پایش کتابشناختی علم و فناوری در حوزه امنیت سایبری

علیرضا رضوانیان[۱]، سید مهدی وحیدی پور[۲]

[۱]استادیار، گروه مهندسی کامپیوتر، دانشگاه علم و فرهنگ، تهران
rezvanian@usc.ac.ir
[۲]استادیار، دانشکده مهندسی برق و کامپیوتر، دانشگاه کاشان، کاشان
vahidipour@kashanu.ac.ir

چکیده

تردیدی نیست که فراوانی استفاده از منابع دیجیتالی و پدیدار شدن فناوری‌های نوظهور در زندگی روزانه افراد رو به افزایش است و همچنین گستردگی محتوا و اطلاعات متنوع، امکان نفوذ و سوء استفاده از افراد و سازمان‌ها را روز به روز افزایش می‌دهد. مطالعات و پژوهش‌های گوناگونی نیز برای حفاظت از منابع دیجیتالی و ارائه راه‌کارهای امنیت سایبری از جنبه‌های مختلف پژوهشی تا صنعتی توسط پژوهشگران و صنعتگران در سال‌های اخیر ارائه شده است. بنابراین، با توجه به اهمیت موضوع امنیت در فضای سایبری، در این مقاله پایش کتابشناختی علم با بررسی مقالات منتشر شده و پایش فناوری با بررسی ثبت اختراعات، مورد بررسی قرار گرفته است. برای بررسی مقالات از منابع نمایه‌شده موجود در پایگاه علمی اسکپوس استفاده شده است و برای بررسی ثبت اختراعات از داده‌های موجود در لنز استفاده شده است. در نهایت گزارش‌های مختلف به تفکیک آمار به‌دست آمده از زوایای مختلف و بر اساس شاخص‌های مختلف ارائه شده است.

کلمات کلیدی: امنیت سایبری، تحلیل کتابشناختی، پایش علم، پایش فناوری.

۱ مقدمه

امروزه با توجه به گسترش کاربردهای دیجیتالی در زندگی بشری، خیلی از نیازهای روزانه انسان‌ها توسط سیستم‌های دیجیتالی با استفاده از کامپیوترهای شخصی، تبلت، موبایل و حسگرهای هوشمند به صورت از راه دور و بدون نیاز به حضور فیزیکی انجام می‌پذیرد. این امر از یک طرف سهولت و مزایای فراوان را برای افراد فراهم آورده و از طرف دیگر افزایش اهمیت امنیت سایبری در سیستم‌های دیجیتالی مختلف مورد استفاده در زمینه‌های اجتماعی، فرهنگی، کاری، تجاری، سازمانی، اداری و کاربردهای مختلف روزانه بشری را نشان می‌دهد [۱]. در این مقاله پس از معرفی مفاهیم اولیه از امنیت سایبری و ارائه آمار متنوعی از اهمیت امنیت در فضای سایبری، در نهایت پایش کتابشناختی علم و فناوری در حوزه امنیت سایبری ارائه شده است.

۲ امنیت سایبری

امنیت سایبری شامل مجموعه‌ای از فناوری‌ها و فرآیندهای طراحی شده به منظور از حفاظت از کامپیوتر، سیستم، شبکه، برنامه‌های کامپیوتری، موبایل و داده‌ها در برابر حملات دیجیتالی است. به طور معمول هدف این نوع از حملات، دسترسی غیرمجاز، تغییر، تخریب و یا از بین بردن اطلاعات مهم و حیاتی، استخراج پول از کاربران، یا ایجاد خلل و توقف در فرآیندهای یک کسب و کار است. امروزه طراحی، پیاده‌سازی و اجرای اقدامات موثر امنیت سایبری در عمل چالش برانگیز است، زیرا تعداد فراوانی از دستگاه‌های دیجیتالی نسبت به جمعیت افراد جامعه وجود دارد و مهاجمان با نیت‌های مختلف هر روز با نوآوری و ابتکارات بیشتری دست به حملات و خرابکاری خود می‌زنند [۲]. یکی از رویکردهای موفقیت آمیز در امنیت سایبری ایجاد چندین لایه حفاظت در کامپیوتر، شبکه، برنامه یا داده‌های موبایل است تا حداقل امنیت لازم فراهم شود. در یک سازمان، کاربران، فرایندها و فناوری‌ها بایستی همگی به صورت یکپارچه به یکدیگر مرتبط باشند تا دفاع موثری در برابر حملات اینترنتی و سایبری ایجاد کنند [۳].

برخی توصیه‌ها برای کاربران، سازمان‌ها و فناوری در ادامه ذکر شده است:

- کاربران بایستی ضرورت اصول امنیتی داده‌های اساسی مانند انتخاب رمز عبور قوی، مراقبت از پیوست‌ها در ایمیل و پشتیبان گیری از داده‌ها را درک کنند. در این مورد آموزش دوره‌ای کاربران می‌تواند مفید باشد.
- سازمان‌ها بایستی چارچوبی برای چگونگی مقابله با حملات سایبری داشته باشند. یک چارچوب مناسب می‌تواند سازمان‌ها را هدایت کند. بدین صورت که چگونه سازمان می‌تواند حملات را شناسایی کند، سیستم‌ها را محافظت کند، تهدیدات را شناسایی و پاسخ دهد، و نسبت به حملات رخ داده محفوظ باشند.
- فناوری برای استفاده توسط سازمان‌ها و افراد نیازمند مجهز شدن به ابزارهای امنیتی مستحکم است تا از حملات سایبری محافظت کند. در حوزه فناوری، سه بخش اصلی باید محافظت شوند: دستگاه‌های پایه‌ای مانند رایانه، دستگاه‌های هوشمند، روتر، شبکه و فناوری رایج مورد استفاده برای محافظت از این موارد شامل فایروال‌های نسل بعدی، فیلترسازی سرویس‌های نام دامنه، حفاظت از نرم‌افزارهای مخرب، نرم‌افزار آنتی‌ویروس و راه‌حل‌های امنیتی ایمیل است.

۱.۲ امنیت سایبری از دیدگاه آمار

براساس آمار بدست آمده از حوادث مرتبط با امنیت سایبری در سال ۲۰۲۲ در سطح جهان، حدود ۱۶۰۰۰ حادثه در صنایع مختلف از ضعف‌های مربوط به امنیت سایبری دچار خسارت شده‌اند.[۱] به عنوان مثال تخمین زده شده است که آژانس اعتباری Equifax در سال ۲۰۱۹ حدود ۵۷۵ میلیون دلار خسارات ناشی از امنیت سایبری را داشته است.[۲] گزارش تفکیکی صنایع خسارت دیده مرتبط با امنیت سایبری در سال ۲۰۲۲ در جدول ۱ فهرست شده است. بنابراین امروزه وجود سیستم تشخیص نفوذ امنیت سایبری به منظور اجتناب از

[1] https://www.statista.com/statistics/194246/cyber-crime-incidents-victim-industry-size
[2] https://www.statista.com/topics/1731/smb-and-cyber-crime/

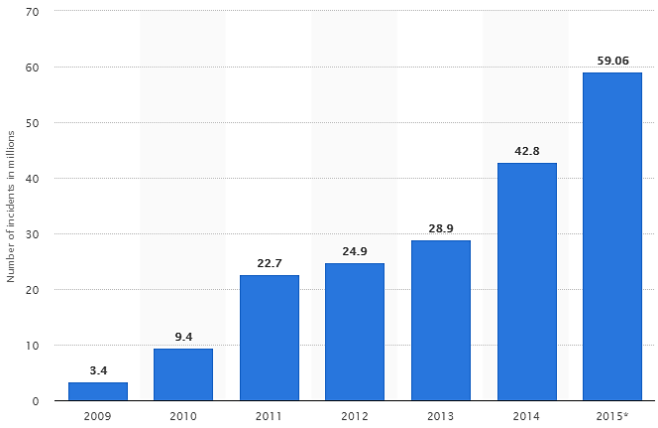
تهدیدات و حملات مختلف برای سازمان‌ها نفوذگران ضروری و حیاتی است [۴].

جدول ۱: گزارش تفکیکی صنایع خسارت دیده مرتبط با امنیت سایبری در سال ۲۰۲۲

مقیاس صنعت / نام صنعت	بزرگ	کوچک	نامشخص	مجموع
اقامتی	۲	۴	۲۴۸	۲۵۴
اداری	۱۴	۸	۱۶	۳۸
کشاورزی	۵	۱	۶۰	۶۶
ساخت و ساز	۱	۷	۷۹	۸۷
آموزش	۱۵	۶۳	۴۱۸	۴۹۶
سرگرمی	۳	۱۳	۴۱۶	۴۳۲
مالی	۳۰	۷۰	۱۷۲۹	۱۸۲۹
سلامت	۱۵	۲۸	۴۷۹	۵۲۲
اطلاعات	۱۱۰	۴۵	۱۹۵۰	۲۱۰۵
مدیریت	۰	۱	۸	۹
ساخت	۲۴	۳۷	۱۷۵۳	۱۸۱۴
معدن	۰	۲	۲۳	۲۵
سایر خدمات	۲	۷	۱۳۴	۱۴۳
خدمات حرفه ای	۵۴	۱۷۶	۱۱۶۶	۱۳۹۶
مدیریت دولتی	۱۱۰	۸۷	۳۰۷۳	۳۲۷۰
املاک	۵	۱۵	۶۳	۸۳
خرده فروشی	۴۴	۶۲	۲۹۸	۴۰۴
عمده فروشی	۲۵	۱۳	۳۱۱	۳۴۹
حمل و نقل	۶	۱۲	۹۹	۱۱۷
خدمات رفاهی	۲۲	۴۲	۳۲	۹۶
ناشناخته	۲	۱	۵۱۹۹	۲۷۷۷
مجموع	۴۸۹	۶۹۴	۱۵۱۲۹	۱۶۳۱۲

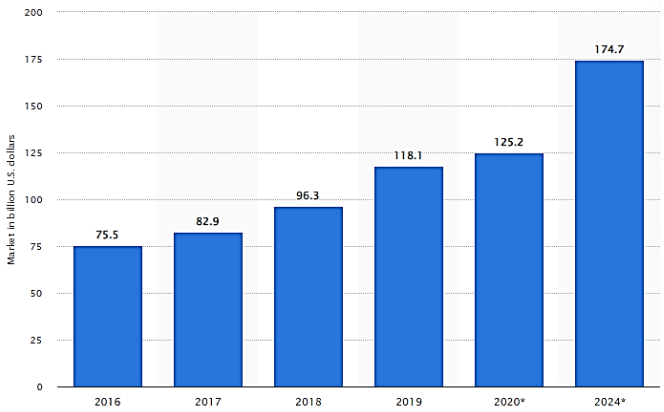
با توجه به افزایش فزاینده تعداد کاربردهای برخط و الکترونیکی مورد استفاده توسط کاربران، وجود سرویس‌های فراوان برخط، وجود داده‌های زیاد و ترافیک بالا، نوع تهدیدات و حملات به حالت پیشرفته‌تر، فزاینده‌تر و هدف‌دارتری درآمده است که اغلب مراکز داده‌ای، خدماتی، دولتی، صنعتی، صنایع دفاعی و نظامی به طور هدفمند و مستمر توسط نفوذگران مورد حمله قرار می‌گیرند [۵]. آمار افزایشی تعداد حوادث مرتبط

با امنیت سایبری در سطح جهان در بازه زمانی ۲۰۰۹ تا ۲۰۱۵ در شکل ۱ ارائه شده است.



شکل ۱: آمار افزایشی تعداد حوادث مرتبط با امنیت سایبری در سطح جهان در بازه زمانی ۲۰۰۹ تا ۲۰۱۵

بدین ترتیب روش‌های سنتی با استفاده از تکنیک‌های آماری، مبتنی بر فراوانی و مبتنی بر الگو صرفاً برای شناسایی حملات قدیمی و تکراری مناسب هستند ولی به منظور شناسایی و جلوگیری از تهدیدات سایبری نوین، پیشرفته و پیچیده امروزی عملاً ناکارآمد محسوب می‌شوند [۶]. بنابراین استفاده از روش‌های هوشمند و نوین براساس داده‌کاوی و شناسایی الگوهای مهم در حملات حائز اهمیت است. پیش‌بینی شده است که تا سال ۲۰۲۴ بیش از ۱۷۴ میلیارد دلار از سهم بودجه به تکنولوژی‌های امنیت اطلاعات اختصاص یابد.[۳] روند افزایشی این تخصیص بودجه از سال ۲۰۱۶ و پیش‌بینی برای سال‌های بعد از آن تا ۲۰۲۴ در شکل ۲ گزارش شده است.



شکل ۲: آمار تخصیص بودجه در فناوری امنیت اطلاعات برای سال‌های ۲۰۱۶ تا ۲۰۲۴

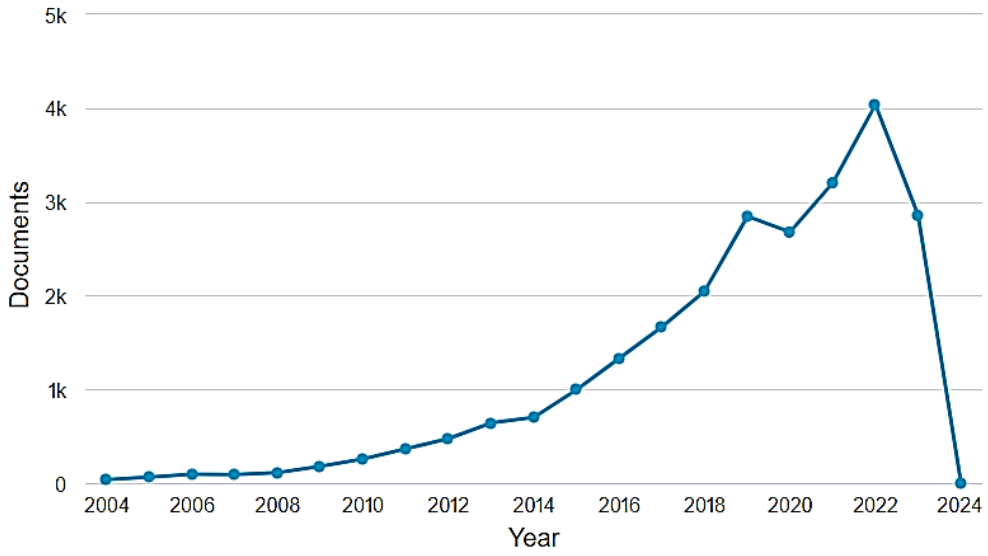
[3] https://www.statista.com/statistics/640141/worldwide-information-security-market-size/

۳ روش پژوهش

فرآیند پژوهش به صورت کتابشناختی [۷] انجام شده است؛ این فرایند شامل استخراج منابع مطالعاتی مرتبط با کارهای انجام شده در رابطه با امنیت سایبری است که در آن تحلیل کتابشناختی از دو منظر انتشار مقالات به عنوان پایش علمی و ثبت اختراعات به عنوان پایش فناوری مورد بررسی قرار گرفته است. انتشار مقالات اهمیت موضوع در حوزه علمی و شکل‌گیری حوزه‌های پژوهشی حال و آینده را مشخص می‌کند. ثبت اختراعات، اهمیت تجاری شدن موضوع در حوزه‌های کاربردی و صنعتی را مشخص می‌کند، بدین مفهوم که نیاز به حل یک مشکل در قالب یک پژوهش به یک فناوری کاربردی قابل خرید و فروش مبدل شده است.

۱.۳ پایش مقالات علمی

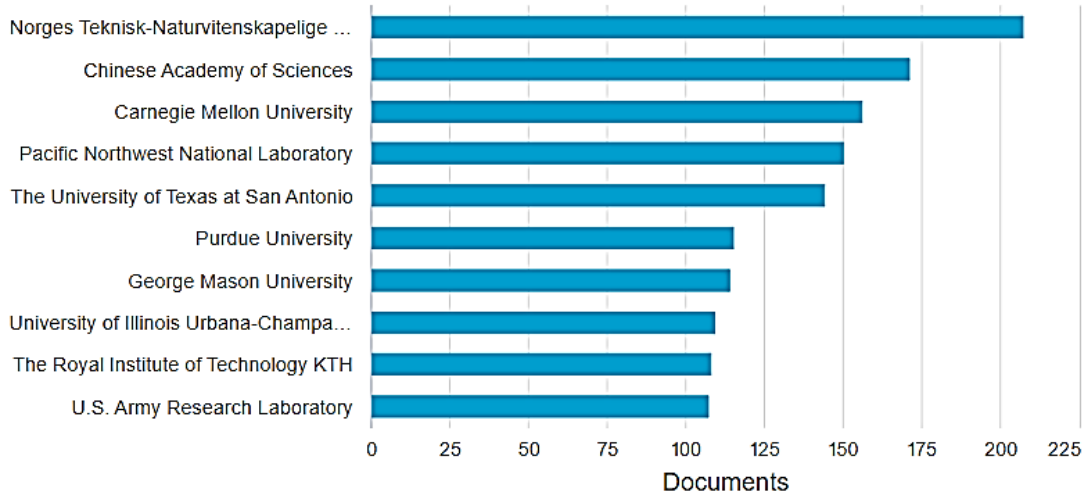
در بخش مقالات منتشر شده با موضوع امنیت سایبری، براساس نتایج پایگاه اسکپوس[۴] ، تعداد ۲۴۶۸۳ مقاله توسط پژوهشگران مختلف در مجلات و کنفرانس‌های مختلف از سال ۲۰۰۴ تا ۲۰۲۴ به چاپ رسیده است. در شکل ۳، نمودار فراوانی تعداد مقالات منتشر شده با موضوع امنیت سایبری به تفکیک سال نمایش داده شده است، که روند فراوانی تعداد مقالات به صورت افزایشی است و این روند از حدود سال ۲۰۱۸ از شتاب بیشتری برخوردار است. علت پایین بودن این آمار برای سال ۲۰۲۳ به این دلیل می‌تواند باشد که اطلاعات مربوط به این سال هنوز کامل نشده است و در انتهای سال، فراوانی مربوط به این سال تکمیل خواهد شد.



شکل ۳: نمودار فراوانی مقالات منتشر شده با موضوع امنیت سایبری به تفکیک سال از ۲۰۰۴ تا ۲۰۲۴

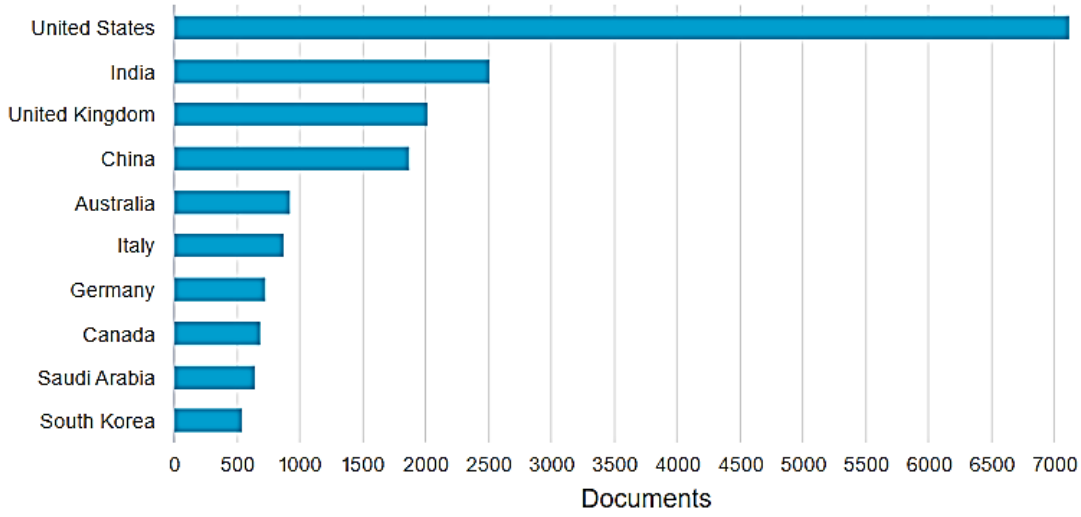
مهم‌ترین مراکز علمی، تحقیقاتی و دانشگاهی پیشتاز که در این حوزه مشغول به فعالیت هستند، در شکل ۴ نشان داده شده است. در رتبه‌های بالا، دانشگاه‌هایی از کشورهای نروژ، چین، آمریکا و سوئد قرار گرفته‌اند.

[۴] نتایج مستخرج از پایگاه دانش https://www.scopus.com در ماه سپتامبر سال ۲۰۲۳



شکل ۴: مهمترین مراکز علمی، تحقیقاتی و دانشگاهی پیشتاز در حوزه امنیت سایبری

آمار مربوط به ۱۰ کشور برتر که در این حوزه فعالیت‌های فراوانی را در حوزه تحقیقاتی دارند، در شکل ۵ گزارش شده است.

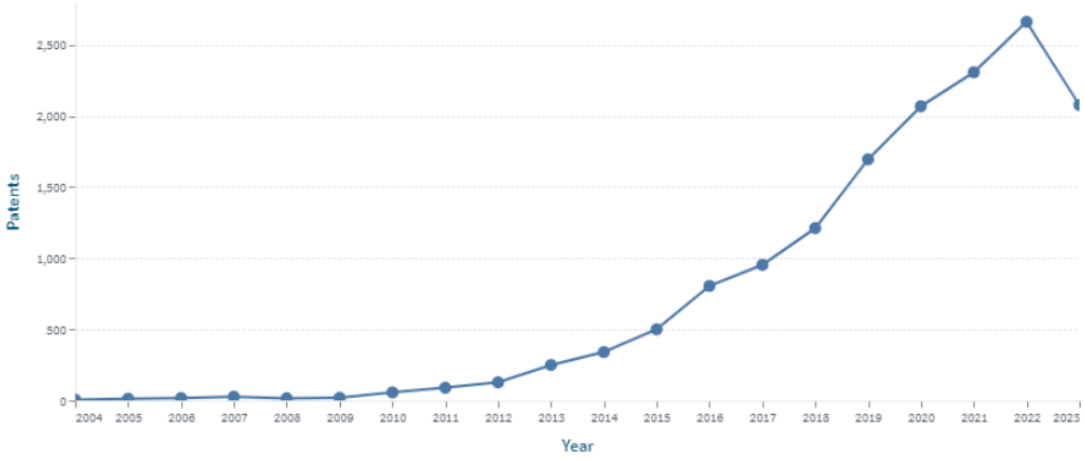


شکل ۵: کشورهای برتر در حوزه تحقیقات پیرامون موضوع امنیت سایبری

۲.۳ پایش فناوری

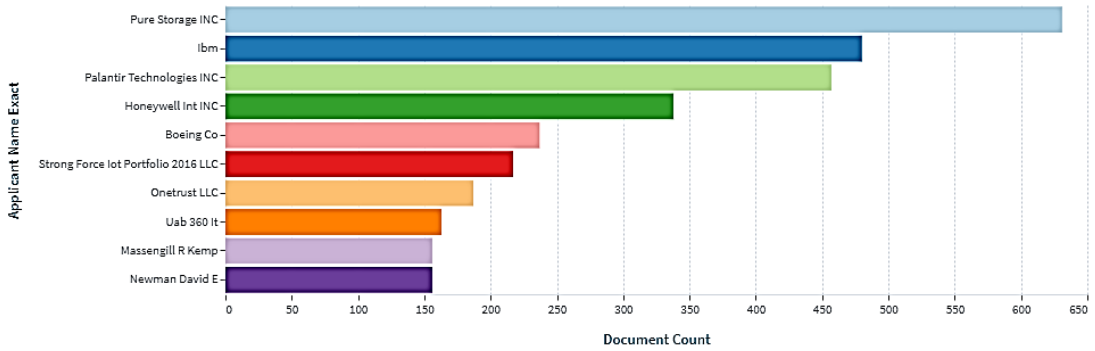
برای پایش فناوری به موارد مربوط به ثبت اختراع توجه می‌شود. بنابراین، در بخش اختراعات ثبت شده با موضوع امنیت سایبری، براساس نتایج پایگاه ثبت اختراعات، تعداد ۱۵۲۳۱ ثبت اختراع توسط مخترعین مختلف در دفاتر ثبت اختراع در کل جهان از سال ۲۰۰۴ تا ۲۰۲۳ به ثبت رسیده است. در شکل ۶، نمودار

فراوانی تعداد اختراعات به ثبت رسیده با موضوع امنیت سایبری به تفکیک سال نمایش داده شده است که روند فراوانی تعداد اختراعات ثبت شده به صورت افزایشی است و این روند از حدود سال ۲۰۱۸ از شتاب بیشتری برخوردار است. علت پایین بودن این آمار برای سال ۲۰۲۳ به این دلیل مربوط می‌شود که اطلاعات مربوط به این سال هنوز کامل نشده است و در انتهای سال، فراوانی مربوط به این سال تکمیل خواهد شد.



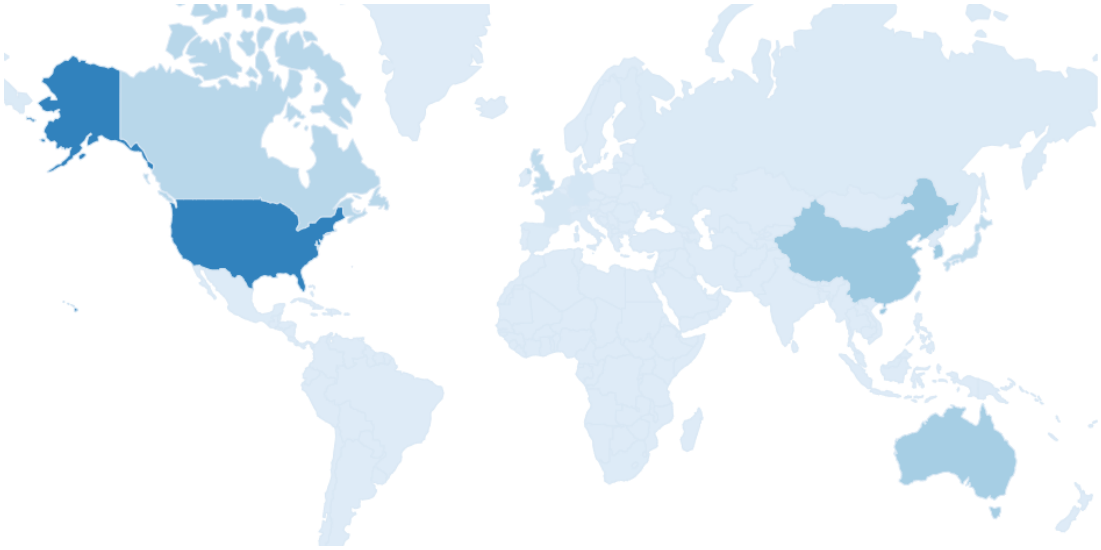
شکل ۶: فراوانی تعداد اختراعات ثبت شده پیرامون موضوع امنیت سایبری به تفکیک سال از ۲۰۰۴ تا ۲۰۲۳

مهمترین سازمان‌ها، موسسات، مراکز علمی و تحقیقاتی پیشتاز در حوزه تجاری سازی موضوع امنیت سایبری که مشغول به فعالیت هستند، در شکل ۷ نشان داده شده است که به طور عمده مربوط به موسسات و سازمان‌هایی از آمریکا هستند.



شکل ۷: مهمترین سازمان‌ها، موسسات، مراکز علمی و تحقیقاتی پیشتاز در حوزه تجاری سازی موضوع امنیت سایبری

از دیدگاه تجاری سازی موضوع امنیت سایبری، نقشه جهانی کشورهای برتر از نظر ثبت اختراع، پیرامون موضوع امنیت سایبری، در شکل ۸ نمایش داده شده است.



شکل ۸: نقشه جهانی کشورهای برتر در حوزه تجاری‌سازی از نظر ثبت اختراع پیرامون موضوع امنیت سایبری

۴ نتیجه گیری

با توجه به افزایش وابستگی و گسترش کاربردهای الکترونیکی در زندگی بشری، خیلی از نیازهای روزانه انسان‌ها توسط سیستم‌های الکترونیکی با استفاده از موبایل به صورت از راه دور و بدون نیاز به حضور فیزیکی انجام می‌پذیرد. این امر از یک طرف سهولت و مزایای فراوانی را برای بشر فراهم آورده است اما از طرف دیگر منجر به افزایش احتمال خسارات ناشی از تهدیدات، حمله و نفوذ در فضای سایبری شده است. در این مقاله، علاوه بر بیان اهمیت موضوع امنیت سایبری، پایش کتابشناختی علم با بررسی مقالات منتشر شده و پایش فناوری با بررسی ثبت اختراعات مورد بررسی قرار گرفت.

مراجع

[1] L. Yuchong, and Q. Liu. “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments”, Energy Reports, vol. 7, pp. 8176-8186, 2021.

[2] Z. Zhang, H. Ning, F. Shi, F. Farha, X. Y. Xu. J. Xu. F. Zhang, K, R. Choo, “Artificial intelligence in cyber security: research advances, challenges, and opportunities”, Artificial Intelligence Review, vol. 55, pp. 1029-1053, 2022.

[3] M. E. Whitman, H. J. Mattord. Principles of information security. Cengage learning, 2021.

[4] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, “Security and Privacy in Cyber-Physical Systems: A Survey of Surveys”, IEEE Design , Test of Computers, vol. 34, no. 4, pp. 7–17, 2017.

[5] Zuech, T. M. Khoshgoftaar, and R. Wald, “Intrusion detection and Big Heterogeneous Data: a Survey”, J. Big Data, vol. 2, no. 1, p. 3, 2015.

[6] Y. Harel, I. Ben Gal, and Y. Elovici, “Cyber Security and the Role of Intelligent Systems in Addressing its Challenges”, ACM Trans. Intell. Syst. Technol., vol. 8, no. 4, pp. 1–12, 2017.

[7] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, W. M. Lim, “How to conduct a bibliometric analysis: An overview and guidelines”. Journal of business research, vol. 133, pp. 285-296, 2021.