳ شناخته می‌شود؛ با این تفاوت که در دورهٔ دوم و در کنار تأثیرگذاری، بر میزان توسعه‌یافتگی این خوشه افزوده‌شده است. در دورهٔ بعدی (۲۰۱٤ تا ۲۰۱۸)، این خوشه در مرز بین ناحیهٔ پیشران و ناحیهٔ ضروری قرار می‌گیرد و از توسعه‌یافتگی آن در این دوره کاسته می‌شود. درنهایت، در دورهٔ چهارم، وارد ناحیهٔ نوظهور یا رو به افول می‌شود که به نظر می‌رسد به‌عنوان خوشه‌ای که به اشباع رسیده، در سال‌های ۲۰۱۹ تا ۲۰۲٤ مطرح‌شده است. تأثیر این خوشه هم ازنظر توسعه‌یافتگی و هم ازنظر تأثیرگذاری و ارتباط با سایر خوشه‌ها کم‌رنگ‌تر می‌شود.

خوشهٔ سرمایه که در فاصله زمانی ۲۰۰٤ تا ۲۰۰۸ به‌عنوان خوشهٔ تخصصی مطرح بود، در دورهٔ بعدی (۲۰۰۹ تا ۲۰۱۳) به خوشه‌های جزئی‌تر تقسیم شد که همگی ازجمله خوشه‌های ضروری حوزه امنیت سایبری محسوب می‌شوند. خوشه‌هایی نظیر بحران سرمایه، پایداری سرمایه و مدیریت ریسک سرمایه، ازجمله خوشه‌های خاص دورهٔ دوم محسوب می‌شوند.

خوشهٔ کشف کلاهبرداری که در فاصلهٔ زمانی ۲۰۰۹ تا ۲۰۱۳ به‌عنوان خوشهٔ ضروری مطرح بود، سپس به‌عنوان خوشه‌ای مستقل و مرکز اصلی در خوشهٔ موضوعی سال‌های ۲۰۱٤ تا ۲۰۱۸ معرفی شد، به‌عنوان خوشه‌ای رو به افول مطرح است. بااین‌حال، در دورهٔ چهارم ۲۰۱۹ تا ۲۰۲٤، در قالب بخشی از خوشهٔ یادگیری ماشینی، به‌عنوان موضوع پیشران این دوره ظاهر می‌شود. در این خوشه، موضوعات مرتبطی مانند یادگیری عمیق، شبکه‌های عصبی، کلاهبرداری کارت اعتباری، کشف آنومالی، ماشین بردار حمایتی، کارت اعتباری وارد شده‌اند.

تحلیل منطقی روند تحولات پژوهشی در حوزه امنیت سایبری در بانک‌ها طی دو دههٔ گذشته حاکی از گذار مفهومی از موضوعات سنتی نظیر «ریسک سرمایه» و «امنیت اطلاعات» به سمت مفاهیم نوینی مانند «یادگیری ماشین»، «یادگیری یکپارچه» و «کشف هوشمند کلاهبرداری» است و بازیگران اصلی صحنه، فناوری‌های نوظهوری مانند «یادگیری یکپارچه»، «هوش مصنوعی» و «فناوری مالی» هستند که نقشی کلیدی در بازتعریف الگوهای امنیتی ایفا می‌کنند. نقشه‌های هم‌واژگانی، روندهای موضوعی و خوشه‌بندی‌های مفهومی حوزه امنیت سایبری نشان می‌دهند که موضوع‌های سنتی در دوره‌های زمانی نزدیک‌تر به زمان حال، دیگر به‌عنوان خوشه‌ای مستقل مطرح نیستند، بلکه با موضوعات جدیدتر ترکیب‌شده و خود خوشه‌ای مستقل را تشکیل داده‌اند. افزون بر این، در برخی موضوعات، خوشه‌های سنتی جای خود را به خوشه‌هایی با موضوعات میان‌رشته‌ای داده‌اند. این تغییرات نشان‌دهندهٔ رشد و بلوغ برخی موضوع‌ها، شکوفایی موضوع‌های نوظهور و نزدیک‌تر شدن محتواهای موضوعی برخی موضوعات به یکدیگر است.

در دوره‌های زمانی اولیه، شاهد شکل‌گیری و اهمیت موضوعاتی هستیم که هدف اصلی آن‌ها پاسخ به تهدیدهای حوزه امنیت سایبری بوده است. زمانی که پس از مواجهه با ریسک‌های متعدد و ناشناخته در این حوزه، به دنبال یافتن

پاسخ به حملات سایبری به‌منظور کاهش میزان خسارات و هزینه‌های وارده بوده‌ایم. اکنون، موضوع‌های موردتوجه پژوهشگران یک‌قدم فراتر رفته و به آینده‌نگری در این حوزه می‌اندیشند. پژوهشگران حوزه امنیت سایبری با تأکید بر محیط بانکداری، در پی کشف روش‌های نوین به‌وسیله الگوریتم‌های پیچیدهٔ فناورانه مانند یادگیری یکپارچه، یادگیری ماشین و یادگیری عمیق هستند تا بتوانند قبل از وقوع خطرات احتمالی، آن‌ها را پیش‌بینی کرده و راه‌حل‌های هوشمندانه با بهینه‌ترین هزینه‌ها ارائه دهند.

بنابراین، نگاه به حوزه امنیت سایبری در محیط بانکداری، بیش‌ازپیش نیازمند رویکردی فناورانه و مبتنی بر تحلیل داده‌های کلان است تا بتواند با یادگیری و کشف موضوع‌های جدید، روندهای پنهان در داده‌ها را شناسایی کرده و به مدیران و متخصصان این حوزه کمک کند.

پیشنهادهای اجرایی پژوهش

- با توجه به پایه و اساسی بودن موضوعات مربوط به خوشه امنیت سایبری، به مدیران حوزهٔ امنیت داده‌ها و امنیت سایبری در شرکت‌های فناوری اطلاعات وابسته به بانک‌ها، پیشنهاد می‌شود به رصد جدیدترین تحولات این حوزه و پیشرفت‌های آن‌ها پرداخته و متخصصان حوزه‌های جدید را شناسایی و به‌کارگیرند.
- با توجه به اینکه موضوع‌های یادگیری یکپارچه، مدل‌های داده‌ای و تحول دیجیتال، در سال ۲۰۲٤ محبوب بوده‌اند، پیشنهاد می‌شود متخصصان حوزه امنیت سایبری و امنیت اطلاعات به شناسایی پژوهش‌های هسته این حوزه پرداخته و با جدیدترین پیشرفت‌های این حوزه آشنا شوند.
- با توجه به این‌که موضوع کلاهبرداری یکی از موضوع‌های مهم سال ۲۰۲٤ است، پیشنهاد می‌شود متخصصان حوزه امنیت سایبری تجارب عملیاتی خود مرتبط با انواع مدل‌های کلاهبرداری و نیز روش‌های مقابله با آن را در سازمان‌های مختلف با یکدیگر به اشتراک گذاشته و نتایج هم‌افزایی را منتشر کنند.
- با توجه به این‌که فناوری مالی موضوع اصلی در سال ۲۰۲۳ بوده است، پیشنهاد می‌شود وب‌گاه‌های به‌روز مرتبط با این حوزه نظیر فینکسترا[1] از سوی متخصصان حوزه امنیت سایبری روزانه موردمطالعه قرار گیرد. علاوه بر این، با توجه به اهمیت موضوع هوش مصنوعی، بخشی از سایت که به‌طور ویژه به موضوع هوش مصنوعی در امور مالی می‌پردازد، موردتوجه قرار گیرد. همچنین وب‌گاه سی آی او[2] درزمینهٔ تحول دیجیتال می‌تواند برای متخصصان این حوزه مفید واقع شود.

پیشنهاد برای پژوهش‌های آتی

- بررسی موضوع‌های نوظهور و تخصصی در حوزهٔ یادگیری ماشین، یادگیری یکپارچه و یادگیری عمیق در حوزه امنیت سایبری.
- شناسایی موضوع‌های تخصصی مربوط به تحول دیجیتال در امنیت سایبری.
- تحلیل موضوعات پراستناد حوزه امنیت سایبری در بانک‌ها در دوره‌های زمانی مختلف و دلایل افزایش استناد به آن‌ها.
- شناسایی موضوع مقاله‌های زیبای خفته در حوزه امنیت سایبری در بانک‌ها.

1 . https://www.finextra.com/
2. https://www.cio.com

- با توجه به اینکه موضوع بانکداری اسلامی یکی از موضوع‌های اصلی پژوهشی در سال ۲۰۲۲ بوده است، پیشنهاد می‌شود دلایل اهمیت این موضوع در آن سال‌ها بررسی گردد تا مشخص شود وجه افزوده این نوع بانک‌ها نسبت به سایر بانک‌های جهانی چگونه بوده که توجه پژوهشگران را به خود جلب کرده است.
- تحلیل موضوعی مقاله‌های دارای حمایت مالی در حوزه امنیت سایبری در بانک‌ها.

تقدیر و تشکر

این مقاله حاصل یک پژوهش مستقل است که توسط نویسندگان انجام‌شده و تحت حمایت هیچ سازمانی قرار نداشته است.

تعارض منافع

نویسندگان اعلام می دارند که در خصوص انتشار این مقاله تضاد منافع وجود ندارد. علاوه بر این، موضوعات اخلاقی، از جمله سرقت ادبی، رضایت آگاهانه، سوء رفتار، جعل داده ها، انتشار و ارسال مجدد و مکرر و همچنین، سیاست مجله در قبال استفاده از هوش مصنوعی از سوی نویسندگان رعایت شده است.

فهرست منابع

آزاد سنجری، س.، و چهارسوقی، ک. (۱۴۰۳). *نوآوری‌ها و توسعه امنیت سایبری در بانک‌های ایران: تحلیل SWOT و مقایسه فرصت‌ها* [مقاله کنفرانسی]. دومین کنفرانس مهندسی و مدیریت فرایندهای سازمانی، تهران. https://civilica.com/doc/2183896

حاجیان، ح.، و زرجینی، ا. (۱۴۰۲). تحلیلی بر کاربردهای داده‌کاوی در صنعت بیمه بر اساس شبکه هم رخدادی واژگان‌ها و شناسایی معتبرترین مجالت با شاخص استناد به پژوهش‌های علمی با استفاده از رویکرد علم‌سنجی. *پژوهشنامه بیمه*، ۱۳(۱)، ۷۱-۸۶. https://doi.org/10.22056/ijir.2024.01.06

عسکریان کاخ، ا.، قویدل، س.، و ریاحی نیا، ن. (۱۴۰۲). تحلیل محتوای چهار دهه پژوهش در سیاست‌های پولی بانک مرکزی: با نگاهی به «عملیات بازار باز» (بر مبنای مدارک نمایه شده در پایگاه وب‌آوساینس در بازه زمانی ۱۹۸۱ – ۲۰۲۰). *مطالعات و سیاست‌های اقتصادی*، ۱۰(۱)، ۲۵-۵۲. https://doi.org/10.22096/esp.2023.522723.1468

عسگری مهر، م.، و مقصودلو، ز.(۱۴۰۲). *مدلی برای مدیریت ریسک امنیت سایبری در تحول دیجیتال (مطالعه موردی یک بانک ایرانی)* [مقاله کنفرانسی]. سیزدهمین کنفرانس بین‌المللی مدیریت، تجارت جهانی، اقتصاد دارایی و علوم اجتماعی. تهران. https://civilica.com/doc/1689447

Akintoye, R., Ogunode, O., Ajayi, M., & Joshua, A. A. (2022). Cyber security and financial innovation of selected deposit money banks in Nigeria. *Universal Journal of Accounting and Finance*, *10*(3), 643–652. https://doi.org/10.13189/ujaf.2022.100302

Aldasoro, I., Doerr, S., Gambacorta, L., Notra, S., Oliviero, T., & Whyte, D. (2024). Generative artificial intelligence and cyber security in central banking. *Journal of Financial Regulation*, *145*, 1–19. https://www.bis.org/publ/bppdf/bispap145.htm

Alqurashi, F., & Ahmad, I. (2024). Scientometric analysis and knowledge mapping of cybersecurity. *International Journal of Advanced Computer Science and Applications*, *15*(3), 1177–1184. https://doi.org/10.14569/IJACSA.2024.01503117

Asgari Mehr, M., & Maghsoodloo, Z. (2023). *A model for cybersecurity risk management in digital transformation: a case study of an Iranian bank* [Conference presentation]. The 13th International Conference on Management, World Trade, Economics, Finance and Social Sciences (pp. 1–21). https://civilica.com/doc/1689447 **[In Persian].**

Askarian Kakh, E., Ghavidel, S., & Riahinia, N. (2023). Four decades content analysis of research on Central Bank monetary policy: Looking at open market operations (based on the documents indexed in the Web of Science database in the Period 1981-2020). *The Journal of Economic Studies and Policies*, *10(1)*, 25–52. https://doi.org/10.22096/esp.2023.522723.1468 **[In Persian].**

Azad Sanjari, S., & Chaharsooghi, S. K. (2025). *Innovations and development of cyber security in Iranian banks: SWOT analysis and comparison of opportunities* [Conference presentation]. 2nd Conference on Organizational Process Engineering and Management (pp. 1–8). https://civilica.com/doc/2183896 **[In Persian].**

Callon, M., Courtial, J. P., Turner, W. A., & Bauin, S. (1983). From translations to problematic networks: An introduction to co-word analysis. *Social Science Information*, *22*(2), 191–235. https://doi.org/10.1177/053901883022002003

Cele, N. N., & Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, *32*(1), 31–48. https://doi.org/10.1108/jfc-10-2023-0263

Chang, H.-C. (2016). The synergy of scientometric analysis and knowledge mapping with topic models: modelling the development trajectories of information security and cyber-security research. *Journal of Information & Knowledge Management*, *15*(4), 1650044. https://doi.org/10.1142/S0219649216500441

Cybersecurity Ventures. (2025). *Global Cybercrime Damage Cost Predictions, 2025 To 2031*. Retrieved August 26, 2025, from https://cybersecurityventures.com/wp-content/uploads/2023/11/CybersecurityCost.pdf

Deora, R. S., & Chudasama, D. M. (2021). Brief Study of Cybercrime on an Internet. *Journal of Communication Engineering & Systems*, *11*(1), 1–6. https://computerjournals.stmjournals.in/index.php/JoCES/article/view/812

Dhawan, S. M., Gupta, B. M., & Elango, B. (2021). Global cyber security research output (1998–2019): A scientometric analysis. *Science and Technology Libraries*, *40*(2), 172–189. https://doi.org/10.1080/0194262X.2020.1840487

Duffy, B. M., & Duffy, V. G. (2020). Data mining methodology in support of a systematic review of human aspects of cybersecurity. In V. Duffy (ed.), *Digital Human Modeling and Applications in Health, Safety, Ergonomics and Risk Management. Human Communication, Organization and Work. HCII 2020. Lecture Notes in Computer Science* (Vol. 12199, pp. 242–253). Springer. https://doi.org/10.1007/978-3-030-49907-5_17

Elango, B., Matilda, S., Martina Jose Mary, M., & Arul Pugazhendhi, M. (2023). Mapping the cybersecurity research: A scientometric analysis of Indian publications. *Journal of Computer Information Systems*, *63*(2), 293–309. https://doi.org/10.1080/08874417.2022.2058644

Hajiyan, H., & Zarjini, A. (2023). A comprehensive analysis of keywords co-occurrence network and the most cited journals on data mining techniques in insurance industry using scientometrics approach. *Iranian Journal of Insurance Research*, *13*(1), 71–86. https://doi.org/10.22056/ijir.2024.01.06 **[In Persian].**

Khasseh, A. A., Soheili, F., Sharif Moghaddam, H., & Mousavi Chelak, A. (2017). Intellectual structure of knowledge in iMetrics: A co-word analysis. *Information Processing & Management*, *53*(3), 705–720. https://doi.org/10.1016/j.ipm.2017.02.001

Kuzior, A., Brożek, P., Kuzmenko, O., Yarovenko, H., & Vasilyeva, T. (2022). Countering cybercrime risks in financial institutions: Forecasting information trends. *Journal of Risk and Financial Management*, *15*(12), 613. https://doi.org/10.3390/jrfm15120613

Lee, W. H. (2008). How to identify emerging research fields using scientometrics: An example in the field of information security. *Scientometrics*, *76*, 503–525. https://doi.org/10.1007/s11192-007-1898-2

Loan, F. A., Bisma, B., & Nahida, N. (2022). Global research productivity in cybersecurity: a scientometric study. *Global Knowledge, Memory and Communication*, *71*(4-5), 342–354. https://doi.org/10.1108/GKMC-09-2020-0148

Martín-Martín, A., Orduna-Malea, E., Ayllón, J. M., & Lopez-Cozar, E. D. (2016). The Counting House, Measuring those Who Count: Presence of Bibliometrics, Scientometrics, Informetrics, Webometrics and Altmetrics in the Google Scholar citations, ResearcherID, ResearchGate, Mendeley & Twitter [Preprint]. Retrieved November 20, 2024, from: http://dx.doi.org/10.13140/RG.2.1.4814.4402/1

Matilde-Espino, Y., & Valencia-Pérez, L.-R. (2022). Bibliometric analysis of scientific production about Mexico regarding cybersecurity issues (2015-2020). *Ciencia Ergo Sum*, *29*(3), e177. https://www.scielo.org.mx/pdf/cies/v29n3/2395-8782-CES-29-03-177.pdf

Nesakumar, A. D., Arthi, S., Lahari, A., Geetha, M., Pavithra, K. N., & Mugilan, P. (2022, November). *Smart ATM card for multiple bank accounts* [Conference presentatiion]. 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC) (pp. 1228–1232). IEEE. https://doi.org/10.1109/IIHC55949.2022.10060834

Olijnyk, N. V. (2015). A quantitative examination of the intellectual profile and evolution of information security from 1965 to 2015. *Scientometrics*, *105*(2), 883–904. https://doi.org/10.1007/s11192-015-1708-1

Omote, K., Inoue, Y., Terada, Y., Shichijo, N., & Shirai, T. (2024). A scientometrics analysis of cybersecurity using e-csti. *IEEE Access*, *12*, 40350–40367. https://doi.org/10.1109/ACCESS.2024.3375910

Orosco-Fabian, J. R. (2024). Cybersecurity in higher education: a bibliometric review. *Revista Digital de Investigación En Docencia Universitaria*, *18*(2), e1933. https://doi.org/10.19083/ridu.2024.1933

Petrosyan, A. (2025). *Estimated cost of cybercrime worldwide 2018-2029*. *Statista*. Retrieved November 20, 2024, from https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

Phaal, R., O'Sullivan, E., Routley, M., Ford, S., & Probert, D. (2011). A framework for mapping industrial emergence. *Technological Forecasting and Social Change*, *78*(2), 217–230. https://doi.org/10.1016/j.techfore.2010.06.018

Pourmadadkar, M., Lezzi, M., & Corallo, A. (2024). Cyber security for cyber-physical systems in critical infrastructures: bibliometrics analysis and future directions. *IEEE Transactions on Engineering Management*, *71*, 15405–15421. https://ieeexplore.ieee.org/document/10740034

Raghuram, S., Tuertscher, P., & Garud, R. (2010). Research note—mapping the field of virtual work: A cocitation analysis. *Information Systems Research*, *21*(4), 983–999. https://doi.org/10.1287/isre.1080.0227

Rai, S., Singh, K., & Varma, A. K. (2019). Global research trend on cyber security: A scientometric analysis. *Library Philosophy and Practice*, *3339*, 1–6. https://digitalcommons.unl.edu/libphilprac/3769/

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A *Survey on Machine Learning Techniques for Cyber Security in the Last Decade*. *IEEE Access*, *8*, 222310–222354. https://doi.org/10.1109/ACCESS.2020.3041951

Shevchuk, R., & Martsenyuk, V. (2024). Neural Networks Toward Cybersecurity: Domaine Map Analysis of State-of-the-Art Challenges. *IEEE Access*, *12*, 81265–81280. https://doi.org/10.1109/ACCESS.2024.3411632

Solms, B. V., & Solms, R. V. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Van Raan, A. F. J. (2014). Advances in bibliometric analysis: research performance assessment and science mapping. In W. Blockmans, L. Engwall, & D. Weaire, *Bibliometrics Use and Abuse in the Review of Research Performance* (pp. 17–28). Portland publishers. https://scholarlypublications.universiteitleiden.nl/handle/1887/31991

Voce, I., & Morgan, A. (2023). Cybercrime in Australia 2023. *Statistical Report,* (43). Australian Institute of Criminology. https://doi.org/10.52922/sr77031

Wanying, Z., Jin, M., & Kun, L. (2018). Ranking themes on co-word networks: Exploring the relationships among different metrics. *Information Processing and Management*, *54*(2), 203–218. https://doi.org/10.1016/j.ipm.2017.11.005

Xu, H., Winnink, J., Yue, Z., Zhang, H., & Pang, H. (2021). Multidimensional scientometric indicators for the detection of emerging research topics. *Technological Forecasting and Social Change*, *163*(120490). https://doi.org/10.1016/j.techfore.2020.120490

Zhang, S. (2024). A visualized bibliometric analysis of artificial intelligence based on biblioshiny (2014-2023). *Scientific Journal of Technology*, *6*(7), 141–151. https://doi.org/10.54691/j4ddc779