Scientometrics Research Journal
Scientific Bi-Qualterly Journal of Shahed University/ Article in Press (Not edited)

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

Sepideh Fahimifar[1]
Amirhossein Momenzadeh[2]

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.

1. Associate Professor, Information Science and Knowledge Management Department, University of Tehran, Tehran, Iran. ORCID: 0000-0001-5182-9159. Email:sfahimifar@ut.ac.ir. (Coreesponding Author)
2. Computer Science Engineering, Data Security and Splunk Expert in SITS Company-Mellat Bank. ORCID: 0009-0007-1064-2612. E mail: a.momenzadeh@sits-co.com

Receive: ../../….
Acceptance: ../../….

Sepideh Fahimifar[1]
Amirhossein Momenzadeh[2]

1. Associate Professor, Information Science and Knowledge Management Department, University of Tehran, Tehran, Iran. ORCID: 0000-0001-5182-9159. Email:sfahimifar@ut.ac.ir. (Coreesponding Author)
2. Computer Science Engineering, Data Security and Splunk Expert in SITS Company-Mellat Bank. ORCID: 0009-0007-1064-2612. E mail: a.momenzadeh@sits-co.com

Receive: ../../….
Acceptance: ../../….

The thematic map 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

Sepideh Fahimifar[1]

Amirhossein Momenzadeh[2]

1. Associate Professor, Information Science and Knowledge Management Department, University of Tehran, Tehran, Iran. ORCID: 0000-0001-5182-9159. Email:sfahimifar@ut.ac.ir. (Coreesponding Author)
2. Computer Science Engineering, Data Security and Splunk Expert in SITS Company-Mellat Bank. ORCID: 0009-0007-1064-2612. E mail: a.momenzadeh@sits-co.com

Receive: ../../….
Acceptance: ../../….

پژوهش‌نامه علم‌سنجی
دوفصلنامه علمی ـ پژوهشی دانشگاه شاهد/ زودآیند ویرایش نشده

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

سپیده فهیمی فر [۱*]
امیرحسین مؤمن زاده [۲]

۱. دانشیار گروه علم اطلاعات و مدیریت دانش، دانشکده مدیریت دولتی و علوم سازمانی، دانشگاگان مدیریت، دانشگاه تهران .(نویسنده مسئول) sfahimifar@ut.ac.ir
۲. مهندس کامپیوتر، متخصص امنیت داده و اسپلانک شرکت زیرساخت امن خدمات تراکنش – بانک ملت، a.momenzadeh@sits-co.com

دریافت: ۰۰۰/۰۰/۰۰
پذیرش: ۰۰۰/۰۰/۰۰

چکیده

هدف: افزایش جرائم سایبری در سال‌های اخیر و افزایش هزینه ناشی از خسارت‌های وارده در این حوزه موجب شده است که مدیران، سیاستگذارن و دولتمردان بیش از پیش امنیت سایبری را مورد توجه قرار دهند، با این وجود درصد کمی از متخصصان دید جامعی نسبت به موضوع‌های مهم این حوزه دارند. این پژوهش با هدف شناسایی موضوع‌های محرک، تخصصی، ضروری و پایه حوزه امنیت سایبری و نیز شناسایی روندهای موضوعی در سال‌های مختلف انجام شده است. همچنین شناسایی موضوع‌های نوظهور و سیر روند تاریخی ظهور و افول موضوع‌ها در دوره‌های زمانی مختلف از جمله اهداف پژوهش است.

روش‌شناسی: رویکرد مطالعه علم‌سنجی است و از روش تحلیل هم‌رخدادی، تحلیل شبکه اجتماعی و شاخص‌های مرکزیت و چگالی استفاده شده است. جامعه آماری پژوهش کلیه مقاله‌های منتشر شده (۲۷۲۰مورد) در حوزه امنیت سایبری در پایگاه وب‌آوساینس از سال ۲۰۰۴ تا ۲۰۲۴ است. به منظور تحلیل هم‌واژگانی و تشکیل خوشه‌ها، فهرست لغات یکپارچه و بازدارنده ساخته و به منظور تحلیل داده‌ها از نرم‌افزار وس ویوور و افزونه تحت وب بیبلیوشاینی استفاده شد.

یافته‌ها: شبکه هم‌رخدادی واژه‌ها نشان داد که موضوع 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 از جمله مهمترین موضوع‌های سال ۲۰۲۴ بوده است. خوشه یادگیری ماشین دارای بیشترین مرکزیت و تراکم است.

نتیجه‌گیری: تحلیل منطقی سیر تحولات پژوهشی در حوزه امنیت سایبری در بانک‌ها طی دو دهه گذشته حاکی از گذار مفهومی از موضوع‌های سنتی نظیر "ریسک سرمایه" و "امنیت اطلاعات" به مفاهیم نوینی نظیر "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.

واژگان کلیدی: امنیت سایبری، بانکداری، علم‌سنجی، بیبلیوشاینی، وس ویوور، تحلیل موضوعی

مقدمه و بیان مسئله

آمارهای متعددی از سرتاسر دنیا در خصوص افرادی که در طول زندگی خود با چالش خدشه‌دار شدن امنیت در محیط اینترنت و شبکه مواجه بوده‌اند منتشر شده است. جرائم سایبری نظیر دزدی هویت، زورگویی اینترنتی، مزاحمت سایبری از جمله مهمترین مشکلات در سطح جهانی نه تنها برای امنیت اشخاص بلکه برای شرکت‌های بین المللی، بانک‌ها و دولت‌ها بوده است (Loan et al., 2022). با توجه به حساسیت امنیت سایبری در محیط بانک‌ها نیاز به ارزیابی مداوم و اصلاح استراتژی‌های امنیت سایبری احساس می‌شود که این امر نیازمند همکاری با شرکت‌هایی است که در حوزه امنیت سایبری فعالیت می‌کنند. هوش مصنوعی در کنار تخصص انسانی می‌تواند بر بهبود این وضع کمک شایان توجهی انجام دهد. بر اساس گزارش پِترویسان[1] (۲۰۲۴) تعداد شاکیان سالانه جرائم اینترنتی در سال ۲۰۲۳، ۸۸۰ هزار نفر و تعداد قربانیان فیشینگ در آمریکا در همان سال ۲۹۹ هزار نفر بوده است. داده‌های نظرسنجی در استرالیا نشان داد که ۲۷ درصد شرکت‌کنندگان با سوءاستفاده آنلاین، ۲۲ درصد با بدافزار، ۲۰ درصد با سرقت هویت و ۸ درصد قربانی کلاهبرداری شده‌اند. به علاوه ۴۷ درصد از شرکت‌کنندگان در پژوهش مذکور حداقل با یک جرم سایبری در طول ۱۲ ماه قبل از شرکت در پژوهش، مواجه بوده‌اند. نزدیک به نیمی از آن‌ها بیش از یک جرم سایبری را تجربه کردند (Voce & Morgan, 2023)

هزینه‌های ناشی از خسارت جرایم سایبری جهانی ۱۹۰ دلار در هر ثانیه، ۱۱,۴ میلیون دلار در هر دقیقه، ۶۸۴,۹ میلیون دلار در هر ساعت، ۱۶ میلیارد دلار در روز، ۱۱۵,۴ میلیارد دلار در هر هفته، ۵۰۰ میلیارد دلار در هر ماه و ۶ تریلیون دلار در سال برآورد شده است (Ezeji, 2022). در سال‌های اخیر هزینه نشت داده‌ها[2] بسیار افزایش یافته است به‌گونه‌ای که برطبق گزارش شرکت امنیتی "آی بی اِم" میانگین هزینه نشت اطلاعاتی به ۴,۳۵ میلیون دلار افزایش یافته است (Kuzior et al., 2022). به‌علاوه هزینه جرائم سایبری در سرتاسر جهان در سال ۲۰۲۴ معادل ۹,۲۲ تریلیون دلار بوده است. همچنین پیش بینی شده است که در فاصله سال‌های ۲۰۲۴ تا ۲۰۲۹ شاخص جهانی "هزینه تخمینی جرائم سایبری" به طور پیوسته افزایش می‌یابد و در حدود ۶۹ درصد رشد پیدا خواهد کرد و به رقم ۱۵,۶۳ تریلیون آمریکا در سال ۲۰۲۹ خواهد رسید. بنابراین سازمان‌ها بیش از پیش با خطرات ناشی از حملات سایبری آشنا شده‌اند و برای شرکت‌های جهانی تقویت تاب‌آوری سایبری تیم‌های امنیت اطلاعات از مهم‌ترین اولویت‌های هزینه کرد در سال ۲۰۲۳ بوده است (Petrosyan, 2024).

بر اساس گزارش آینده شغلی که در سال ۲۰۲۳ منتشر شده است، شغل‌هایی 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. اکثر شغل‌هایی که در آینده پیشرفت بسیار زیادی خواهند کرد شغل‌های مرتبط با فناوری هستند و در مقابل اکثر شغل‌هایی که تعداد آن‌ها کاهش خواهد یافت، شغل‌های مرتبط با دفتری یا منشی‌گری، متصدیان بانک و کارکنان مرتبط، کارمندان خدمات پستی و کارمندان مربوط به تهیه بلیط خواهند بود (Aldasoro et al., 2024). بنابراین بحث امنیت اطلاعات به ویژه در حوزه‌های مالی از جمله مهم‌ترین حوزه‌های مورد توجه در سال‌های پیش رو است. با این وجود تنها درصد کمی از متخصصان این حوزه دید جامعی از موضوع‌های مهم و همه جنبه‌های این صنعت دارند (Alqurashi & Ahmad, 2024). بدیهی است، امنیت سایبری موضوع مورد توجه و مورد علاقه طیف وسیعی از ذی‌نفعان است به آن دلیل که توجه به این موضوع می‌تواند از حمله‌های سایبری، دزدی‌های هویتی و نشت اطلاعات جلوگیری کند و به مدیریت ریسک کمک نماید. این مفهوم یکی از موضوعات در حال رشد با تأثیر و نتایجی بسیار گسترده است (von Solms & von Solms, 2018). بنابراین روش‌ها و فعالیت‌های مرتبط با امنیت سایبری با هدف حفاظت از داده‌ها، اطلاعات و شبکه‌های شخصی و سازمانی در

[1] Petrosyan
[2] data breaches

برابر تمام تهدیدات ممکن، چه داخلی و چه خارجی، طراحی شده‌اند (Akintoye et al., 2022). پژوهش‌های حوزه امنیت سایبری در اوج شکوفایی هستند و به منظور ارزیابی پژوهش‌های این حوزه تکنیک‌های علم‌سنجی از دیدگاه کمی و به‌ویژه کیفی می‌تواند بسیار مفید واقع شود (Loan et al., 2022).

آگاهی از موضوع‌ها و ایده‌های مهم یک حوزه علمی به صورت 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 حوزه امنیت سایبری به دو دسته اصلی تقسیم می‌شوند: دسته اول، پژوهش‌هایی 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 که به شناسایی موضوع‌های پرکاربرد، خوشه‌های موضوعی و تحلیل‌های هم‌استنادی پرداخته‌اند که در کنار دید کمی، تحلیل کیفی این پژوهش‌ها نسبت به پژوهش‌های نخست به منظور 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). با این وجود بررسی پژوهش‌های گذشته نشان می‌دهد که طیف منابع گردآوری شده منطبق با هدف پژوهش نبوده است؛ چرا که مهم‌ترین بخش تحلیل داده‌ها در علم‌سنجی بحث گردآوری منابع است. اکثر پژوهش‌های قبلی از طیف محدودی از کلیدواژه‌ها به منظور بازیابی منابع مرتبط استفاده کردند و به نظر می‌رسد نیاز به تحلیل موضوع‌های مقاله‌ها به صورت جامع وجود دارد. دوم آن که تعداد معدودی از پژوهش‌های گذشته به بررسی موضوع‌های نوظهور، تخصصی، محرک یا پیشران این حوزه پرداخته‌اند. همچنین بررسی روندهای تاریخی موضوع‌ها در بازه‌های زمانی مختلف و روند تحول آن‌ها در کم‌تر پژوهشی بررسی شده است.

همواره پژوهش‌های جدید مبنای تصمیم‌ها و پژوهش‌های آینده بوده و از همه مهم‌تر می‌توانند موجب دستاوردهای عملی در محیط واقعی باشند. رصد پژوهش‌ها به شیوه‌هایی نظیر فراترکیب، مرور سیستماتیک و علم‌سنجی می‌تواند شمای کلی از میزان پیشرفت، همکاری‌ها، موضوع‌های مورد توجه و نظایر آن را در اختیار قرار دهد. بنابراین آگاهی از روند پژوهشی، 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 نماید. با توجه به اهمیت موضوع امنیت سایبری به ویژه در سال‌های اخیر و کافی نبودن دانش متخصصان این حوزه در زمینه طیف‌های موضوعی گسترده حوزه مورد اشاره و نیز اهمیت حفظ داده‌های مشتریان و محرمانگی داده‌ها در محیط‌های مالی به خصوص بانک‌ها، نیاز به آگاهی از روندهای موضوعی این حوزه احساس می شود. این پژوهش با هدف شناسایی حوزه‌های موضوعی با شبکه هم‌رخدادی[1] واژگان، پیگیری تحول مفاهیم[2]، کشف موضوع‌های نوظهور، روندهای موضوعی[3] و نقشه‌های موضوعی[4] با تحلیل تماتیک ۴ بخشی است. بنابراین این پژوهش درصدد پاسخگویی به این سوال است که موضوعات اصلی و تحول‌یافته حوزه امنیت سایبری در محیط بانکداری چه موضوعاتی هستند و روند تحول آن‌ها در دوره‌های زمانی مختلف چگونه بوده است؟

سؤال‌های پژوهش/فرضیه‌های پژوهش

پرسش‌هایی که پژوهش حاضر قصد پاسخگویی به آن را دارد عبارتند از:

۱- روند انتشارات و روند استنادات پژوهش‌های انجام شده در حوزه امنیت سایبری در بانک‌ها چگونه بوده است؟

۲-شبکه هم‌رخدادی واژگان در حوزه امنیت سایبری در بانک‌ها چگونه است؟

[1] Co-occurrence network
[2] Thematic evolution
[3] Trend Topics
[4] Thematic Map

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

۴- در نقشه موضوعی حوزه امنیت سایبری در بانک‌ها موضوع‌های محرک، تخصصی، ضرروری و نوظهور چه موضوع‌هایی هستند؟

۵- روندهای موضوعی مهم و پرتکرار و موضوع‌های محرک، تخصصی، ضروری و نوظهور یا رو به افول در دوره‌های زمانی مختلف چه موضوع‌هایی بوده‌اند؟

چارچوب نظری

امنیت سایبری مجموعه‌ای جامع از همه تکنیک‌ها 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 به ویژه بعد از دوره همه‌گیری کرونا با توجه به افزایش ارتباطات در سطح مجازی اهمیت ویژه‌ای یافت. اتحادیه اروپا و دولت‌های عضو آن نیز در آن دوره و بعد از آن 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 کامپیوتر و سرقت اطلاعات، داده‌های رمزنگاری‌نشده، خدمات شخص ثالث غیرقابل اعتماد، 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 به واسطه کلیک در محیط اینترنت بیش از پیش محبوب شده است (Nesakumar et al., 2022). با این حال حفاظت و امنیت داده‌های مشتریان و رکوردهای تراکنش‌ها دارای اهمیت ویژه‌ای است. در نتیجه سنجه‌های امنیت سایبری قوی به منظور محافظت از تخلف‌ها و کلاهبرداری‌ها ضروری است.

حوزه پژوهشی امنیت سایبری طیف گسترده‌ای از زمینه‌ها، از شبکه، نرم‌افزار و سخت‌افزار گرفته تا رمزنگاری، احراز هویت و مقابله با حملات سایبری را شامل می‌شود (Omote et al., 2024). پژوهش‌های زیادی سالانه در حوزه امنیت سایبری در محیط بانکی به منظور جلوگیری از تهدیدهای فضای سایبری و نیز استراتژی‌های مقابله با ریسک‌های محتمل انجام می‌شود (Cele & Kwenda, 2024). امروزه اکثر بانک‌های مرکزی ابزارهای هوش مصنوعی مولد را به منظور کشف سریع تهدیدهای سایبری و به حداقل رساندن زمان پاسخ به تهدیدها پذیرفته‌اند. با این حال با ظهور هوش مصنوعی مولد خطرات حملات مهندسی اجتماعی و افشای غیرمجاز داده‌ها افزایش یافته است. بنابراین نیاز به سرمایه‌گذاری بر روی نیروی انسانی کارآمد که در حوزه امنیت سایبری و برنامه‌نویسی هوش مصنوعی تخصص دارند از سوی بانک‌های مرکزی به شدت 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 کنند و کدام گزینه‌های راهبردی را دنبال نمایند، تصمیم‌گیری کنند. این تصمیم‌گیری‌ها چالش‌برانگیز است، زیرا تحولات بازار، فناوری و صنعت، پیچیده و پویا هستند و کمبود اطلاعات و عدم‌قطعیت در پیش‌بینی‌ها نیز بر دشواری آن می‌افزاید (Phaal et al., 2011). برای بنیادهای پژوهشی و سیاست‌گذاران، شناسایی به‌موقع موضوع‌های

پژوهشی نوظهور[1] بسیار اهمیت دارد، چرا که به توسعه حوزه‌های پژوهشی نویدبخش کمک می‌کند. فناوری‌های نوظهور موضوع بحث‌های زیادی 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، نشان‌دهنده توجه روزافزون به این فناوری‌ها و موضوعات مرتبط با آن‌هاست. پروژه‌های مختلفی که توسط شورای تحقیقات اروپا[2] برای شناسایی حوزه‌های نوظهور انجام شده است، نمونه‌ای از علاقه فزاینده به این موضوع هستند (Xu et al., 2021).

بهترین آینه یک رشته علمی، منابعی است که جامعه علمی آن رشته منتشر می‌کنند (Martín-Martín et al., 2016) هر ساله تقریباً یک میلیون مقاله علمی در حال انتشار است، آیا می توانیم تمامی این پیشرفت‌ها را دنبال کنیم و از الگوهای پنهان شده آن‌ها باخبر شویم؟ (Van Raan, 2014). بیشتر مرورهای ادبیات موجود از دیدگاه تجربه‌های پژوهشگران انجام می‌شود و امکان دارد که این مرورها تحت تأثیر محدودیت زمانی و توانایی شناختی پژوهشگران مربوطه در حوزه مورد علاقه قرار گیرند. بنابراین ممکن است برخی مقاله‌ها وارد مرور آن پژوهشگر نشوند (Raghuram et al., 2010).

کلیدواژه‌های مقاله‌های علمی چه به صورت دستی (توصیفگرهای موضوعی و کلیدواژه‌های نویسندگان) و یا چه به صورت خودکار تولید شده باشند؛ نماینده‌ای از پیشرفت‌ها، ساختار و موضوع‌های یک حوزه علمی به واسطه تحلیل واژگان هستند (Callon et al., 1983). برخلاف روش‌های کتابسنجی نظیر تحلیل هم‌استنادی و تحلیل هم‌نویسندگی، تحلیل هم‌واژگانی روش محتوا-مداری است که به واسطه آن مفاهیم موضوعی تفسیر می‌شود. فراوانی اصطلاح به عنوان تعداد رخداد آن اصطلاح در مجموعه‌ای مشخص تعریف می‌شود و اغلب به منظور توصیف تم‌های موضوعی مهم یک حوزه به حساب 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 شبکه‌های هم‌واژگانی پیاده‌سازی شده است. ساختار شبکه‌های هم‌واژگانی ماورای رخداد کلمه هستند و می‌توانند اهمیت کلیدواژه را مورد سنجش قرار دهند (Zhao et al., 2018). به منظور تحلیل واژگان اصطلاحات اغلب از عناوین، متن کامل اثر، چکیده‌ها، اصطلاحات موضوعی و کلیدواژه‌های نویسندگان استفاده می‌شود (Zhao et al., 2018).

پیشینه پژوهش

پیشینه پژوهش در داخل

پژوهش‌های متعددی به بررسی مبحث امنیت سایبری در محیط بانکی از ابعاد مختلف پرداخته‌اند، با این حال نگاه به این حوزه از دیدگاه علم‌سنجی نادیده گرفته شده است. عسکریان کاخ، قویدل و ریاحی نیا (۱۴۰۲) به بررسی مقالات مجلات و کنفرانس‌های منتشر شده در حوزه موضوعی سیاست‌های پولی در بانک اطلاعاتی وب‌آوساینس پرداختند. آنها از نرم‌افزار راور پریمپ، وس ویوور[3] و اکسل استفاده کردند. پرکارترین نویسندگان، پربسامدترین کلیدواژه‌ها، و مجلات هسته، پراستنادترین مقالات در اثر پژوهشی آن‌ها شناسایی شد. 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 بهینه‌کردن شاخص‌ها از گروهی از متخصصان موضوعی استفاده کردند. در نهایت، 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 تاییدی تفسیر شد. آن‌ها به این نتیجه رسیدند که بیمه سایبری، استراتژی‌های سازمانی، راهبری فناوری در سازمان، مشتری، کارمندان، قوانین کشوری بر روی مدیریت ریسک امنیت

[1] Emerging research topics (ERTs)
[2] European Research Council (ERC)
[3] VOSviewer

سایبری تأثیرگذار است. حاجیان و زرجینی (۱۴۰۲) با رویکرد علم‌سنجی و با استفاده از نرم‌افزار وس ویوور، به بررسی مقالات منتشر شده در بانک اطلاعاتی وب‌آوساینس در حوزه موضوعی بیمه پرداختند. آن ها شبکه هم‌رخدادی واژگان در حوزه موضوعی داده کاوی و بیمه، کشف تخلفات بیمه، ریسک و مدیریت آن را ترسیم کردند. به‌علاوه به شناسایی مجلات مهم و کشورهای منتشرکننده مقالات نیز پرداختند.

مردانی شهر بابک و زالی نژاد (۱۴۰۳) به منظور ارتقای فرهنگ امنیت سایبری در محیط بانکداری چارچوبی را تدوین نمودند. چارچوب مذکور به بهبود تاب‌آوری در مقابل تهدیدهای سایبری، افزایش اعتماد مشتریان و بهبود کارایی سیستم‌های امنیتی کمک خواهد کرد. 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 به عنوان فرصت، ایجاد روابط نزدیک با نهادهای نظارتی، سیاست‌ها و استانداردهای سخت‌گیرانه داخلی را به عنوان نقاط قوت، حملات سایبری از سوی دولت‌ها، ضعف قوانین حفاظت از داده‌ها، سرعت پایین تطابق با تغییرات فناورانه را به عنوان تهدید و عدم انطباق ساختار سازمانی مطابق با استانداردهای امنیتی، کمبود نیروی انسانی متخصص، ضعف در آموزش و آگاهی کارکنان را به عنوان ضعف شناسایی کردند.

پیشینه پژوهش در خارج [نظم تاریخی از قدیم به جدید رعایت شود]

در حوزه‌های مرتبط با امنیت سایبری تاکنون پژوهش‌هایی با رویکرد کتابسنجی و علم‌سنجی به زبانی به غیر از فارسی انجام شده است. نخستین پژوهش در حوزه امنیت اطلاعات، از سوی لی (Lee, 2008) انجام شد که از داده‌های نمایه استنادی علوم استفاده کرد و به تحلیل هم‌واژگانی به منظور مشخص نمودن موضوع‌های مهم این حوزه پرداخت. اُلیجنیک (Olijnyk, 2015) به تحلیل مقاله‌های منتشر شده در مجله‌ها و مقاله‌های منتشر شده در کنفرانس‌ها در حوزه امنیت اطلاعات در پایگاه اسکوپوس از سال ۱۹۶۵–۲۰۱۵ پرداخت و از کلیدواژه‌های امنیت اطلاعات، تضمین اطلاعات، امنیت سایبری و تنوع نگارش آن، امنیت کامپیوتر، امنیت ارتباطات، امنیت داده و امنیت شبکه برای جستجوی منابع مرتبط استفاده کرد. به علاوه با استفاده از نرم‌افزار وس ویوور به تحلیل واژگان پرداخت. رمزنگاری و مدیریت امنیت اطلاعات به عنوان موضوع مورد توجه چندین دهه و موضوع‌هایی نظیر شناسایی نفوذ، امنیت داده‌های پزشکی، نهان‌نگاری و امنیت بی‌سیم به عنوان موضوع‌های نوظهور مطرح شدند. پژوهشی مشابه نیز، با هدف بررسی تولیدات علمی در حوزه امنیت اطلاعات و امنیت سایبری با رویکرد علم‌سنجی و ترسیم نقشه‌های دانشی از سال ۱۹۹۵ تا ۲۰۱۵ در نمایه استنادی علوم اجتماعی و نمایه استنادی هنر و علوم انسانی انجام شده است. در مجموع، ۱۷۵۰ مقاله در حوزه امنیت اطلاعات و ۵۳۸ مقاله در حوزه امنیت سایبری با نرم‌افزار سایت‌اسپیس مورد تحلیل قرار گرفتند. رایانش ابری جدیدترین اصطلاحی است که از سال ۲۰۱۱ به بعد مورد توجه بوده است. مقاله‌هایی که به هر دو موضوع امنیت اطلاعات و امنیت سایبری مربوط بودند، به موضوع انرژی برق بسیار توجه داشته‌اند که نشان‌دهنده‌ی مسئله آسیب‌پذیری زیرساخت‌های کنترلی متصل به اینترنت است (Chang, 2016). ارزیابی داده‌های پژوهشی در حوزه امنیت سایبری در بانک اطلاعاتی اسکوپوس از سال ۲۰۰۱ تا ۲۰۱۸ موضوع پژوهش دیگری بوده است. رای و همکاران (Rai et al., 2019) به تحلیل نویسندگان، موسسات، همکاری‌ها و بودجه‌های پژوهشی پرداختند. در این پژوهش تنها از واژه امنیت سایبری به منظور گردآوری داده‌ها در قسمت جستجوی عنوان بانک اطلاعاتی استفاده شده است.

دافی و دافی (Duffy & Duffy, 2020) به مرور سیستماتیک و شناسایی موضوع‌های نوظهور عوامل مرتبط انسانی در امنیت سایبری با استفاده از تحلیل محتوا و تکنیک‌های علم‌سنجی تا سال ۲۰۲۰ در دو پایگاه وب‌آوساینس و گوگل اسکالر پرداخته‌اند. آن‌ها از ابزارهایی نظیر ووس ویور، مکس کیودا۱، هارزیگ۱، اوتورمپر۲ برای تحلیل پژوهش‌ها استفاده کردند.

[1] MAXQDA

کلیدواژه‌های مورد جستجو برای گردآوری منابع تنها محدود به امنیت سایبری و عامل انسانی۳ بوده است. عوامل انسانی و ارگونومی کاربردی۴ مهمترین موضوع پرتکرار در پژوهش‌های این حوزه بوده است. مشابه با پژوهش لی (Lee, 2008)، لون، بیسما و ناهید (Loan et al., 2022) در مطالعه‌ای به تحلیل مجموعه مقاله‌های نمایه شده در مجموعه هسته وب‌آوساینس از سال ۲۰۱۱ تا ۲۰۲۰ در حوزه‌های امنیت سایبری، امنیت وب، امنیت اطلاعات و امنیت کامپیوتر پرداختند. مجموعه داده‌ها به فرمت نرم‌افزار اکسل ذخیره شده است و با استفاده از افزونه تحت وب بیبلیوشاینی[5] و نرم‌افزار وس ویوور به تحلیل داده‌ها پرداختند. تنوع کلیدواژه‌های مورد جستجو برای گردآوری داده‌ها در این پژوهش کمتر از پژوهش حاضر است. پژوهش آن‌ها نشان داد، که متداول‌ترین کلیدواژه مورد استفاده از سوی نویسندگان، کلیدواژه امنیت سایبری و بعد از آن تنوع نگارشی این کلیدواژه به صورت ترکیب دو کلیدواژه امنیت و سایبر با فاصله و بعد از آن با خط تیره بوده است. کلیدواژه‌های امنیت، امنیت کامپیوتری و امنیت اطلاعات، حفظ محرمانگی، یادگیری ماشین، اینترنت اشیا، تشخیص نفوذ، رمزنگاری، شبکه هوشمند برق در رتبه‌های بعد قرار دارند.

برخی پژوهش‌ها تولیدات علمی با موضوع امنیت سایبری خاص یک کشور را بررسی کرده‌اند. به عنوان نمونه تولیدات علمی مربوط به امنیت سایبری در کشور مکزیک از جمله پژوهش‌های اخیر در این حوزه به شمار می‌رود که با رویکرد کتابسنجی و با هدف بررسی تعداد مقالات سالانه، تعداد مقالات در هر نشریه، سهم مؤسسات و نویسندگان، و محتوای موضوعی مقالات انجام شده است (Matilde-Espino & Valencia-Pérez, 2022).

اِلانگو (Elango et al., 2023) از منظر جنبه‌های انسانی نیز به مسئله امنیت سایبری با رویکرد علم‌سنجی نیز توجه کرد و با استفاده از نرم‌افزارهای اکسل، پکیج بیبلیومتریکس آر، وس ویوور و یوسی‌نِت به کشف ساختارهای اجتماعی و مفهومی منابع منتشرشده از سوی پژوهشگران هندی پرداخت. در مجموع 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 ۲۰۱۴ به شبکه‌های هوشمند در سال ۲۰۱۵، سپس محاسبه ابری در سال ۲۰۱۷ تغییر یافته است. سپس در بازه ۲۰۱۸ تا ۲۰۲۰ از کنترل نظارتی و جمع‌آوری داده‌ها[6] در سال ۲۰۱۸ به یادگیری عمیق در سال ۲۰۲۰ تغییر یافته است.

پورمددکار و دیگران (Pourmadadkar et al., 2024) به تحلیل کتابسنجی منابع منتشر شده در پایگاه وب‌آوساینس و اسکوپوس در حوزه امنیت سایبری در سیستم‌های سایبری–فیزیکی۷ (در مجموع۱۶۴۹ مدرک) پرداختند. آن‌ها از تحلیل هم‌رخدادی واژگان با هدف شناسایی خوشه‌های موضوعی استفاده کردند که در مجموع ۷ خوشه شناسایی شد. توسعه دانش در این حوزه به ۴ دوره زمانی امنیت داده‌ها در سیستم‌های کنترل نظارتی و گردآوری داده‌ها۸، امنیت زیرساخت‌های حیاتی۹، امنیت سایبری سیستم‌های کنترل صنعتی۱۰ و امنیت سایبری سیستم‌های سایبر–فیزیکی۱۱ تقسیم شده است.

اُمُت و دیگران (Omote et al., 2024) به شناخت انواع حوزه‌های موضوعی امنیت سایبری با بررسی پژوهش‌های ده درصد

---

[1] Harzing
[2] AuthorMapper
[3] Cybersecurity AND human factors
[4] Applied Human Factors and Ergonomics(AHFE)
[5] Biblioshiny
[6] SCADA
[7] Cyber–physical systems (CPSs)
[8] Supervisory Control and Data Acquisition
[9] Critical infrastructures
[10] Industrial control systems
[11] Cyber–physical systems (CPSs)

برتر در فاصله سال‌های ۲۰۱۰ تا ۲۰۱۹ که حتما دو سال از زمان انتشار آن‌ها گذشته باشد پرداختند. یافته‌ها نشان داد که این حوزه به ۴ 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 به کارگیری شبکه‌های عصبی در امنیت سایبری به واسطه تحلیل علم‌سنجی و به کارگیری نرم‌افزار سایت اسپیس انجام شده است. جامعه پژوهش انواع منابع منتشر شده در این حوزه از سال ۲۰۰۳ تا ۲۰۲۳ در پایگاه مجموعه هسته وب‌آوساینس بوده است. به علاوه منابع گردآوری شده 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 (در مجموع ۲۰۱۸ منبع) جمع‌آوری شده است. حوزه یادگیری عمیق، یادگیری ماشین و تشخیص نفوذ، امنیت سایبری، شبکه‌های عصبی، اینترنت، الگوریتم، بهینه-سازی، داده‌های بزرگ و اینترنت اشیاء به ترتیب از مهم‌ترین موضوعاتی بوده‌اند که فراوانی بالاتری نسبت به سایر کلیدواژه‌ها داشته‌اند. به علاوه کلیدواژه‌های امنیت سایبری، داده‌کاوی و شبکه عصبی به ترتیب بیش‌ترین میزان استناد را در بازه‌های مختلف با توجه به دوره زمانی مورد بررسی به خود اختصاص داده‌اند (Shevchuk & Martsenyuk, 2024). در حوزه آموزش عالی نیز به امنیت سایبری با رویکرد کتابسنجی با استفاده از نرم‌افزار دیتارَپر[1]، وس ویوور و بیلیومتریکس توجه شده است و به بررسی منابع منتشر شده در پایگاه اسکوپوس در مجموع ۱۱۸ اثر پرداختند. در این حوزه بیش‌تر پژوهش‌ها به مسئله امنیت سایبری، تهدیدات سایبری، آگاهی از امنیت سایبری، نقض امنیت سایبری، امنیت اطلاعات، و مقررات عمومی حفاظت از داده‌ها پرداخته‌اند (Orosco-Fabian, 2024).

جمع‌بندی از مرور پیشینه

نگاهی به پژوهش‌های گذشته نشان می‌دهد که تحلیل مطالعات حوزه امنیت سایبری و امنیت اطلاعات به عنوان یک مسئله مهم به صورت کلی یا با توجه به جنبه‌های خاص آن مورد توجه قرار گرفته است. بنابراین پرداختن به حوزه امنیت سایبری به صورت مطالعات کلان محور یا موضوع‌محور بوده است. موضوع امنیت سایبری در ارتباط با عامل انسانی، آموزش، سیستم‌های سایبری–فیزیکی، شبکه‌های عصبی به صورت خاص در پژوهش‌ها بررسی شده و در سایر پژوهش‌ها موضوع امنیت سایبری و امنیت اطلاعات به صورت کلی بررسی شده است. به لحاظ موضوعی، پژوهشی به بررسی حوزه‌های موضوعی امنیت سایبری در محیط بانکداری نپرداخته است. این در حالی است که حوزه بانکداری به عنوان حیاتی‌ترین زیرساخت اقتصادی می‌تواند با چالش‌های مهم، اساسی و منحصربه‌فردی به صورت روزانه مواجه باشد. هدف عمده پژوهش‌های گذشته شناسایی روندها و بازیگران کلیدی این حوزه بوده است. با این وجود تحلیل روندهای موضوعی، تحلیل موضوع های مهم در دوره‌های زمانی مختلف و تحول آن‌ها، شناسایی موضوع های محرک، ضروری، نوظهور در کنار هم و تحلیل پررنگ شدن و کم‌رنگ شدن پرداختن به یک حوزه موضوعی در پژوهشی مورد توجه نبوده است؛ در نتیجه پژوهش حاضر سعی بر آن دارد که تمامی این وجوه را پوشش می‌دهد. در نتیجه پژوهش حاضر، چشم‌انداز جامع‌تر و دقیق‌تری از روندهای موضوعی مهم در حوزه 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.

اکثر پژوهش‌های قبلی از پایگاه وب‌آوساینس و اسکوپوس برای جمع‌آوری داده‌ها استفاده کرده‌اند. دوره زمانی، انواع منابع مورد بررسی، دامنه موضوعی و نرم‌افزار مورد استفاده در پژوهش‌ها متنوع بوده است. با این حال، نرم‌افزار وس ویوور به عنوان شاخص‌ترین نرم‌افزار در کنار سایر نرم‌افزارها برای تحلیل هم‌رخدادی استفاده شده است. تنوع کلیدواژه‌ها برای جستجو و گردآوری منابع در تعداد زیادی از پژوهش‌ها محدود بوده است. به علاوه در اکثر پژوهش‌ها از فهرست لغات و یا فهرست لغات بازدارنده

[1] Datawrapper

استفاده نشده است. در این پژوهش برای ایجاد یکدستی، تنوع نگارش کلمات، جمع یا مفرد بودن کلمات، اختصارات و نظایر آن به عنوان فهرست لغات اصطلاحنامه در نظر گرفته شد و فهرست واژگان بازدارنده نیز ساخته و در افزونه تحت وب بیبلیوشاینی از آن استفاده شد.

روش‌شناسی پژوهش

با توجه به اینکه هدف پژوهش شناسایی حوزه‌های موضوعی و گرایش‌های نوظهور، محرک، ضروری و سیر تحول موضوع‌ها در حوزه امنیت سایبری در حیطه تخصصی بانکداری است، با رویکرد علم‌سنجی به تحلیل کلیدواژه‌های مقاله‌ها پرداخته شد. بدین منظور از تحلیل هم‌رخدادی، تحلیل شبکه اجتماعی و شاخص‌های مرکزیت و چگالی استفاده شد. جامعه پژوهش کلیه مقاله‌های منتشر شده در حوزه امنیت سایبری در بانک‌ها در پایگاه اطلاعاتی وب‌آوساینس از سال ۲۰۰۴ تا ۲۰۲۴ است که با توجه به اینکه شروع نمایه شدن این مقاله‌ها در پایگاه مذکور از سال ۲۰۰۴ بود، بازه مذکور انتخاب شد. جستجو در تاریخ ۲۸ اسفند ۱۴۰۳ انجام و داده‌ها گردآوری شدند. علت انتخاب این پایگاه آن است که مقالات با کیفیت جهانی که به عنوان مقالات آی‌اِس‌آی شناخته می‌شوند در این پایگاه منتشر می‌شوند و از جمله مقالات هسته محسوب می‌شوند. با جستجو در فیلد Topic این پایگاه با کلیدواژه‌های مترادف و یا با نوع نگارش متفاوت کلیه مدارک مرتبط بازیابی شدند. به علاوه با توجه به حساسیت و اهمیت کلیدواژه‌های جستجو با مشورت متخصصان حوزه امنیت سایبری کلیه کلیدواژه‌های مرتبط در نظر گرفته شدند. از میان انواع منابع بازیابی شده، تنها مقاله‌های انگلیسی زبان و در میان سال‌های مورد بررسی، تمامی سال‌ها به جز سال ۲۰۲۵ در جستجو مدنظر قرار گرفتند. علت عدم انتخاب مقاله‌های سال ۲۰۲۵ آن است که تنها ۲ ماه از شروع سال سپری شده است و این مقاله‌ها نیز در این مدت کوتاه هم به لحاظ کمیت و هم به لحاظ استنادی قابل مقایسه با سایر مقاله‌ها نیستند. راهبرد جستجو در بخش جستجوی پیشرفته پایگاه عبارتست 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)

در مجموع ۲۷۷۰ مدرک بازیابی شد که از میان آن‌ها تعدادی از مدارک به دلیل تکراری بودن حذف شدند. تعدادی از مدارک نیز تاریخ نشر آن‌ها مربوط به سال ۲۰۲۵ بود که آن‌ها نیز از مجموعه مدارک حذف شدند و تعداد کل مدارک مورد تحلیل ۲۷۲۰ مقاله بود.

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 ماخذ آن‌ها با فرمت txt. دانلود شدند. سپس به منظور تحلیل داده‌ها از افزونه تحت وب بیبلیوشاینی و نرم‌افزار وس ویوور استفاده شد. با توجه به اینکه بیبلیوشاینی کل داده‌ها را در یک فایل می‌پذیرد، داده‌های جمع‌آوری شده در یک فایل تجمیع شدند. افزونه تحت وب بیبلیوشاینی به واسطه نصب و اجرای نرم‌افزار آر در مرورگر قابل فراخوانی خواهد بود. به منظور استفاده از این پکیج باید متناسب با سیستم عامل خود و نسخه نرم‌افزار آر کدهایی را در برنامه آر اجرا نمود تا امکان استفاده از این افزونه مهیا شود. بیبلیوشاینی می‌تواند به عنوان جایگزین برخی نرم‌افزارهای حوزه علم‌سنجی استفاده شود، زیرا ترسیم بسیاری از نقشه‌ها و محاسبه شاخص‌ها را می‌توان به واسطه این نرم‌افزار انجام داد.

در نهایت، پژوهشگران اقدام به ساخت فهرست لغات به منظور یکدستی و فهرست لغات بازدارنده به صورت جداگانه به منظور استفاده در بیبلیوشاینی نمودند. به دلیل اینکه فهرست کلیدواژه‌های بازدارنده و مترادف از قبل مشخص نیست و چنین فهرستی در هر حوزه موضوعی ممکن است متفاوت باشد، نخست تمامی کلیدواژه‌ها به واسطه نرم‌افزار وس ویوور استخراج و از فرمت txt. به فرمت xlsx. تبدیل شدند. 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

کلیات مدارک مورد بررسی

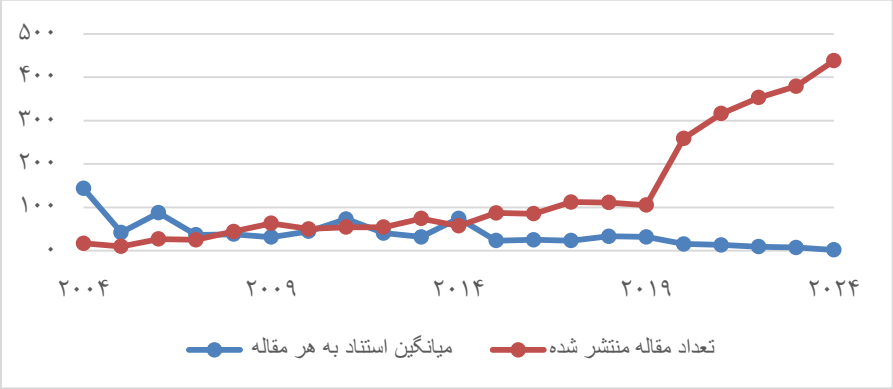
۲۷۲۰ مقاله منتشر شده در این حوزه در ۱۰۳۳ مجله منتشر شده است. نزدیک به ۳۰ درصد از آثار با همکاری نویسندگان بین‌المللی نگارش شده است. به علاوه تعداد زیادی از پژوهش‌های حوزه امنیت سایبری در محیط بانکی با مشارکت گروهی پژوهشگران نگارش شده است. همچنین هر مدرک به طور متوسط ۱۹ استناد را به خود اختصاص داده است. با توجه به نرخ رشد سالانه مقاله‌ها، می‌توان استنباط کرد که این حوزه از جمله موضوع‌های مهم و قابل پژوهش به شمار می‌آید.

شکل ۱. توصیف مجموع مقاله‌های حوزه امنیت سایبری در بانک

پاسخ به پرسش اول پژوهش. روند انتشارات و روند استنادات پژوهش‌های انجام شده در حوزه امنیت سایبری در بانک‌ها چگونه بوده است؟

نمودار ۱- تعداد مقاله‌های منتشر شده در هر سال (رنگ نارنجی) و متوسط میزان استناد به مقاله‌ها (رنگ آبی) را در هر سال نشان می‌دهد. از سال ۲۰۰۴ تا ۲۰۲۴ تعداد مقاله‌ها در این حوزه رشد تصاعدی داشته است. از سال ۲۰۲۰ به بعد تعداد مقاله‌ها از ۲۵۹ مقاله به ۴۳۸ مقاله در سال ۲۰۰۴ رسیده است که نشان می‌دهد اهمیت امنیت در فضای دیجیتالی در محیط بانک‌ها روز به روز بیش‌تر شده است.

همچنین نگاهی به روند استنادات در سال‌های مختلف نشان می‌دهد که میانگین استناد به ازای هر مقاله در سال ۲۰۰۴ بیش از دیگر سال‌ها (۱۴۳) بوده است. میانگین استناد به ازای هر مقاله روند افزایشی و کاهشی داشته است. بعد از آن، سال ۲۰۰۶ و سال ۲۰۱۴ 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

به منظور تعدیل تاثیر سال انتشار مقاله بر میزان دریافت استناد از شاخص میانگین استناد سالانه به ازای هر مقاله استفاده شد. فرمول محاسبه این میانگین به شرح زیر است:

تعداد کل استناد ها (تعداد مقاله‌ها× تعداد سال های سپری شده از زمان انتشار)

با توجه به جدول۱- سال‌های ۲۰۰۴، ۲۰۱۴، ۲۰۱۱ و ۲۰۱۹ بالاترین میانگین استناد سالانه به ازای هر مقاله را به خود اختصاص داده‌اند. در میان مقاله‌های مورد بررسی، مقاله درباره توپولوژی شبکه تجزیه واریانس‌ها: اندازه‌گیری میزان اتصال شرکت‌های مالی[1] از سوی دیبولد و ییلماز[2] (۲۰۱۴) دارای بیش‌ترین استناد (۲۶۰۵ استناد) است. بعد از آن مقاله‌ای با عنوان ارزش در معرض ریسک خودرگرسیونی شرطی با استفاده از رگرسیون چارکی[3] به نویسندگی اِنگِل و منگلنیس[4] (۲۰۰۴) توانسته ۱۲۲۶ استناد را کسب کند.

جدول ۱. میانگین استناد سالانه به مقاله‌ها

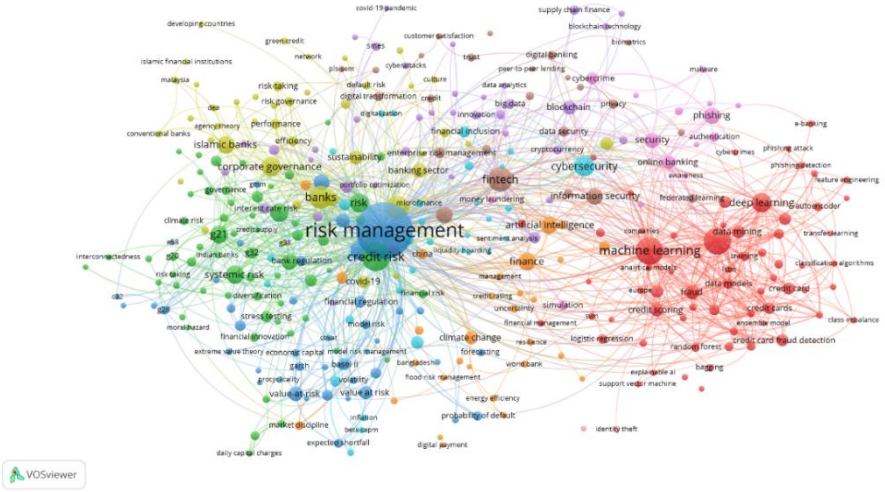
سال انتشار	تعداد سال‌های قابل استناد	میانگین استناد سالانه به ازای هر مقاله
۲۰۰٤	۲۲	٦/٥١
۲۰۰٥	۲۱	۲
۲۰۰٦	۲۰	٤/۳۸
۲۰۰۷	۱۹	۱/۹۱
۲۰۰۸	۱۸	۲/۱۰
۲۰۰۹	۱۷	۱/۸۳
۲۰۱۰	۱٦	۲/۷۷
۲۰۱۱	۱٥	٤/۸٦
۲۰۱۲	۱٤	۲/۸۹
۲۰۱۳	۱۳	۲/٤٥
۲۰۱٤	۱۲	٦/۲۱
۲۰۱٥	۱۱	۲/۱
۲۰۱٦	۱۰	۲/٥۱
۲۰۱۷	۹	۲/٥٥

[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

۲۰۱۸	۸	٤/۱۲
۲۰۱۹	۷	٤/٥۱
۲۰۲۰	٦	۲/٥٥
۲۰۲۱	٥	۲/٦٥
۲۰۲۲	٤	۲/۲٦
۲۰۲۳	۳	۲/۳۸
۲۰۲٤	۲	۰/۹٤

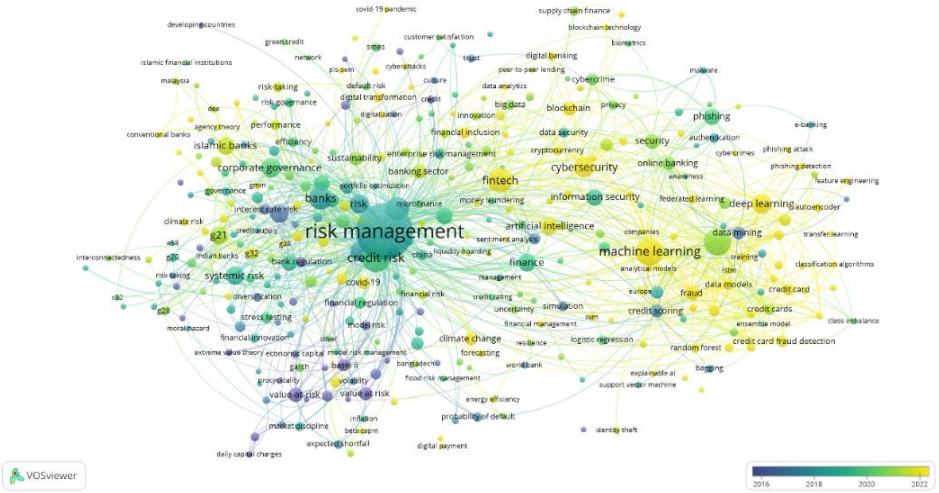
پاسخ به پرسش دوم پژوهش. شبکه هم‌رخدادی واژه‌ها در حوزه امنیت سایبری در بانک‌ها چگونه است؟

شبکه هم‌رخدادی واژه‌ها با استفاده از کلیدواژه‌های نویسندگان ترسیم شد. شرط ورود به شبکه حداقل ۵ رخداد در نظر گرفته شد و در مجموع ۳۵۲ کلیدواژه وارد نقشه شدند. بر اساس تعداد فراوانی در مقاله‌ها، کلیدواژه مدیریت ریسک (۴۵۶ رخداد)، یادگیری ماشین (۱۱۳ رخداد)، ریسک اعتباری (۱۱۷ رخداد)، کشف کلاهبرداری(۱۰۴ رخداد) بیش‌ترین تعداد رخداد را به خود اختصاص داده‌اند. بعد از آن، واژه‌های بانکداری، فناوری مالی، بانک، جی۲۱، یادگیری عمیق و کلاهبرداری قرار دارند. بررسی قدرت ارتباطی پیوندها نیز نشان می‌دهد که موضوع‌های ذکر شده به همان ترتیب دارای بیش‌ترین قدرت ارتباطی هستند (شکل ۲-).



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

نقشه مصورسازی پوششی کلیدواژه‌ها (شکل ۳-) نشان می‌دهد که بر اساس میانگین سال انتشار، نرخ توجه به کلیدواژه‌ها از رنگ آبی پررنگ به زرد تغییر کرده است. این بدین معنی است که کلیدواژه‌ها هر چه به رنگ آبی نزدیک‌تر باشند، به طور متوسط پژوهش‌های قدیمی‌تر به این موضوعات اختصاص یافته‌اند و هر چه به رنگ زرد نزدیک‌تر باشند، این کلیدواژه‌ها از جمله موضوع‌های پژوهشی سال‌های اخیر به حساب می‌آیند. یادگیری ماشین، یادگیری عمیق، فناوری مالی، هوش مصنوعی، امنیت سایبری، مدل‌های داده‌ای، کشف کلاهبرداری و کارت اعتباری از جمله موضوع‌های مهم سال‌های اخیر هستند (شکل ۳-).



شکل ۳. نقشه مصورسازی پوششی حوزه امنیت سایبری در بانک‌ها

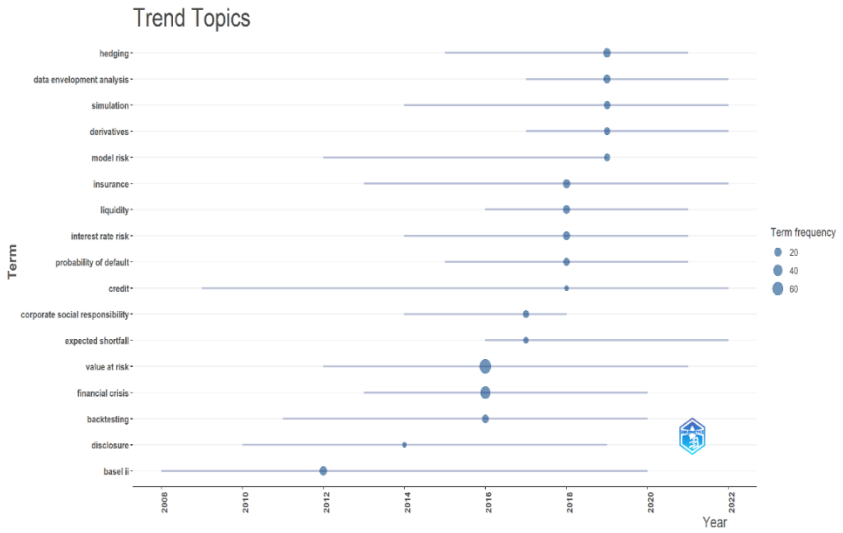
پاسخ به پرسش سوم پژوهش. تحول موضوعات پرتکرار در دوره‌های زمانی مختلف چگونه است؟

به منظور 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 بازه زمانی در نظر گرفته شد. نخست موضوعاتی که از ابتدای سال ۲۰۰۴ تا سال ۲۰۱۹ (شکل ۴-) از جمله موضوعات پرتکرار بوده‌اند و دوره ی دوم، تحولات سال‌های اخیر از سال ۲۰۲۰ تا ۲۰۲۴ (شکل ۵-) در نظر گرفته شد. دلیل آن که نمودار نخست از سال ۲۰۰۸ شروع شده است آن است که با توجه به اهمیت تکرار کلیدواژه‌ها برای ورود به نمودار در فاصله سال‌های ۲۰۰۴ تا ۲۰۰۸ موضوعاتی به عنوان نقطه اوج یا محبوب وجود نداشته است.

خط افقی نشان‌دهنده نقطه شروع زمانی استفاده از کلیدواژه در مقاله‌ها تا نقطه 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.

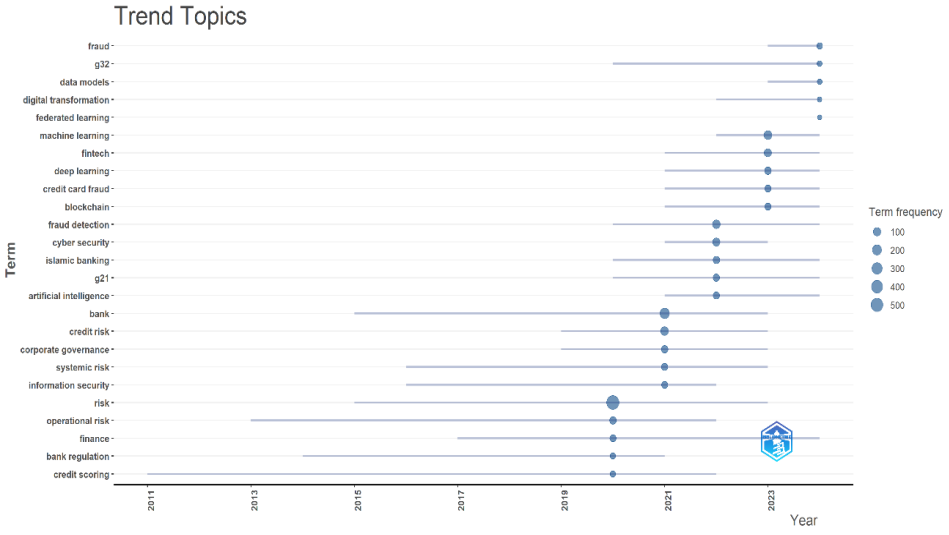
دو موضوع حداکثر زیان احتمالی[1] با ۷۲ مورد تکرار در مقالات و بحران مالی با ۴۹ مورد تکرار در مقالات از جمله روندهای موضوعی محبوب مقاله‌های این حوزه در سال ۲۰۱۶ بوده است. شروع توجه به موضوع حداکثر زیان احتمالی از سال ۲۰۱۲ بوده است و تا پایان سال ۲۰۱۹ نیز ادامه داشته است. موضوع بحران مالی از سوی پژوهشگران از سال ۲۰۱۳ مورد توجه قرار گرفت. موضوع مقرارت و چارچوب‌های بین‌المللی برای اندازه‌گیری و مدیریت ریسک در بانک‌ها از سال ۲۰۰۸ نیز مورد توجه بوده است، اما اوج محبوبیت آن در سال ۲۰۱۶ اتفاق افتاده است. اقدامات مالی برای کاهش ریسک نیز با فراوانی ۲۱ از سال ۲۰۱۵ به آن پرداخته شده است و دارای بیش‌ترین محبوبیت در سال ۲۰۱۹ است.

[1] Value at Risk (VaR)



شکل ٤. حوزه‌های موضوعی محبوب از سال ۲۰۰٤-۲۰۱۹

موضوعات کلاهبرداری، مدل‌های داده‌ای، یادگیری یکپارچه و تحول دیجیتال از جمله روندهای موضوعی در سال ۲۰۲۴ 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 از جمله موضوعات پرتکرار پژوهشگران بوده‌اند. سال ۲۰۲۱ موضوع‌های بانک، ریسک اعتباری، حکمرانی مشارکتی، ریسک نظام‌مند و امنیت اطلاعات به اوج محبوبیت در پژوهش‌ها رسیدند. در نهایت 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 ۲۰۲۰-۲۰۲٤

پاسخ به پرسش چهارم پژوهش. در نقشه موضوعی حوزه امنیت سایبری در بانک‌ها موضوع‌های محرک، تخصصی، ضرروری و نوظهور چه موضوعاتی هستند؟

این نمودار دارای دو محور چگالی و مرکزیت است. چگالی نشان‌دهنده 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 می دهد. هر چه میزان مرکزیت بیشتر باشد، احتمال اینکه آن موضوع مورد توجه 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 خوشه بندی کلیدواژه‌ها، ۴ خوشه شناسایی شد. خوشه ریسک، خوشه یادگیری ماشین، خوشه فناوری مالی و در نهایت خوشه حداکثر زیان مالی. نمودار به ۴ بخش اصلی تقسیم شده است. این چهار بخش عبارت‌اند از:

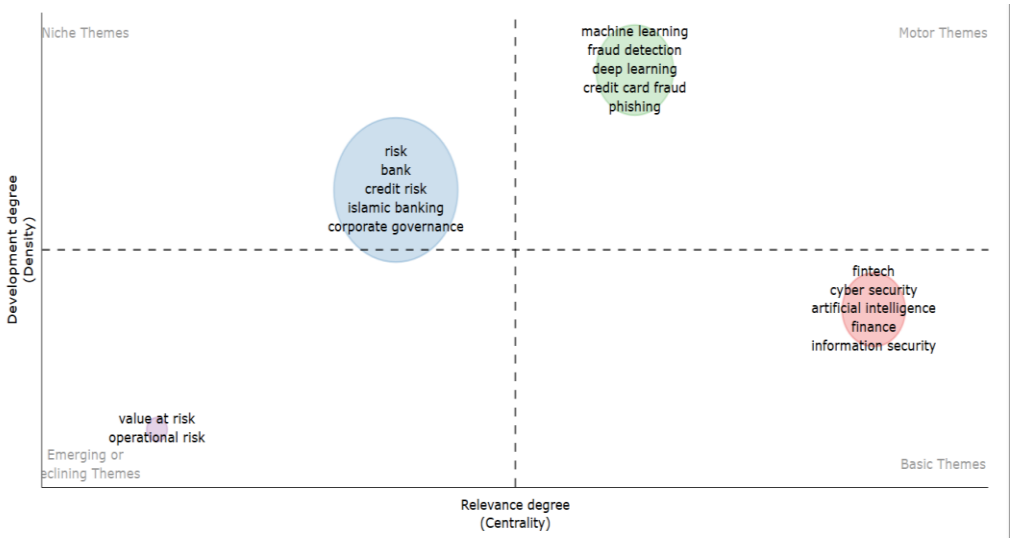
۱- ناحیه محرک و پیشران[2] بالا-راست: این ناحیه در سمت راست بالا قرار دارد و موضوعاتی را نشان می‌دهد که تأثیرگذاری بالا و تراکم بالا دارند. موضوعات این ناحیه به‌عنوان هسته و محرک اصلی پژوهش شناخته می‌شوند و از نظر ساختار و ارتباطات داخلی بین موضوعی و ارتباط با سایر موضوع‌ها غنی هستند. به علاوه این موضوعات به شدت تأثیرگذارند. این خوشه با عنوان خوشه 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[3] پایین-راست: این ناحیه در سمت راست پایین قرار دارد و شامل موضوعاتی با تأثیرگذاری بالا اما تراکم پایین یا توسعه یافتگی پایین است. این‌ها موضوعات پراستناد و مهم هستند، اما ارتباطات داخلی کمتری دارند و بیشتر به‌عنوان پایه‌های اصلی پژوهش دیده می‌شوند. موضوعات مربوط به این چارک نمودار معمولا از جمله موضوعات داغ و یا روندهای پژوهشی به حساب می‌آیند(Zhang, 2024). خوشه ی فناوری مالی شامل موضوعات فناوری مالی، امنیت سایبری، هوش مصنوعی، سرمایه و امنیت اطلاعات است. این موضوعات دارای بلوغ و پختگی کمی هستند، اما در حوزه بسیار مهم هستند.

۳-ناحیه نوظهور یا رو به افول[4] پایین- چپ: این ناحیه در سمت چپ پایین قرار دارد و شامل موضوعاتی با تأثیرگذاری پایین و تراکم پایین است. خوشه‌های مربوط به این قسمت به دو بخش قابل تقسیم‌اند: موضوعاتی که به تازگی مطرح شده‌اند و صرفا پژوهش‌های کمی به آن‌ها اختصاص یافته یا موضوعاتی که در حال فراموشی هستند و در آن حوزه موضوعی قابل طرح نیستند. بنابراین این موضوعات بیشتر در حال رشد یا در مرحله گذار هستند و ممکن است به مرور زمان به ناحیه موتور انتقال یابند یا از اهمیتشان کاسته شود. خوشه حداکثر زیان مالی که در حوزه بانکداری در این ناحیه قرار دارد شامل موضوعاتی نظیر حداکثر زیان مالی و ریسک عملیاتی است. با توجه به این خوشه و نیز نقشه مصورسازی پوششی می‌توان استنباط کرد که خوشه حداکثر زیان مالی در مرحله کاهش توجه قرار داد.

٤-ناحیه تخصصی و خاص[5] 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.خوشه ریسک شامل موضوعات ریسک، بانک، ریسک اعتباری، بانکداری اسلامی و حکمرانی مشارکتی، نشان دهنده 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 مشغولند(شکل ۶-).

[1] Walktrap
[2] Motor Themes
[3] Basic Themes
[4] Emerging or Declining Themes
[5] 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؟

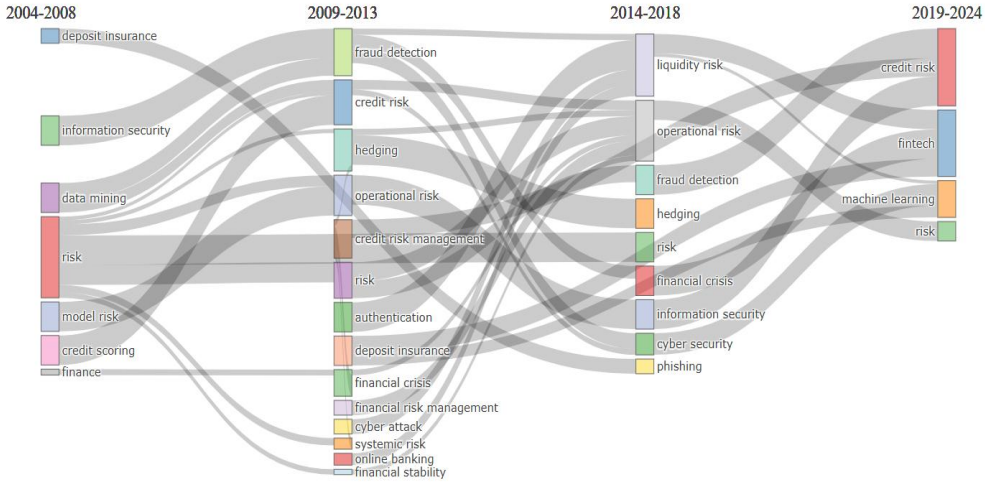
برای بررسی روند تاریخی موضوعات، بر اساس تاریخ نشر مقالات مورد بررسی ۴ دوره زمانی انتخاب شد(شکل ۷-). دوره اول از سال ۲۰۰۴ تا ۲۰۰۸ را به خود اختصاص می‌دهد. در این دوره موضوعات اصلی شامل بیمه سپرده‌ها، امنیت اطلاعات، داده‌کاوی، ریسک، ریسک مدلی، امتیازدهی اعتباری و سرمایه بوده است. دوره دوم از سال ۲۰۰۹ تا 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 است. دوره سوم از سال ۲۰۱۴ تا ۲۰۱۸ به موضوعات ریسک نقدینگی، ریسک عملیاتی، کشف کلاهبرداری، احراز هویت، ریسک، بحران مالی، امنیت اطلاعاتی، امنیت سایبری و فیشینگ پرداخته است. در نهایت دوره چهارم از سال ۲۰۱۹ تا ۲۰۲۴ موضوعات اصلی ریسک اعتباری، فناوری مالی، یادگیری ماشین و ریسک بوده است.

مهمترین موضوع مورد بحث در سال‌های اولیه شکل‌گیری پژوهش‌های حوزه امنیت سایبری در بانک به مسئله کلی ریسک مربوط بوده است که در سال‌های بعد این موضوع جزئی‌تر شده است. موضوع اصلی پژوهش در فاصله سال‌های ۲۰۰۹-۲۰۱۳ موضوع کشف کلاهبرداری بوده است. این امر نشان می‌دهد که در سال‌های مورد بررسی، مسئله فعالیت‌های مشکوک و فریبنده و دسترسی‌های غیرمجاز از جمله دغدغه‌های اصلی آن دوره بوده است. این موضوع در دوره بعد ۲۰۱۴-۲۰۱۸ به موضوعات تخصصی‌تر نظیر ریسک نقدینگی، بحران مالی و امنیت سایبری تبدیل شده 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 مورد توجه قرار گرفت و مفاهیمی که به صورت خاص به انواع ریسک‌ها در محیط بانکی می‌پردازند نظیر ریسک اعتباری، ریسک عملیاتی، مدیریت ریسک و نظایر آن به صورت جزئی‌تر مورد توجه قرار گرفتند.

در فاصله سال‌های ۲۰۱۴ تا ۲۰۱۸ مهمترین موضوع ریسک نقدینگی بوده است که از سه مفهوم احراز هویت، حمله سایبری و بانکداری پیوسته در سال‌های ۲۰۰۹-۲۰۱۳ نشات گرفته است. می‌توان اینطور استنباط کرد که چنانچه احراز هویت مشتریان بانک‌ها دچار اختلال شود و یا به واسطه حمله سایبری هکرها به اطلاعات مشتریان دسترسی داشته باشند، احتمال ریسک

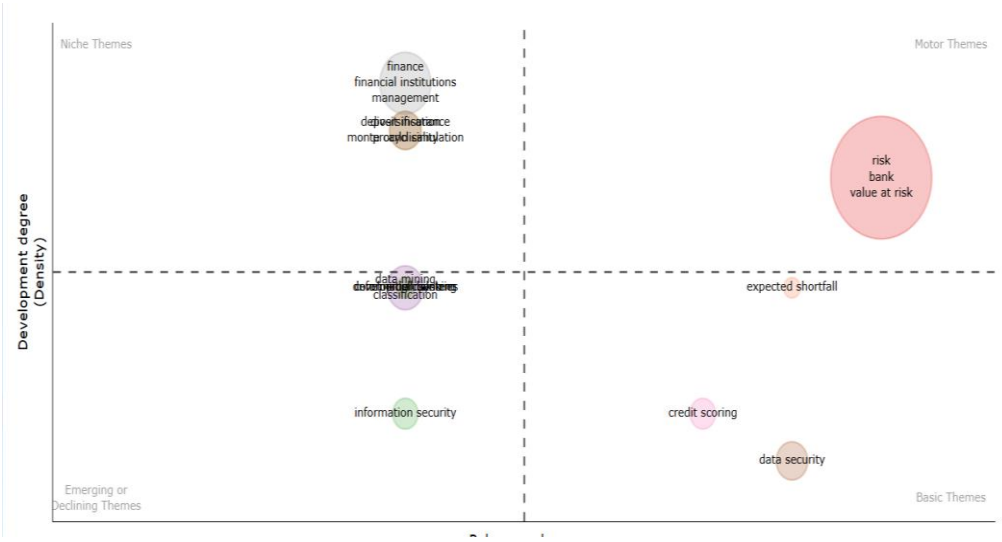
نقدینگی وجود دارد و این امر با وجود اهمیت بانکداری پیوسته، روز به روز بیشتر خواهد شد. به علاوه در این دوره شاهد اهمیت موضوع امنیت در فضای دیجیتالی در بانکداری هستیم.

در دوره چهارم در سال‌های ۲۰۱۹ –۲۰۲۴، مفاهیم اصلی بیشتر به سمت فناوری تمایل پیدا کرده است و مفهوم یادگیری ماشین به عنوان یک مفهوم جدید در این سال‌ها ظهور کرده است. با این حال هنوز ریسک اعتباری به عنوان موضوع اصلی در این حوزه مطرح است. در این دوره شاهد حضور فناوری‌های هوشمند و جدید در حوزه بانک و بانکداری هستیم.



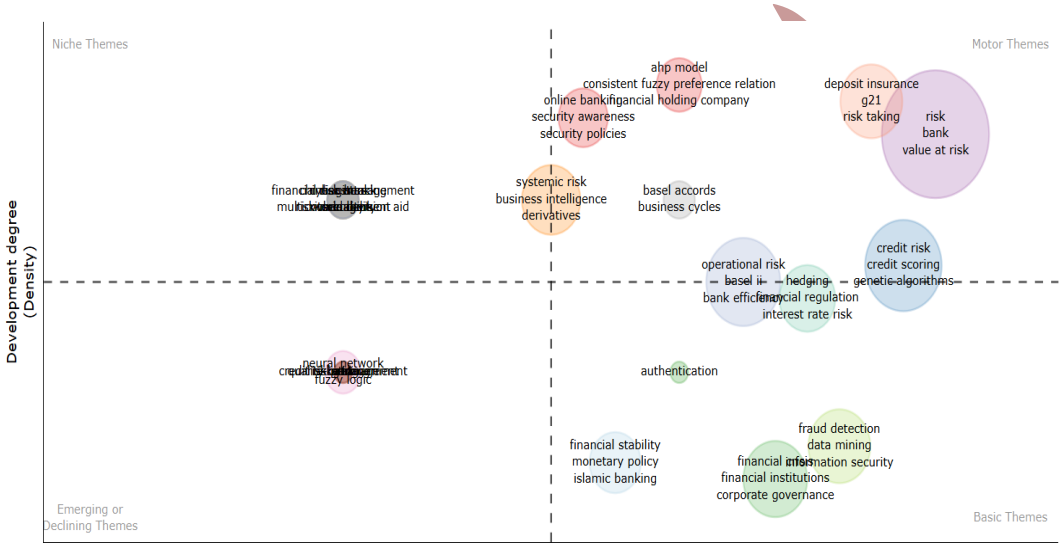
شکل ۷. روندهای موضوعی مهم و پرتکرار در بازه‌های زمانی مختلف و تحول آن‌ها

در سال های ۲۰۰۴ تا ۲۰۰۸ خوشه داده کاوی، بانکداری تجاری و امنیت اطلاعات از جمله موضوعات نوظهور در حوزه امنیت سایبری در بانک‌ها هستند. خوشه امنیت داده، امتیازدهی اعتباری و متوسط ضرردهی بانک‌ها از جمله موضوعات کاربردی و ضروری دوره مذکور محسوب می‌شدند. این موضوعات از جمله موضوعات اساسی این دوره به حساب می‌آیند، اما هنوز توسعه نیافته‌اند. خوشه ریسک و موضوعات مرتبط با آن به عنوان خوشه پیشران و محرک در این سال‌ها به حساب می‌آیند. خوشه سرمایه شامل موضوعات مؤسسه‌های سرمایه‌ای و مدیریت و خوشه تنوع بخشی به عنوان موضوعات تخصصی از سوی برخی پژوهشگران مورد توجه قرار گرفته است. این موضوعات در سال‌های ابتدایی خود دارای ارتباط قوی با سایر خوشه‌های موضوعی نیستند، اما به آن‌ها به صورت عمیق‌تر پرداخته شده است (شکل ۸–).



شکل ۸. روند تحول موضوعات در فاصله سال‌های ۲۰۰٤-۲۰۰۸

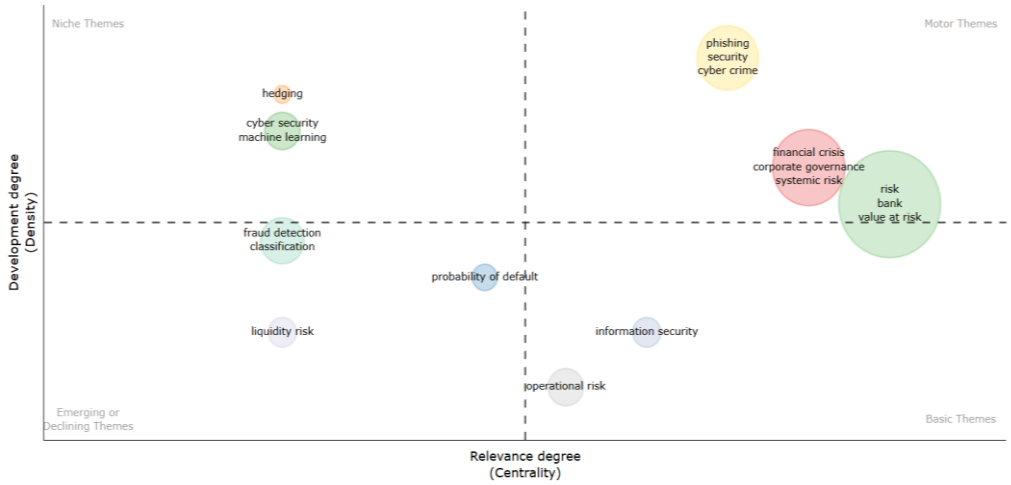
تنوع و تعدد خوشه‌ها در سال‌های ۲۰۰۹ تا ۲۰۱۳ قابل توجه است، این امر به ویژه در ناحیه ضروری و ناحیه محرک (پیشران) نمود بیشتری دارد. خوشه‌های موضوعی شبکه عصبی و خوشه مدیریت ریسک اعتباری به عنوان خوشه‌های نوظهور در سال‌های ۲۰۰۹-۲۰۱۳ در پژوهش‌های حوزه امنیت سایبری در محیط بانکداری ظاهر می‌شوند. در این دوره شاهد هستیم که انواع ریسک‌ها نظیر ریسک اعتباری، ریسک سیستمی و ریسک عملیاتی خود به عنوان خوشه‌های مجزا مطرح شده‌اند. خوشه‌های جدیدی به عنوان خوشه‌های محرک شامل خوشه بانکداری پیوسته، خوشه احراز هویت، خوشه بیمه سپرده گذاری و خوشه مدل سلسله مراتبی، خوشه توافق نامه‌های بازل (مقرارت بین‌المللی به منظور مدیریت ریسک در بانک‌ها)، خوشه پوشش ریسک[1] از جمله خوشه‌های اصلی این دوره به عنوان موضوع‌های پیشران مطرح شدند. خوشه‌های پایداری سرمایه، بحران سرمایه، تشخیص کلاهبرداری و احراز هویت نیز در این دوره به عنوان موضوعات ضروری و پایه مطرح شدند؛ موضوعاتی که میزان ارتباط آن‌ها با سایر خوشه‌ها بیش‌تر است(شکل ۹-).



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

موضوع ریسک نقدینگی از جمله خوشه‌های نوظهور در دوره زمانی سوم ۲۰۱۴-۲۰۱۸ است. در این دوره خوشه کشف کلاهبرداری به ناحیه موضوعی رو به افول وارد می‌شود. بدین معنی که خوشه مذکور در سال‌های مورد بررسی به عنوان موضوع پژوهشی مهم مورد توجه نیست. خوشه فیشینگ نیز به عنوان خوشه جدید در این سال‌ها به عنوان خوشه پیشران و محرک مورد توجه پژوهشگران قرار می‌گیرد(شکل ۱۰-).

[1] hedging



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

تنوع موضوعی در سال‌های ۲۰۱۹-۲۰۲۴ نسبت به دو دوره قبل آن کمتر شده است. خوشه یادگیری ماشین و موضوعات آن خوشه به عنوان موضوع محرک و پیشران، خوشه ریسک اعتباری به عنوان موضوع تخصصی، خوشه ریسک به عنوان خوشه رو به افول و خوشه فناوری مالی به عنوان خوشه ضروری مطرح است(شکل ۱۱-).

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

بحث و نتیجه‌گیری

اهمیت امنیت سایبری در بانک‌ها با توجه به حجم داده‌های زیاد و با ارزش و نیز اهمیت حریم شخصی افراد و اطلاعات آن‌ها در این مراکز روز به روز بیشتر می‌شود. اکثر پژوهش‌های حوزه امنیت سایبری و امنیت اطلاعات حاصل همکاری گروهی است (Loan et al., 2022). نتایج این پژوهش نیز نشان داد درصد بالایی از آثار با همکاری گروهی نگارش شده است.

بررسی نقشه مصورسازی پوششی با استفاده از نرم‌افزار ووس ویوور گویای آن است که در سال‌های اخیر به طور متوسط اهمیت موضوع‌های یادگیری ماشین، یادگیری عمیق، فناوری مالی و هوش مصنوعی از سوی پژوهشگران بیشتر شده است. نتایج پژوهش‌های لون، بیسما و ناهید (Loan et al., 2022) و شفچوک و مارتسنیوک (Shevchuk & Martsenyuk,

(2024. در مورد یادگیری ماشین با نتایج این پژوهش تطابق دارد. با این وجود با نتایج پژوهش‌های پورمددکار (Pourmadadkar et al., 2024) و امت (Omote et al., 2024) متفاوت است. دلیل این تفاوت می‌تواند مربوط به بررسی موضوع خاص‌تر در حوزه امنیت سایبری (سیستم‌های سایبری فیزیکی) در پژوهش پورمددکار و تفاوت سال‌های مورد بررسی در پژوهش امت (Omote et al., 2024) (۲۰۱۰–۲۰۱۹) باشد.

موضوع حداکثر زیان احتمالی و بحران مالی که از جمله موضوع‌های محبوب در سال ۲۰۱۶ بوده‌اند، محبوبیت خود را بعد از آن سال‌ها از دست داده‌اند. نگاهی به نقشه مصورسازی پوششی کلیدواژه‌ها نیز این امر را تایید می‌کند.

از جمله مهمترین روندهای پژوهشی که در سال ۲۰۲۴ در حوزه امنیت سایبری در بانک‌ها به اوج محبوبیت خود رسیدند، موضوع کلاهبرداری بود که با وجود اهمیت بانکداری اینترنتی و اپلیکیشن‌های تلفن همراه این موضوع بیش از پیش اهمیت یافته است. به علاوه موضوع یادگیری یکپارچه در سال ۲۰۲۴ مطرح و در همان سال نیز به اوج محبوبیت خود رسیده است. این موضوع از جمله تازه‌ترین و پیچیده‌ترین روش‌های یادگیری ماشین است که بدون ارسال داده، مدل‌ها آموزش می‌بینند. بحث یادگیری ماشین نیز موضوع مهم سال ۲۰۲۳ بوده است. نتایج پژوهش شفچوک و مارتسنیوک (Shevchuk & Martsenyuk, 2024) در حوزه شبکه عصبی و امنیت سایبری منطبق با پژوهش حاضر است. آن‌ها نیز موضوع یادگیری ماشین را به عنوان پرطرفدارترین موضوع مورد بررسی پژوهشگران معرفی کردند.

در سال‌های ابتدایی پژوهش (۲۰۰۴–۲۰۰۸) در این حوزه، خوشه‌های امنیت اطلاعات، داده‌کاوی و بانکداری تجاری به عنوان مفاهیم اولیه و مهم پژوهش ظهور کردند. در دوره زمانی دوم(۲۰۰۹–۲۰۱۳) خوشه‌های امنیت اطلاعات و داده‌کاوی وارد خوشه بزرگ‌تر تشخیص کلاهبرداری شدند و از موضوعات نوظهور پژوهش به موضوعات ضروری پژوهش در این حوزه تبدیل شدند. ربط موضوعی خوشه‌هایی نظیر داده‌کاوی، امنیت اطلاعات و تشخیص کلاهبرداری به دیگر موضوعات مرتبط با امنیت سایبری در محیط بانکداری با توجه به افزایش مرکزیت بیشتر شد. خوشه امنیت اطلاعات در دوره زمانی سوم (۲۰۰۹–۲۰۱۳) همچنان به عنوان خوشه ضروری در حوزه امنیت سایبری جای گرفته است، با این تفاوت که در این دوره خود به عنوان هسته اصلی خوشه‌ای مستقل است. نتایج پژوهش لون، بیسما و ناهید (Loan et al., 2022) نیز نشان داد که امنیت اطلاعات متداول‌ترین حوزه موضوعی مورد بررسی در فاصله سال‌های ۲۰۱۱ تا ۲۰۲۰ در کنار سایر موضوعات نظیر امنیت، امنیت کامپیوتری، حفظ محرمانگی و نظایر آن بوده است.

خوشه امتیازدهی اعتباری که در سال‌های ۲۰۰۴–۲۰۰۸ از جمله موضوعات ناحیه ضروری به حساب می‌آمد، در فاصله سال‌های ۲۰۰۹–۲۰۱۳ وارد خوشه ریسک اعتباری شده و در مرز بین ناحیه ضروری و ناحیه محرک قرار می‌گیرد. این بدین معنی است که این موضوع همراه با موضوعات مربوط به خوشه خود در این دوره زمانی از جمله موضوعات پویا و پیش رونده پژوهشی محسوب می‌شود. به علاوه این خوشه در عین ارتباط قوی با موضوعات داخل خوشه خود، با خوشه‌های دیگر نیز در حال برقراری ارتباطات موضوعی مناسبی است. این امر نشان دهنده آن است که ارتباط بین حوزه‌ای موضوعات در این خوشه‌ها با خوشه‌های دیگر در همین ناحیه افزایش یافته است و احتمال شکل‌گیری موضوعات جدیدتر با ترکیب خوشه‌ها انتظار می‌رود. خوشه ریسک که شامل انواع ریسک‌ها نظیر ریسک عملیاتی، بازاری و اعتباری است، به عنوان خوشه محرک در دو دوره زمانی ۲۰۰۴–۲۰۰۸ و ۲۰۰۹–۲۰۱۳ به حساب می‌آید؛ با این تفاوت که در دوره دوم در کنار تأثیرگذاری، بر میزان توسعه یافتگی این خوشه افزوده شده است. این خوشه در دوره بعد ۲۰۱۴–۲۰۱۸ در مرز بین ناحیه پیشران و ناحیه ضروری قرار می‌گیرد و از توسعه یافتگی آن در این دوره کاسته می‌شود و در نهایت در دوره چهارم وارد ناحیه نوظهور یا رو به افول می‌شود که به نظر می‌رسد به عنوان خوشه‌ای که به اشباع رسیده است در سال‌های ۲۰۱۹–۲۰۲۴ مطرح شده است. تأثیر این خوشه هم به لحاظ توسعه یافتگی و هم به لحاظ تأثیرگذاری و ارتباط با سایر خوشه‌ها کمرنگ‌تر می‌شود.

خوشه سرمایه که به عنوان خوشه تخصصی در فاصله سال‌های ۲۰۰۴–۲۰۰۸ مطرح بود، در دوره زمانی بعد آن (۲۰۰۹–۲۰۱۳) به خوشه‌های جزئی‌تری تقسیم شده است که همگی از جمله خوشه‌های ضروری حوزه امنیت سایبری محسوب می‌شوند. خوشه‌هایی نظیر بحران سرمایه، پایداری سرمایه و مدیریت ریسک سرمایه از جمله خوشه‌های خاص دوره دوم محسوب می‌شود.

خوشه کشف کلاهبرداری به عنوان خوشه ضروری در فاصله سال‌های ۲۰۰۹–۲۰۱۳ مطرح، سپس به عنوان خوشه‌ای مستقل و به عنوان مرکز اصلی خوشه در سال‌های ۲۰۱۴–۲۰۱۸ به عنوان خوشه موضوعی رو به افول مطرح می‌شود. با این وجود در دوره زمانی چهارم ۲۰۱۹–۲۰۲۴ به عنوان بخشی از خوشه یادگیری ماشین به عنوان موضوع پیشران آن دوره مطرح است. در خوشه یادگیری ماشین سایر موضوعات مرتبط نظیر یادگیری عمیق، شبکه عصبی، کلاهبرداری کارت اعتباری، کشف آنومالی، ماشین بردار حمایتی، کارت اعتباری وارد شدند.

تحلیل منطقی سیر تحولات پژوهشی در حوزه امنیت سایبری در بانک‌ها طی دو دهه گذشته حاکی از گذار مفهومی از موضوعات سنتی نظیر "ریسک سرمایه" و "امنیت اطلاعات" به مفاهیم نوینی نظیر "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 داده‌اند که موضوع‌های سنتی در دوره‌های زمانی نزدیک‌تر به زمان حاضر دیگر به عنوان خوشه مستقل مطرح نیستند، این موضوع‌ها با موضوع‌های جدیدتر ترکیب شده و خود خوشه‌ای مستقل را تشکیل داده‌اند. به علاوه در برخی موضوعات، خوشه‌های سنتی جای خود را به خوشه‌هایی با موضوعات میان رشته‌ای داده‌اند. تغییرهای بوجود آمده نشان از رشد و بلوغ برخی موضوع‌ها، شکوفایی موضوع‌های جدید و نزدیک‌تر شدن محتوای موضوعی برخی موضوع‌ها به یکدیگر است. در دوره‌های زمانی اولیه شاهد شکل‌گیری و اهمیت موضوع‌هایی هستیم که هدف آن پاسخ به تهدیدهای حوزه امنیت سایبری است. زمانی که بعد از مواجه شدن با ریسک‌های متعدد و ناشناخته این حوزه، درصدد یافتن پاسخ به حملات سایبری به منظور کاهش میزان خسارات و هزینه‌های وارده بوده‌ایم. هم اکنون موضوع‌های مورد توجه پژوهشگران یک قدم فراتر رفته و به سمت آینده‌نگری این حوزه گام برداشته است. پژوهشگران حوزه امنیت سایبری با تأکید بر محیط بانکداری به دنبال کشف شیوه‌های نو به واسطه الگوریتم‌های پیچیده فناورانه نظیر یادگیری یکپارچه، یادگیری ماشین و یادگیری عمیق هستند تا بتوانند قبل از وقوع خطرات احتمالی، آن‌ها را پیش‌بینی نموده و راه حل هوشمندانه‌ای را با بهینه‌ترین هزینه‌ها در نظر گیرند.

بنابراین نگاه به حوزه امنیت سایبری در محیط بانکداری بیش از پیش نیازمند نگاهی فناورانه و مبتنی بر تحلیل داده‌های کلان است، تا بتواند با یادگیری و کشف موضوع‌های جدید، روندهای پنهان در داده‌ها را شناسایی نموده و به مدیران و متخصصان این حوزه کمک نماید.

پیشنهادهای اجرایی پژوهش

- با توجه به پایه و اساسی بودن موضوعات مربوط به خوشه امنیت سایبری، به مدیران حوزه 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 به کارگیرند.
- با توجه به اینکه موضوع‌های یادگیری یکپارچه، مدل‌های داده‌ای و تحول دیجیتال، در سال ۲۰۲۴ 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 ۲۰۲۴ 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 نمایند.

- با توجه به این که فناوری مالی موضوع اصلی در سال ۲۰۲۳ بوده است، پیشنهاد می‌شود سایت‌های به روز مرتبط با این حوزه نظیر فینکسترا[1] از سوی متخصصان حوزه امنیت سایبری روزانه مورد مطالعه قرار گیرد. به علاوه با توجه به اهمیت موضوع هوش مصنوعی، بخشی از سایت که به طور ویژه به موضوع هوش مصنوعی در امور مالی می‌پردازد، مورد توجه قرار گیرد. همچنین سایت سی آی او[2] در زمینه تحول دیجیتال می‌تواند برای متخصصان این حوزه مفید واقع شود.

پیشنهاد برای پژوهش‌های آتی

- بررسی موضوع‌های نوظهور و تخصصی در حوزه 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؛
- با توجه به اینکه موضوع بانکداری اسلامی یکی از موضوع‌های اصلی پژوهشی در سال ۲۰۲۲ بوده است پیشنهاد می شود علل اهمیت این موضوع در آن سال‌ها بررسی گردد تا مشخص شود وجه افزوده این نوع بانک‌ها نسبت به سایر بانک‌های جهانی چه 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 انجام شده و تحت حمایت هیچ سازمانی قرار نداشته است.

فهرست منابع

آزادسنجری، 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 زرینی، ا (۱۴۰۲). تحلیلی بر کاربردهای دادهکاوی در صنعت بیمه بر اساس شبکهٔ همرخدادی 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 سیاست های پولی بانک مرکزی: با نگاهی به «عملیات بازار باز» (بر مبنای مدارک نمایه شده در پایگاه وب آوساینس در بازه زمانی ۱۹۸۱ –۲۰۲۰). مطالعات و سیاست‌های اقتصادی، ۱۹(۱)، ۲۵-۵۲. https://doi.org/10.22096/esp.2023.522723.1468

مردانی شهربابک، س.، و زالی نژاد، ع. (۱۴۰۰۳). ارائه چارچوب نوین تعالی فرهنگ امنیت سایبری در بانکداری مدرن [مقاله کنفرانسی]. یازدهمین همایش سالانه بانکداری نوین و نظام‌های پرداخت. تهران. https://mbps.mbri.ac.ir/fa/page.php?rid=94

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.

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

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. Int. J. Adv. Comput. Sci. Appl, 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. The 13th International Conference on Management, World Trade, Economics, Finance and Social Sciences, 1–21. https://civilica.com/doc/1689447 [In Persian].

Askariyan Kakh, E., Ghavidel, S., & Riyahinia, 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). Economic Studies and Policies, 19, 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. 2nd Conference on Organizational Process Engineering and Management, 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), 1–33. https://doi.org/10.1142/S0219649216500441

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. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 12199 LNCS, 242–253. 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

Ezeji, C. L. (2022). Disruptive technology on the cyberspace: The Contestation Between Criminal Justice System and Cybercriminals. International Journal of Development Studies, 5(1), 192–214. https://doi.org/10.26772/cijds-2022-05-01-012

Hajiyan, H., & Zarjini, A. (2024). 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., Moghaddam, H. S., & Chelak, A. M. (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), 1–22. 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(3), 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

Mardani Shahrbabak, S., & Zalinejad, A. (2024). Presenting a Novel Framework for Enhancing Cybersecurity Culture in Modern Banking. 11th Annual Conference on Modern Banking and Payment Systems, 1–21. https://mbps.mbri.ac.ir/fa/page.php?rid=94[In Persian].

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. ArXiv Preprint ArXiv:1602.02412. https://arxiv.org/abs/1602.02412

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), 1–14. https://doi.org/10.30878/ces.v29n3a11

Nesakumar, D., Arthi, S., Lahari, A., Geetha, M., Pavithra, K. N., & Mugilan, P. (2022). Smart ATM card for multiple bank accounts. 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), 1228–1232. 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%0D

Orosco-Fabian, J. R. (2024). Cybersecurity in higher education: a bibliometric review. Revista Digital de Investigación En Docencia Universitaria, 18(2), 1–12. https://doi.org/10.19083/ridu.2024.1933

Petrosyan, A. (2024). Annual cost of cybercrime worldwide 2018-2029. 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://doi.org/10.1109/TEM.2024.3489273

Raghuram, S., Tuertscher, P., & Garud, R. (2010). 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://doi.org/10.37591/joces.v11i1.812

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

Van Raan, A. F. (2014). Advances in bibliometric analysis: research performance assessment and science mapping. In 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 no. 43. Australian Institute of Criminology. https://doi.org/10.52922/sr77031

von Solms, B., & von Solms, R. (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

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, 1–25. 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

Zhao, W., Mao, J., & Lu, K. (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