BİTLİS EREN ÜNİVERSİTESİ
FEN BİLİMLERİ DERGİSİ

ISSN: 2147-3129 / e-ISSN: 2147-3188

Article Type	: Research Article	**Year**	: 2025
Received	: September 9, 2025	**Volume**	: 14
Revised	: November 18, 2025	**Issue**	: 4
Accepted	: November 27, 2025	**Pages**	: 2712-2734
DOI	: 10.17798/bitlisfen.1780997		

THE PLACE OF GENERATIVE ARTIFICIAL INTELLIGENCE IN DIGITAL SECURITY STUDIES

Sevinç AY [1], **Songül KARAKUŞ** [2,*]

[1] *Fırat University, Distance Education Center, Elazığ, Türkiye*

[2] *Bitlis Eren University, Computer Engineering Department, Bitlis, Türkiye*

**** Corresponding Author:*** *skarakus@beu.edu.tr*

ABSTRACT

Digital security has become critically important today as cyber threats continue to diversify. This study aims to systematically examine the place of generative artificial intelligence in the digital security literature. In this context, documents obtained from a search using the keywords generative artificial intelligence and cybersecurity or information security have been compiled from the Web of Science (WoS) and Scopus databases as of September 3, 2025. As a result of the compilation, 37 duplicate documents were removed, and the remaining 350 papers were analyzed using RStudio, VOSviewer, and Gephi. The research covers themes such as the distribution of academic studies by year, author productivity, collaboration networks, country, institution, resource allocation, keywords, and topics covered. The findings reveal that research in the field increased particularly between 2024 and 2025. According to Lotka's law, author productivity indicates that most authors contribute with a single publication, while a small number of productive authors have played a central role in the development of the field. The keyword analysis demonstrates that generative AI research is developing in two directions, both in the context of health/data privacy and cybersecurity/threat analysis. Finally, a country-by-country analysis reveals that the USA and India are the leading countries contributing most to the field, while the rate of international collaboration is low. In conclusion, this study demonstrates that generative AI is an important interdisciplinary research theme in digital security and is expected to guide future studies.

Keywords: Generative artificial intelligence, Information security, Cyber security, Digital security, Bibliometric analysis.

1 INTRODUCTION

With the acceleration of digitalization today, security threats have also diversified, and digital security has become one of the most critical areas of our time. Risks such as fake content, data manipulation, cyber attacks, and phishing attempts threaten the security of everyone, from individuals to states. Moreover, with the exponential increase in data flow, the rapid detection of security vulnerabilities and the development of effective countermeasures have become critically important. At this point, generative artificial intelligence technologies attract attention not only with their ability to produce content but also with their ability to prepare attack scenarios, perform threat simulations, and dynamically develop security protocols. While the same technologies make our lives easier, on the other hand, the misuse of these same technologies has also led to new security risks in the field of digital security.

Generative artificial intelligence (GAI) is a large language model that learns the relationships between pre-trained models and content such as text, audio, images, code, etc., and uses what it has learned to generate various content based on the questions asked [1]. GAI applications have been actively used in daily life since 2022, thanks to advances in artificial intelligence technologies. In addition to GAIs that can produce new things by processing multiple data sources, such as ChatGPT, Gemini, and Copilot, there are also GAI tools developed for specific areas [2].

This study aims to evaluate the studies on GAI and digital security, that is, information security or cyber security, using the bibliometric analysis method, and to reveal the current status and potential effects of GAI in the field of digital security. In this context, bibliometric analysis of studies on GAI and digital security is of great importance. Such analyses quantitatively reveal the trends and collaboration networks of scientific publications in the literature and provide a strategic roadmap for researchers and institutions. Some of the studies conducted on this subject are given below.

Herrador and Rehberger [3] conducted a study on SpAIware, which poses a security threat by exploiting persistent memory vulnerabilities in large language model (LLM) applications. In this context, the authors investigated how malicious individuals can use GAI to inject malicious instructions into multiple chat sessions and enable data leaks. In their study, Aldasoro et al. [4] conducted a survey on cyber security experts working in major central banks. The results from the survey findings indicate that GAI will increase the speed of cyber threat detection and response, and that investment in expert human resources is necessary to counter

data leak risks. Hatipoğlu et al. [5] developed a web platform to raise users' awareness about threats and detections in Internet of Things (IoT) networks and provided training and testing opportunities on IoT security on synthetic network datasets. As a result, thanks to this developed platform, users have been able to improve their ability to understand and detect cyber threats in different scenarios. Ankalaki et al. [6] have comprehensively examined artificial intelligence methods such as machine learning, deep learning, natural language processing, explainable artificial intelligence, and GAI to reduce various cyber risks and increase cyber security. In their study, Sönmez Sarıkaya and Bahtiyar [7] proposed a GAI-based framework to overcome the problem of insufficient data for intrusion detection systems in Uncrewed Aerial Vehicles (UAVs). The study also emphasized the importance of synthetic data in developing more robust and adaptable intrusion detection systems. In a study conducted by Coppolino et al. [8], the impact of GAI on cybersecurity was examined, and a new strategy called attack concealment with conditional generative adversarial networks (GANs) was proposed. With this strategy, an attempt was made to deceive artificial intelligence-based intrusion detection systems by injecting synthetic traffic. As a result, it has been observed that the proposed approach is successful in different datasets and attacks. Ferrag et al. [9] conducted a comprehensive study examining the role of GAI and Large Language Models (LLM) in cybersecurity. This study addresses vulnerabilities, defense strategies, and performance evaluations of LLMs, along with applications such as hardware security, intrusion detection, malware, and phishing prevention. In addition, new techniques and future research directions are being discussed to ensure the safer and more effective use of LLMs. In the study by Badawy [10], a security framework based on generative artificial intelligence, GANs, and federated learning was proposed to protect 6G-based IoT networks against cyber threats. The proposed approach effectively prevents phishing, malware, and DoS attacks by leveraging the high speed, low latency, and network slicing features of 6G. Shree et al. [11] evaluated GAI and Bidirectional Encoder Representations from Transformers (BERT) based approaches against increasing cyber threats for the complex security needs of 6G networks. According to the experimental results, it has been seen that the BERT model offers an effective solution for real-time threat detection in resource-constrained IoT environments, where it stands out with an accuracy rate of 91.2%. Finally, in another study, Priya and Kapilamithran [12] conducted research to enhance the security of encryption protocols by revealing the weaknesses of the Advanced Encryption Standard (AES) algorithm. In this context, they examined AES vulnerabilities using the Padding Oracle Attack (POA) and artificial intelligence methods. Their proposed approach was based on breaking the AES key by extracting the plaintext length from the ciphertext and predicting web page passwords.

This study addresses the following problem. Despite the growing number of studies on generative artificial intelligence, there is still no systematic and comprehensive overview of how GenAI is positioned within the digital and cybersecurity literature. Existing research remains fragmented, focusing either on technological developments (e.g., large language models, deep learning, synthetic data) or on cybersecurity risks (e.g., cyber-attacks, adversarial machine learning, phishing, malware). However, the field lacks an integrated bibliometric assessment that maps the intellectual structure, key contributors, thematic clusters, and emerging trends of GenAI-related security research. Therefore, the core research problem of this study is to systematically identify how generative AI is conceptualized, clustered, and connected within the broader cyber/digital security domain.

The remainder of the study is organized as follows. The second section discusses the databases and research method used in the study, the third section discusses the findings, and the final section provides a general evaluation and offers various recommendations.

2 MATERIALS AND METHODS

Within the scope of the study, bibliometric analysis was applied to publications in Web of Science (WoS) and Scopus databases. The search was conducted on September 3, 2025, and all fields where the terms "information security" or "cyber security" appeared together with the terms "generative AI", "generative artificial intelligence", "GAI", or "GenAI" were taken into account. The search strategies used in the study are presented in Table 1.

Table 1. Primary search strategy – main dataset

Database	Query
WoS	TS=(("information security" OR "cyber security") AND ("generative AI" OR "generative artificial intelligence" OR "GAI" OR "GenAI"))
Scopus	TITLE-ABS-KEY(("information security" OR "cyber security") AND ("generative AI" OR "generative artificial intelligence" OR "GAI" OR "GenAI"))

VOSviewer (version 1.6.20), R Studio (version 2024.12.1), Bibliometrix package program, and Gephi (version 0.10.1) were used for bibliometric analysis. Using the biblioshiny package for the RStudio program, the distribution of publications by year, author analysis according to Lotka's law, source analysis according to Bradford's law, and analysis of the most relevant countries and affiliations were performed. VOSviewer 1.6.20 was used for co-occurrence author analysis and keyword network analysis. In the data cleaning step, a thesaurus was created and a duplicate merging process was applied to remove alternative spellings or synonyms. Then, bibliometric analysis methods were applied to the data.

The obtained network data were exported in Pajek format by VOSviewer and then imported into Gephi 0.10.1 software to calculate the centrality measurements of the nodes. Here, the relative importance of nodes within the network was revealed by calculating the eigenvalue centrality.

2.1 Data Cleaning and Analysis

As a result of the search, 40 publications were found in the WoS database, and 347 publications were found in the Scopus database. The obtained data were exported in BibTeX format and combined using codes prepared in Biblioshiny software. During the data integration process, 37 duplicate documents were removed.

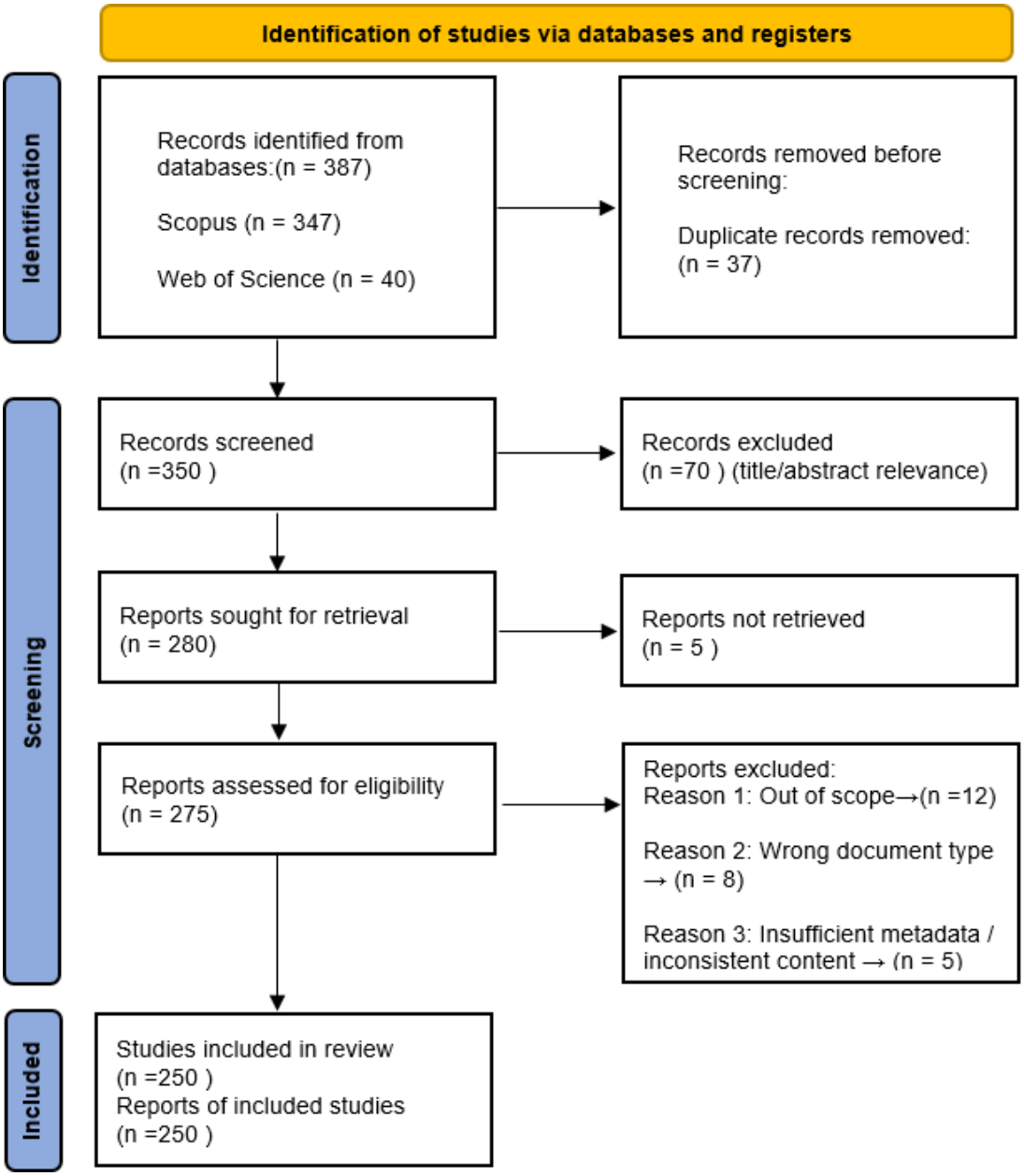

Figure 1. PRISMA 2020 Flow Diagram

The PRISMA 2020 flowchart was used to transparently present the dataset identification, screening, eligibility, and inclusion stages. The diagram summarizes how many records were retrieved, removed, assessed, and included in the final bibliometric analysis. Figure 1 presents the PRISMA 2020 flowchart.

During the analysis process, basic bibliometric indicators, including publication trends by year, citation counts, and author productivity, as well as co-authorship, co-occurrence of authors, and keyword co-occurrence networks, were examined. Using these methods, the research landscape of the field was systematically evaluated; prominent authors, journals, and institutions at the intersection of cybersecurity and information security with GAI were identified, and thematic clusters and emerging trends were revealed. Basic information about the data obtained from the WoS database is presented in Table 2.

Table 2. Main information about the data

Description	Results
Timespan	2020:2026
Sources (Journals, Books, etc.)	139
Documents	350
Annual growth rate %	20.09
Document average age	0.631
Average citations per doc	5.331
References	1980
Document Contents	
Keywords plus (ID)	2272
Author's keywords (DE)	2685
Authors	
Authors	1080
Authors of single-authored docs	40
Authors Collaboration	
Single-authored docs	56
Co-authors per doc	3.51
International co-authorships %	2.857

The dataset examined in this study consists of a total of 350 documents covering the years 2020–2026, where 2026 entries represent online-first publications. There are 139 different sources where studies are published, and it is seen that research in the field is increasing rapidly, with an annual growth rate of 20.09%. Since the average age of the documents is 0.631 years, it is understood that the subject is a very current research area. Although the average number of citations per document is limited to 5,331, considering the newness of the field, this value has a high potential to increase in the coming years. When author contributions were examined, it was determined that a total of 1080 researchers contributed to the studies, 40 of them produced

single-authored works, and overall, there were an average of 3.51 authors per document. The international collaboration rate was very low at only 2.857%, indicating that research was mostly conducted at the national level.

Document types article (n=91), article; early access (n=2), book (n=9), book chapter (n=44), conference paper (n=146), conference review (n=14), editorial (n=7), editorial material; They are listed as early access (n=1), letter (n=3), note (n=1), proceedings paper (n=13), review (n=18), short survey (n=1). When evaluated in terms of document types, it is seen that conference proceedings and articles are predominant, while book chapters and a limited number of compilations contribute to the field. Overall, the findings reveal that studies at the intersection of information security, cybersecurity, and generative artificial intelligence are a rapidly developing field, but not yet sufficiently integrated at the international level.

3 RESULTS AND DISCUSSION

3.1 Annual Scientific Production

Within the scope of the study, firstly, the distribution of publications by year was examined. According to the distribution of publications, the highest number of studies was conducted in 2025 (160 publications) and 2024 (153 publications). Some Scopus/WoS records show that articles were published online in 2024-2025, but the publication year is 2026.

In accordance with bibliometric rules, datasets retain the year assigned to the database, with 2026 being identified as the online-first items (n=3) within the annual production range. The analysis obtained from the R Studio program, showing the distribution of articles by year, is presented in Figure 2.

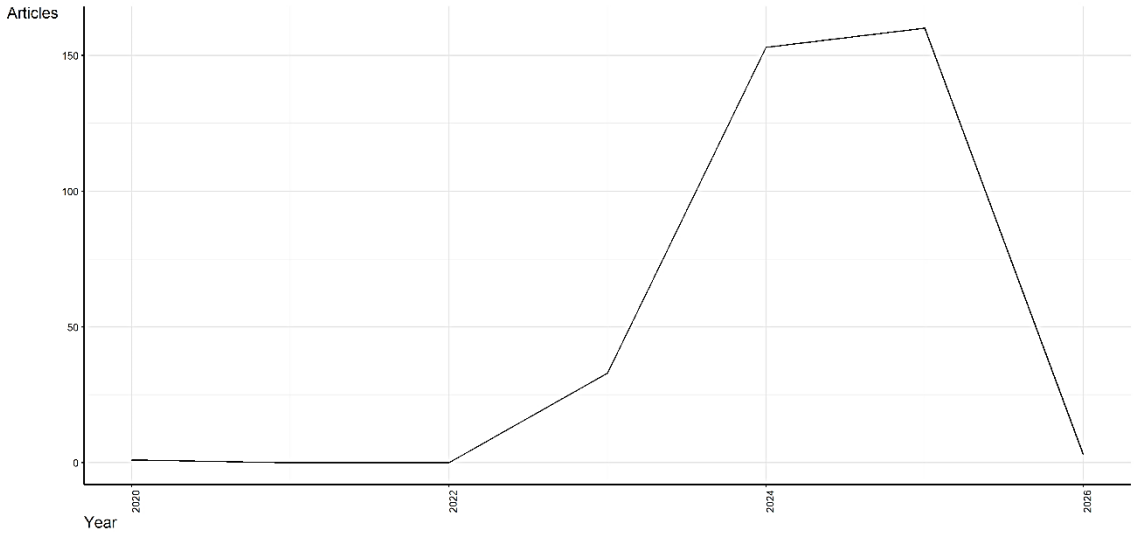

Figure 2. Distribution of Articles by Year

As seen in Figure 2, a remarkable change is observed in scientific production over the years. The first studies in the field started in 2020, and production remained very limited in the first years. Since 2023, working speeds have shown a significant upward trend. There was a rapid increase, especially in 2023, and the studies reached the highest level in 2025. This situation reveals that the field has gained great momentum in recent years, but periodic fluctuations can also be observed in the number of publications.

3.2 Author Analysis

When the data was examined, it was seen that the studies of 1080 authors were obtained. Among the authors who have contributed the most to the field, NA N (n=14), JHANJHI N (n=10), KHAN A (n=5), SINGH S (n=5), and ALI G (n=4) stand out. The productivity of authors over time is presented in Figure 3.

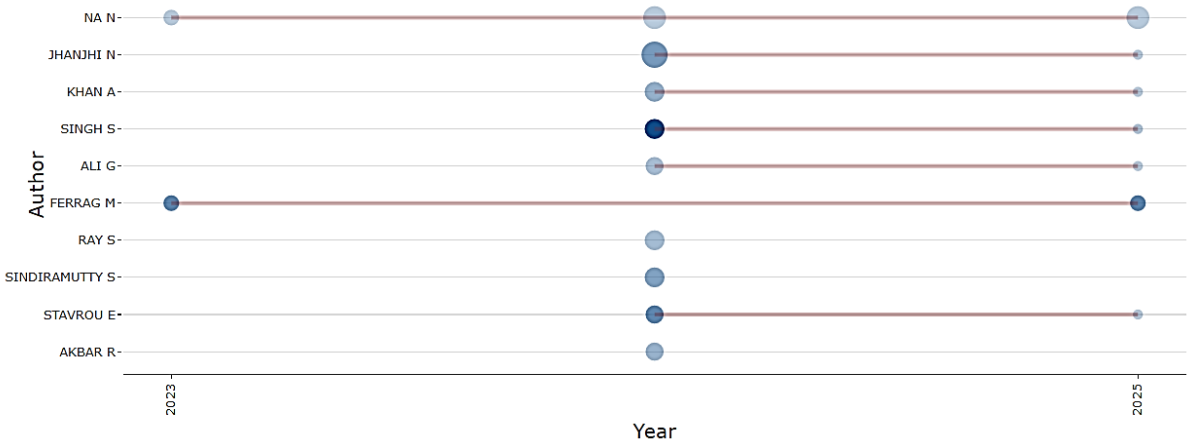

Figure 3. Authors' Production Over Time

Figure 3 shows the productivity trend of authors over the years. According to the findings, while a limited number of authors contributed in the early periods, it is noteworthy that productivity increased significantly, especially in the post-2020 period. This increase reveals both the increasing interest in the field and the diversification of collaborations among researchers. In addition, an increase in the production of individual authors has been observed in certain years, and this is thought to be related to pioneering studies that have provided short-term momentum in the field. Overall, the chart shows that writer productivity follows a fluctuating but upward trend.

Author Productivity According to Lotka's Law

Lotka's law is a fundamental bibliometric principle that describes the distribution of productivity among authors publishing in a field. This law reveals that while a small number of authors produce a large number of publications, the vast majority contribute only a single study. While authors who have contributed to the field are analyzed with Lotka's law, authors who are likely to contribute in the future can also be identified. The productivity of authors according to Lotka's law is shown in Table 3.

Table 3. Author productivity through Lotka's law

Documents written	N of authors	Proportion of authors
1	981	0.908
2	75	0.069
3	15	0.014
4	5	0.005
5	2	0.002
10	1	0.001
14	1	0.001

As shown in Table 3, author productivity was examined within the framework of Lotka's law in the data between 2020 and 2026. The findings show that the vast majority of researchers contributing to the field are represented by a single publication. In fact, 90.8% (n=981) of the authors produced only one publication, 6.9% (n=75) produced two publications, 1.4% (n=15) produced three publications, 0.5% (n=5) produced four publications, and 0.2% (n=2) produced five publications. The number of authors who have published ten publications is limited to only one (0.1%).

This distribution supports the classical pattern predicted by Lotka's law. It appears that contributions to the field are largely made through individual publications, but a small number of highly productive authors play a central role in the development of the literature. This finding also shows that the period covered by the study points to a newly developing field of research. Lotka's law states that as the number of publications produced by an author increases, the number of such authors decreases exponentially. The basic mathematical form of the law is as Eq. 1.

$$f(r) = \frac{C}{r^{\alpha}}, \ln f(r) = \ln C - \alpha \ln r \quad (1)$$

Here, r is represented as the number of publications produced by an author, f(r): The proportion of authors who produced this number of publications, C: The norming coefficient, and α: The Lotka exponent. Based on this equation, the writer productivity data were subjected to log–log regression, and the slope coefficient directly yielded the Lotka exponent (α). Since the regression slope obtained in the study was approximately, it is assumed that $\alpha \approx 2.7$. This value shows that very few authors in the field produce multiple publications, while the vast majority are represented by a single publication.

A co-authorship network map was created by specifying the criteria of at least one publication and at least one citation. Network maps for the nine authors who met the threshold were presented. Figure 4 presents the co-occurrence authors analysis showing the co-authorship network.

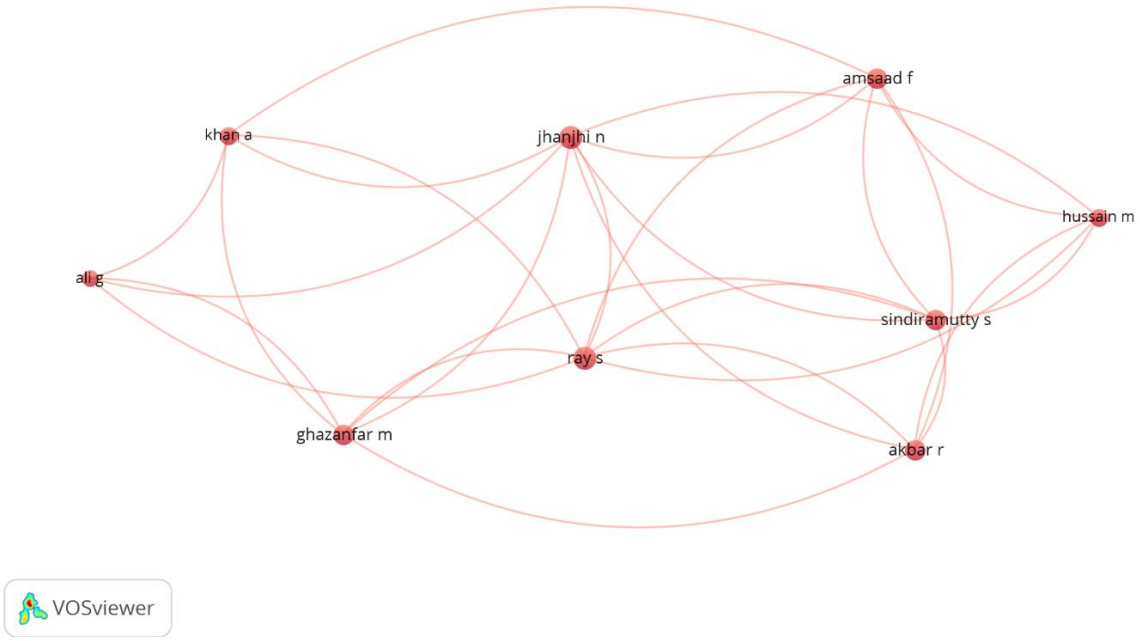

Figure 4. Co-occurrence Authors Analysis

Linear Logarithmic Layout was selected as the normalization method within the scope of the analysis. This method makes clusters more distinct and clear in large and complex networks. Because attraction and repulsion forces are arranged linearly and logarithmically, tightly connected nodes (e.g., frequent collaborators) move closer together, while less connected nodes move farther apart. As seen in Figure 4, authors such as Jhanjih N, Ray S, and Ghazanfar M are in a central position and have collaborated with more than one author. Authors on the fringes, such as Khan A and Hussain M, have a more limited number of connections. This network indicates that there are small but interconnected clusters of authors on the studies, but not a very high level of international collaboration.

3.3 Most Relevant Countries and Affiliations

Within the scope of bibliometric analysis, the countries and affiliations that contributed the most to the field were examined. Table 4 presents the most relevant countries and affiliations along with their article numbers.

Table 4. Most prolific contributors

Most Relevant Countries			Most Relevant Affiliations		
No	Country	Articles	No	Institution	Articles
1	USA	103	1	University of Petra	19
2	India	66	2	Taylor's University Malaysia	12
3	UK	24	3	University of California	9
4	China	23	4	College of Engineering	8
5	Australia	18	5	Uniformed Services University (Hlth Sci)	6
6	Italy	18	5	Birla Institute of Technology and Science	5
7	Finland	11	7	Birla Inst Technoland Sci	5
8	Jordan	11	7	The University of Jordan	5
9	Malaysia	10	9	Universiti Islam Sultan Sharif Ali	5
10	Saudi Arabia	9	10	Open University of Cyprus	4

According to the findings presented in Table 4, the country that has contributed the most to the field is the United States (103 publications), followed by India (66 publications) and the United Kingdom (24 publications). China, Australia, and Italy are also among the countries that have made significant contributions. At the institutional level, the University of Petra (19 publications) stands out, while Taylor's University Malaysia (12 publications) and the University of California (9 publications) are among the other strong players. Institutions such as the College of Engineering (8 publications) and the Uniformed Services University (6 publications) also appear to have made significant contributions. Data show that countries such as the USA and India, in particular, exhibit strong productivity in terms of both the number of publications and the contribution of different institutions.

3.4 Sources Analysis

Among the sources where the publications were published most, the first 5 places were taken by IEEE Access (n=16), Lecture Notes in Computer Science (n=11), Lecture Notes in Networks and Systems (n=11), CEUR Workshop Proceedings (n=9), and Communications in Computer and Information Science (n=5). Figure 5 shows the most relevant sources.

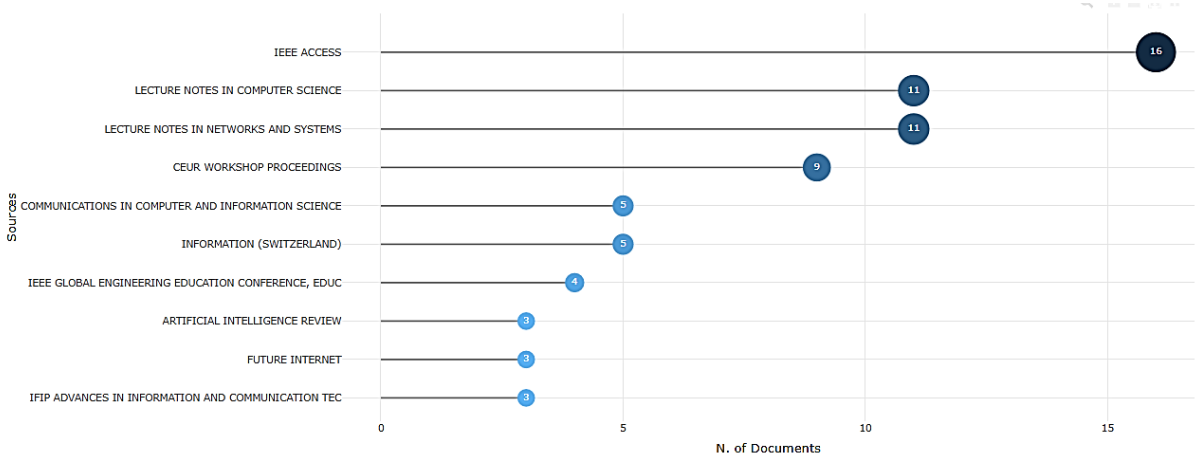

Figure 5. Most Relevant Sources

Most Productive Resources According to Bradford's Law

The studies conducted in the field of information security, cyber security, and generative artificial intelligence between 2020 and 2026 were examined according to the Bradford law, and the most productive resources are presented in Table 5. Bradford's law is a fundamental bibliometric principle that describes how articles published in a given field are distributed across different journals. This law, defined by Bradford, states that a core group of journals will emerge by arranging the journals in which articles are published in order of decreasing productivity [13]. This core group of journals contains a significant portion of the articles in the relevant field, while the remaining publications are distributed across other regions containing a similar number of articles [14, 15, 16]. In this study, by applying Bradford's law, the most productive journals at the intersection of information security or cybersecurity and generative artificial intelligence were determined, and it was observed that the distribution of publications in the literature was concentrated around the core journals.

Table 5. Core sources by Bradford's law

Rank	Source Title	Frequency	Cumulative	Zone
1	IEEE Access	16	16	Zone 1
2	Lecture Notes in Computer Science (LNCS)	11	27	Zone 1
3	Lecture Notes in Networks and Systems (LNNS)	11	38	Zone 1
4	CEUR Workshop Proceedings	9	47	Zone 1
5	Communications in Computer and Information Science (CCIS)	5	52	Zone 1
6	Information (Switzerland)	5	57	Zone 1
7	IEEE EDUCON	4	61	Zone 1
8	Artificial Intelligence Review	3	64	Zone 1

Table 5 (continued). Core sources by Bradford's law

Rank	Source Title	Frequency	Cumulative	Zone
9	Future Internet	3	67	Zone 1
10	IFIP Advances in Information and Communication Technology	3	70	Zone 1
1–17	Total Zone 1 (17 journals)	117	117	Zone 1
18–46	Total Zone 2 (29 journals)	117	234	Zone 2
47–113	Total Zone 3 (67 journals)	116	350	Zone 3

According to Bradford's law, the resources in the top 10 and Zone 1 are presented in Table 5. Zone 1, under this law, refers to the small number of core journals that publish the most articles in the field; Zone 2 refers to mid-level publications spread across a larger number of journals; and Zone 3 refers to peripheral journals spread across a larger number of journals but with a small number of publications in each. According to Bradford's law, this distribution indicates that the literature is largely concentrated in a certain core group of journals. Here, IEEE Access and the Lecture Notes series stand out as central sources where research on information security, cybersecurity, and generative artificial intelligence is published. This situation reveals that publications in the field covered by the study are directed mostly to engineering and computer science-focused journals; thus, there is an interdisciplinary trend. Bradford Zones and k-multiplier are presented in Table 6.

Table 6. Bradford zones and k-multiplier

Zone	Journals	Articles	Percentage
Zone 1 (Core)	17	117	33.4%
Zone 2	29	117	33.4%
Zone 3	67	116	33.1%
Total	113	350	100%

When evaluated according to the table, Bradford Multiplier (k) is calculated as Eq. 2.

$$k = \frac{29}{17} \approx 1.70 \tag{2}$$

Bradford analysis identified a core set of 17 journals (Zone 1) producing the first 117 articles, followed by 29 journals in Zone 2 and 67 journals in Zone 3. A k-value between 1.5 and 2.5 is typical for emerging interdisciplinary fields. The Bradford multiplier was k = 1.70, indicating moderate source dispersion and a well-defined core literature.

The most frequently examined network structure within the scope of source analysis is the three-field plot. This network examines the distribution among sources, authors, and keywords. A three-field plot is presented in Figure 6.

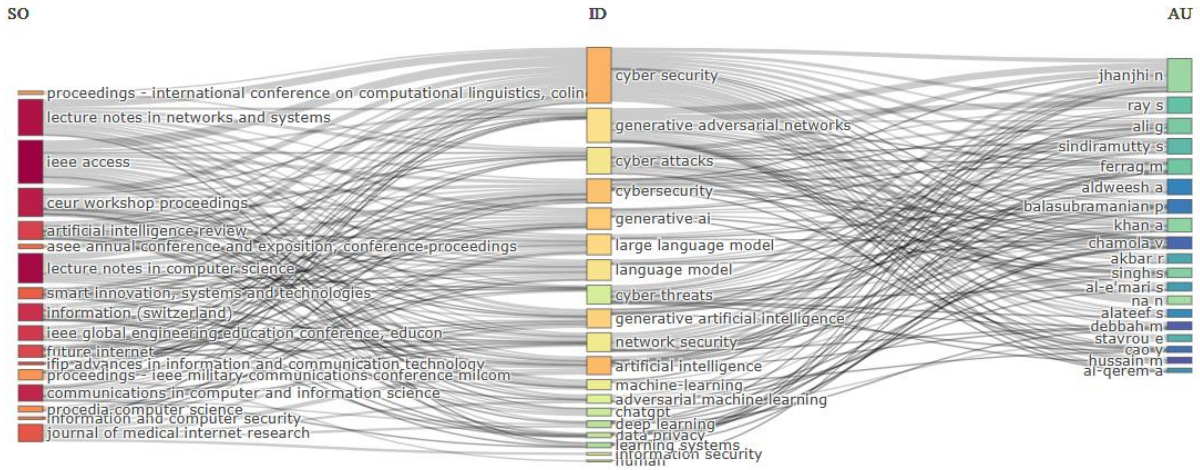

Figure 6. Three-Field Plot

A three-field plot was prepared by selecting sources on the left, keyword plus in the middle, and authors on the right. The number of items is selected as 20. In general, the graph shows that the studies published in certain journals are concentrated with keywords focused on cybersecurity and generative artificial intelligence, and a few authors stand out in this field, creating a significant center in the literature.

3.5 Keyword Analysis and Thematic Map

The most frequently used keyword analysis in studies on the use of generative AI in information security and cybersecurity was visualized using the VOSviewer program. A minimum occurrence threshold of five was applied, and only keywords appearing at least five times in the dataset were included in the co-occurrence network. Additionally, full counting was used, and association strength was determined by normalization. Figure 7 shows the co-occurrence analysis of author keywords prepared for this purpose.

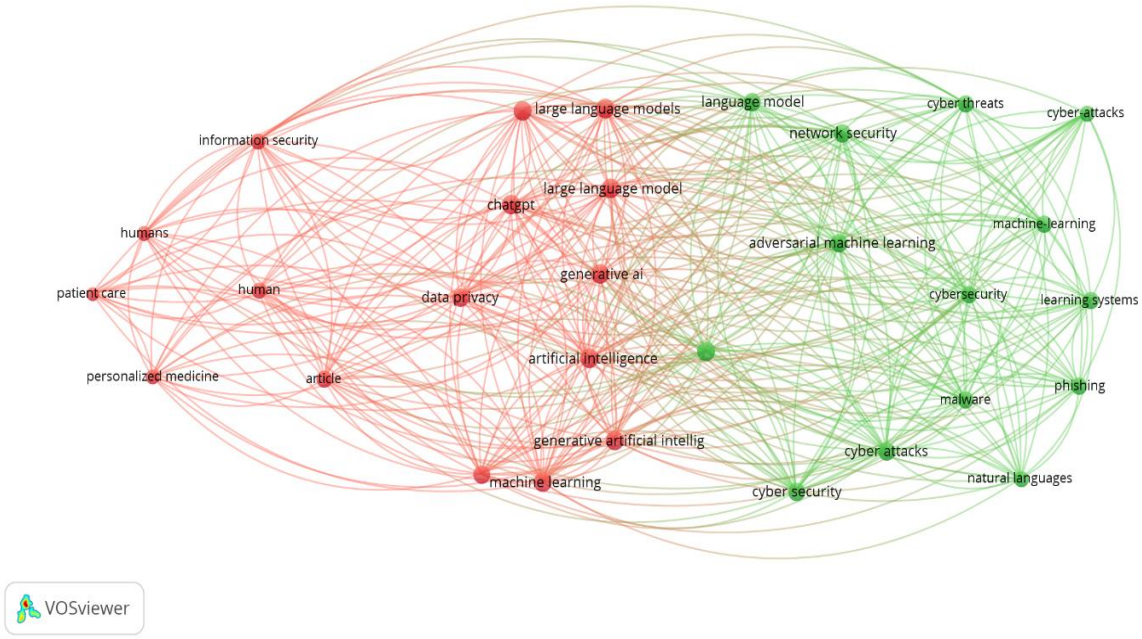

Figure 7. Co-occurrence Author Keywords Analysis

Figure 7 presents the network analysis based on the co-occurrence of author keywords. Keywords consist of two main clusters. The red cluster focuses more on topics such as artificial intelligence, machine learning, generative AI, data privacy, health, human, and personalized medicine. This cluster highlights the use cases of generative AI in the context of healthcare, personalized medicine, and data privacy. The green cluster is shaped around keywords such as cyber security, cyber attacks, network security, adversarial machine learning, phishing, learning systems, and natural languages. This cluster reflects the aspect of generative AI related to cybersecurity threats, attacks, and defense systems. Concepts such as "artificial intelligence", "generative artificial intelligence," and "machine learning" serve as a bridge between both clusters and are seen in the literature to create an interdisciplinary connection. This situation demonstrates that generative AI research is developing in two directions, both in the context of health/data privacy and cybersecurity/threat analysis.

Another analysis examined within the scope of the study is a thematic map. A thematic map is a visualization technique used in bibliometric analysis. It classifies keyword clusters into four areas according to the relevance degree and development degree criteria [17, 18]. These are engine themes, niche themes, basic themes, and declining or emerging themes. Motor themes are themes that have both high centrality and high density. It expresses the strong themes that drive development and guide research in the field. Niche themes are themes with high density but low centrality. It represents more specific and narrow topics that are studied extensively in a particular field but have little contribution to the general field. Basic themes are themes with high centrality and low density values. They constitute the fundamental

building blocks of the field, but their research depth is limited. Declining or emerging themes (lower left quadrant) have low values in terms of both centrality and density. The themes in this group can be either declining or emerging. The prepared thematic map is presented in Figure 8.

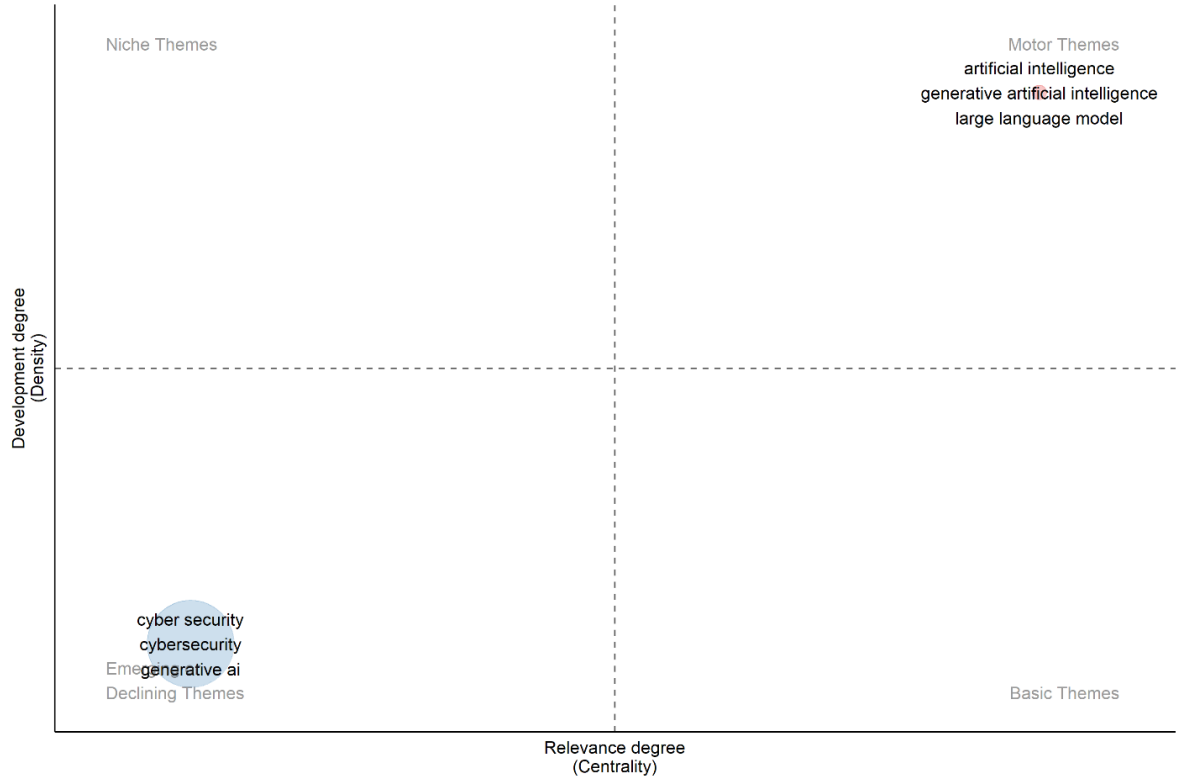

Figure 8. Thematic Map

According to Figure 8, according to the data obtained in the field, the motor themes are artificial intelligence, generative artificial intelligence, and large language models. These concepts are the driving force of the field and show high centrality and development. In other words, it constitutes the main axis of the research. Declining/emerging themes cyber security cybersecurity, generative AI. These themes are low centrality and low development. This situation indicates that these issues have either lost importance or are just beginning to develop. In the context of the study, the relationship between generative artificial intelligence and cybersecurity is still in the development stage. Niche themes and basic themes were left blank in this study. That is, the research focused mainly on motor themes and emergent/retracted themes.

Thematic evolution analysis was carried out for the years 2023 and 2025, which were considered as the breaking point in the distribution of studies by year. Thematic evolution analysis was conducted to examine how the intellectual structure of the field has changed across the three time slices (2020–2023, 2024–2025, and 2026). Thematic evolution is presented in Figure 9.

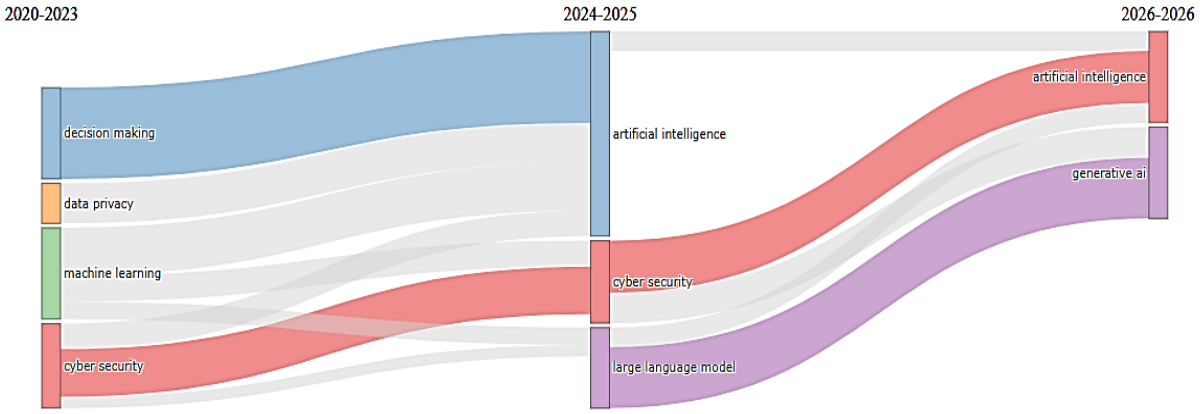

Figure 9. Thematic Evolution

The results show that early themes such as decision making, data privacy, machine learning, and cyber security in 2020–2023 converge into broader umbrella topics particularly artificial intelligence and cyber security during 2024–2025. In the final period (2026), the thematic structure becomes more specialized: streams originating from earlier AI-driven themes evolve into large language models and generative AI, while cyber-security maintains continuity as a stable core theme. The appearance of "large language model" and "generative AI" as end-point topics reflects the shift toward model-specific risks (e.g., prompt injection, deepfake misuse), indicating that the field is transitioning from general AI discussions to concerns focused on advanced generative architectures.

3.6 Cluster Analysis with Gephi

Cluster analysis is based on the principle of collecting data with similar characteristics into the same group. In a bibliometric context, it is also described as bringing together articles from the same domain. Cluster analysis, a content-based method, is considered an important variant of network analysis.

In this study, network analysis was conducted using Gephi 0.10.1 software to examine the relationships between author keywords. The Louvain algorithm was applied during the clustering process, and a modularity index ranging from -1 to +1 was calculated to measure density differences between clusters. This determined the structure and density of clusters within the network. ForceAtlas2 layout (scaling = 2.0, gravity = 1.0), Louvain resolution = 1.2 is set. The size of nodes in the graph reflects the importance and centrality of the author or keyword in the network. The modularity index was calculated using the Eq. 3.

$$Q = \frac{1}{2m} \sum_{ij} (A_{ij} \frac{k_i k_j}{2m}) \ \delta(c_i, c_j) \quad (3)$$

Here, A_{ij} represents the connection between nodes i and j; k_i represents the sum of the weights of the edges connected to node i; and m represents half the weights of all edges. The $\delta(c_i, c_j)$) function shows whether nodes i and j are in the same cluster.

This analysis reveals the relationships between clusters and also reveals the core thematic areas of each cluster. This systematically identifies the clusters around which the most prominent themes in the study's research focus. Figure 10 visualizes the resulting cluster structure.

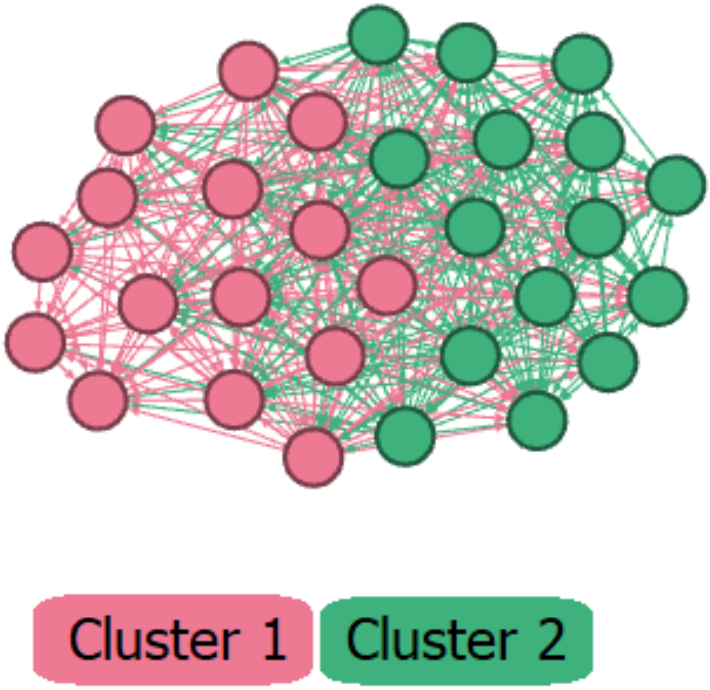

Figure 10. ForceAtlas2 Structure of Two Clusters

The network data obtained from the analysis performed with VOSviewer was exported in .NET format and imported into Gephi for more detailed analysis. Utilizing Gephi's advanced visualization and analysis features, a network structure consisting of 30 nodes and 366 edges was examined. In Gephi, nodes represent published articles, and edges represent the connections between these articles [19]. The modularity value was calculated as 0.071 as a result of the formulas applied to the network. ForceAtlas2 was chosen as the layout algorithm, and two clusters were identified as a result of the analysis.

The cluster analysis revealed two main themes. The first cluster represents artificial intelligence and learning technologies, focusing on keywords such as generative AI, artificial intelligence, machine learning, deep learning, and large language models. The second cluster, consisting of concepts such as cybersecurity, cyber-attacks, phishing, adversarial machine learning, malware, and network security, reflects cybersecurity-focused research. These findings demonstrate that generative AI studies in the literature constitute a dual-faceted research area, encompassing both technology development (AI and learning systems) and security applications.

The results of the network analysis demonstrate that concepts such as Generative AI, Artificial Intelligence, ChatGPT, Machine Learning, Deep Learning, and Information Security establish strong connections with various themes in the literature. Generative AI, in particular, has been linked to concepts such as personalized medicine, patient care, humans, and data privacy in the healthcare field, and to themes such as cyberattacks, cyber threats, and adversarial machine learning in the security field. Similarly, Artificial Intelligence and Machine Learning appear to connect to both healthcare (e.g., patient care, natural language processing) and cybersecurity (e.g., cyberattacks, phishing, network security) focused topics. ChatGPT and Large Language Models, on the other hand, are associated with new and emerging themes, reflecting the field's current research trends. These findings demonstrate that generative AI is being addressed in an interdisciplinary manner in both healthcare and cybersecurity, with research focusing on distinct subthemes.

3.7 Sensitivity Analysis

To evaluate the robustness of the findings, a broader (expanded) search strategy was applied. This expanded query included additional generative AI model families (e.g., LLMs, diffusion models, GANs), threat-relevant terms (deepfake, prompt injection, jailbreak), and a wider set of security-domain keywords (cybersecurity, network security, digital security). The expanded search was used exclusively for sensitivity testing and was not part of the primary dataset. Table 7 shows the extended queries used for sensitive analysis.

Table 7. Expanded search strategy used for sensitivity analysis

Database	Expanded Search Query
WoS (Expanded)	TS=(("information security" OR "cyber security" OR cybersecurity OR "network security" OR "digital security" OR "data security" OR "computer security") AND ("generative AI" OR "generative artificial intelligence" OR "GAI" OR "GenAI" OR "large language model" OR "large-language model" OR LLM OR "foundation model" OR "diffusion model" OR "generative model" OR "generative models" OR GAN OR "generative adversarial network" OR "generative adversarial networks" OR deepfake OR deepfakes OR "synthetic media" OR "text-to-image" OR "text-to-image model" OR "text-to-image models" OR "prompt injection" OR "prompt-injection" OR jailbreak OR jailbreaks))
Scopus (Expanded)	TITLE-ABS-KEY (("information security" OR "cyber security" OR cybersecurity OR "network security" OR "digital security" OR "data security" OR "computer security") AND ("generative AI" OR "generative artificial intelligence" OR "GAI" OR "GenAI" OR "large language model" OR "large-language model" OR LLM OR "foundation model" OR "diffusion model" OR "generative model" OR "generative models" OR GAN OR "generative adversarial network" OR "generative adversarial networks" OR deepfake OR deepfakes OR "synthetic media" OR "text-to-image" OR "text-to-image model" OR "text-to-image models" OR "prompt injection" OR "prompt-injection" OR jailbreak OR jailbreaks))

The narrow search produced 387 raw records, which, after removing 37 duplicates, resulted in approximately 350 unique documents. In comparison, the expanded search returned 474 raw records, and following the same deduplication procedures, 401 unique documents remained. This means that the expanded query contributed an additional 51 unique publications (≈14.5% increase) beyond the narrow dataset.

Despite the larger coverage of the expanded dataset, the main structural patterns remained consistent. The leading countries (China, USA), core sources (IEEE Access, Computers & Security), and dominant thematic axes (privacy health applications and cyber-threat/defense mechanisms) were preserved across both datasets. The broader query primarily introduced additional recent topics particularly LLM security, prompt injection, and AI red teaming which emerged after 2023.

The dominant thematic axes, (i) privacy, data governance, and health-related AI applications, and (ii) adversarial attacks, cyber-threat intelligence, and defensive mechanisms, were preserved in both datasets. The additional records in the expanded search primarily introduced subclusters related to LLM vulnerabilities, deepfake manipulation, prompt injection,

and jailbreak attacks, but these did not form new independent thematic structures. Therefore, the expanded dataset confirms that the main findings derived from the narrow search are robust and not sensitive to query expansion.

4 CONCLUSION AND SUGGESTIONS

With the diversification of security threats brought about by digitalization, digital security has become a critical area today. This study systematically examines the place of generative artificial intelligence in the digital security literature. A search was conducted on September 3, 2025, using the Web of Science and Scopus databases, using the keywords "generative artificial intelligence" and "cybersecurity" or "information security." After excluding common publications, the remaining 350 unique publications were analyzed using RStudio, VOSviewer, and Gephi. The analysis results show that the distribution of publications by year reveals a rapid increase in research in the fields of generative artificial intelligence and digital security since 2023. When author productivity is examined according to Lotka's law, most authors contributed to the literature with a single publication, and the United States and India stand out as the countries with the highest contributions. Furthermore, it is observed that publications are concentrated in core journals such as IEEE Access and Lecture Notes in Computer Science. Keyword and thematic analyses reveal that generative artificial intelligence focuses on two main areas: healthcare, data privacy, and artificial intelligence applications, and cybersecurity, attack detection, and threat analysis.

The red cluster (AI and learning technologies) requires concrete measures such as privacy-risk assessments, transparent model cards, synthetic-data governance policies, and traceable AI pipelines. The green cluster (cybersecurity and adversarial threats) calls for red-team test suites, SBOM style supply chain traceability for AI models, adversarial robustness benchmarks, and secure prompt engineering guidelines. Together, these cluster-specific recommendations strengthen both the safe development and the secure use of generative AI systems.

Overall, based on the results of the analysis, research can be increased at the international level to foster more integrated and interdisciplinary development of the field. Various guidelines and standards can be developed regarding the safe use of generative AI in critical areas such as healthcare, data privacy, etc. Because digital security research is still in its infancy, risks related to the misuse of generative AI can be identified, and methodologies can be developed to mitigate these risks.

Conflict of Interest Statement

There is no conflict of interest between the authors.

Statement of Research and Publication Ethics

The study is complied with research and publication ethics.

Artificial Intelligence (AI) Contribution Statement

The use of artificial intelligence in this article has been limited solely to assisting with translation in certain sections.

Contributions of the Authors

Sevinç AY: Methodology, analysis and interpretation, writing original draft, writing review and editing, conclusions and recommendations, resources.

Songül KARAKUŞ: Introduction and literature, writing original draft, writing review and editing, conclusions and recommendations, resources.

REFERENCES

[1] B. Ersöz and H. İ. Bülbül, "Üretken Yapay Zekâ Fırsatlar ve Tehditler: Bibliyometrik Analiz," in *Proc. UBMK 2024 – IXth International Conference on Computer Science and Engineering*, 2025, pp. 337–342.

[2] E. Güler, S. Uğur, and C. Güler, "Eğitim fakültesi öğretim elemanlarının üretken yapay zekâya yönelik farkındalıklarının belirlenmesi ve öğretmen yetiştirmede kullanımına yönelik öneriler," *Mehmet Akif Ersoy Üniversitesi Eğitim Fakültesi Dergisi*, no. 74, pp. 618–647, 2025.

[3] M. Herrador and J. Rehberger, "SpAIware: Uncovering a novel artificial intelligence attack vector through persistent memory in LLM applications and agents," *Future Generation Computer Systems*, early access, vol. 174, p. 107994, 2026.

[4] I. Aldasoro, S. Doerr, L. Gambacorta, S. Notra, T. Oliviero, and D. Whyte, "Generative artificial intelligence and cyber security in central banking," *Journal of Financial Regulation*, vol. 11, no. 1, pp. 119–128, 2025.

[5] Z. Hatipoglu, B. Yaman, S. Ceylan, and U. Kose, "Cyber Security Training with Generative Artificial Intelligence Supported Web Platform Using IoT Cyber Threat Scenarios," in *Proc. 2024 Cyber Awareness and Research Symposium (CARS)*, IEEE, Oct. 2024, pp. 1–6.

[6] S. Ankalaki, A. A. Rajesh, M. Pallavi, G. S. Hukkeri, T. Jan, and G. R. Naik, "Cyber attack prediction: From traditional machine learning to generative artificial intelligence," *IEEE Access*, vol. 13, pp. 44662-44706, 2025.

[7] B. S. Sarikaya and Ş. Bahtiyar, "GenAI-Based Jamming and Spoofing Attacks on UAVs," *IEEE Access*, vol. 13, pp. 107596-107620, 2025.

[8] L. Coppolino, S. D'Antonio, G. Mazzeo, and F. Uccello, "The good, the bad, and the algorithm: The impact of generative AI on cybersecurity," *Neurocomputing*, vol. 623, p. 129406, 2025.

[9] M. A. Ferrag, F. Alwahedi, A. Battah, B. Cherif, A. Mechri, N. Tihanyi, T. Bisztray, and M. Debbah, "Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities," *Internet of Things and Cyber-Physical Systems*, 2025, pp.1-46.

[10] W. Badawy, "6G-Enabled IoT Networks Cyber Threat Prevention Using Generative AI," in *Proc. 2024 International Conference on Future Telecommunications and Artificial Intelligence (IC-FTAI)*, IEEE, Dec. 2024, pp. 1–4.

[11] T. N. Shree, K. Sundarakantham, J. Dhivya, and B. Gayathri, "Detecting Cyber Threat Using Gen-AI," in *Proc. 2025 International Conference on Computational, Communication and Information Technology (ICCCIT)*, IEEE, Feb. 2025, pp. 845–851.

[12]] L. Priya and S. Kapilamithran, "Exploiting AES encryption vulnerabilities through padding oracle attacks and generative AI techniques," in *Proc. 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, IEEE, Oct. 2024, pp. 682–689.

[13] E. Garfield, "Bradford's Law and Related Statistical Patterns," *Essays of an Information Scientist*, vol. 4, pp. 476–483, 1980.

[14] E. Torun and K. Bozkuş, "Sınıf yönetimi araştırmalarının bibliometrik analizi," *Studies in Educational Research and Development*, vol. 6, no. 1, pp. 20–51, 2022.

[15] Y. Tonta and U. Al, "Türkçe Makalelerin Dergilere Dağılımı ve Bradford Yasası," *Bilgi Dünyası*, vol. 9, no. 1, pp. 41–66, 2008.

[16] D. H. Hertzel, "Bibliometrics, history of the development of ideas," in *Encyclopedia of Library and Information Science*, A. Kent, Ed. New York: Marcel Dekker, 1987, pp. 144–219.

[17] M. J. Cobo, A. G. López-Herrera, E. Herrera-Viedma, and F. Herrera, "Science mapping software tools: Review, analysis, and cooperative study among tools," *Journal of the American Society for Information Science and Technology*, vol. 62, no. 7, pp. 1382–1402, 2011.

[18] M. Aria and C. Cuccurullo, "bibliometrix: An R-tool for comprehensive science mapping analysis," *Journal of Informetrics*, vol. 11, no. 4, pp. 959–975, 2017.

[19] Gephi, *Gephi—Makes Graphs Handy*, 2013. [Online]. Available: https://gephi.org. [Accessed: Sep. 3, 2025].