Research Article

Bibliometric Analysis of Publication in the Field of Artificial Intelligence and Cyber Security

Songul Karakus and Sevinc Ay

***Abstract*— With the rapid changes in technology, artificial intelligence and cybersecurity have become two important areas inseparable from each other in today's digital world. The aim of this article is to analyze academic research on artificial intelligence and cybersecurity using bibliometric analysis method by providing an overview of artificial intelligence and cybersecurity. The findings obtained from the bibliometric analysis conducted between 2002-2025 (available at the time of the search) using the Web of Science database revealed that there were a total of 1296 publications and 4023 authors related to artificial intelligence and cybersecurity. The most frequently used keywords were examined by the authors using the VOSviewer software, and as a result of this examination, cybersecurity was found to be repeated 344 times, and artificial intelligence was found to be repeated 238 times. It has been also seen that the data obtained included publications from 97 countries and the country with the highest number of publications has China with 282 publications. The relationships between artificial intelligence and cyber security technologies have been also visualized with VOSviewer software. While artificial intelligence has been suggested in the theme analysis, methods such as intrusion detection system and feature selection have been identified as niche themes. As a result, this study shows the current status of studies on artificial intelligence and cyber security. It is also thought to guide future studies in this field.**

Index Terms— **Artificial intelligence, Bibliometric analysis, Cyber security, R Studio, VOSwiever program.**

I. Introduction

ARTIFICIAL INTELLIGENCE can be defined as computer systems or computer software that can imitate human intelligence functions such as learning, problem solving, visual perception, decision making based on past experiences, etc. Artificial intelligence technologies include almost all areas including health [1], education [2], finance and banking systems [3], automotive [4], e-commerce and marketing [5, 6], agriculture [7], law [8], human resources [9], energy [10], environment [11], art [12], tourism [13], search engines [14], translation [15], storytelling [16], games [17] and cybersecurity [18].

Cyber security can be defined as various measures, strategies or technologies that aim to protect digital systems, computers, devices, networks, data and information systems against all kinds of cyber attacks, threats, disruptions, theft and abuse. With the widespread adoption of digital technologies alongside the internet, cybersecurity has become critically important not only in protecting our personal data in the digital realm but also in safeguarding highly sensitive information at the government level [19]. According to the relevant literature, cyber security has three main objectives: confidentiality, integrity and availability. They have been briefly called the CIA trio. Confidentiality is the preservation of personal data and confidential matters to which access authority must be granted. Integrity means that data cannot be changed or any action can be taken without authorization. Finally, usability can be expressed as using the relevant system as expected [20].

In recent years, artificial intelligence and cybersecurity have begun to attract more and more attention in today's digital world. While artificial intelligence is a support element in detecting threats and improving defense strategies in the field of cyber security, it can also be a threat element when used in cyber attacks by malicious people. Therefore, we can talk about a two-way impact of artificial intelligence in the field of cyber security.

In this study, a bibliometric analysis of the studies conducted in the fields of artificial intelligence and cyber security was conducted to find out the general trend. Bibliometrics is defined as the statistical and mathematical analysis of publications prepared on a subject or field using data such as year, citation, author, country, subject, source and university. The bibliometric analysis method is a method that examines and analyzes studies in scientific literature and explains them with numerical data. This analysis can be used to determine the direction in which the studies are trending, author and institution interactions, distribution across countries, academic networks, etc. in order to reveal the necessary information from scientific maps and networks [21, 22, 23]. In addition, with this method, relationship densities, power values and connections between data, maps or networks are determined [24]. Connections reveal the potential for similarities, relationships or partnerships that are obtained as a result of the analysis of the resulting data with different elements. With the bibliometric

Songul Karakus, is with Department of Computer Engineering University of Bitlis Eren, Bitlis, Turkey,(e-mail: skarakus@beu.edu.tr).
https://orcid.org/0000-0003-1999-0203

Sevinc Ay, is with Department of Distance Education Center University of Firat, Elazig, Turkey, (e-mail: say@firat.edu.tr).
https://orcid.org/0009-0001-6309-0889

Manuscript received Nov 24, 2024; accepted Mar 07, 2025.
DOI: 10.17694/bajece.1585201

analysis method, analyses such as citation analysis, authors and collaborations, keyword and trend analysis, number of publications, etc. can be performed [25]. Bibliometric analysis is a very powerful method for evaluating scientific studies, ensuring collaborations and determining the current situation.

Studies on artificial intelligence and cyber security are very important in identifying possible threats in this area and taking security measures or making existing security measures more effective. Particularly, the development of artificial intelligence in areas such as machine learning, deep learning, natural language processing, and the internet of things significantly affects cyber security applications. Artificial intelligence-based methods are used in cyber security for threat detection and anomaly detection [26, 27], malware detection [28], network intrusion detection [29], response to cyber attacks [30], vulnerability detection and penetration testing [31], social engineering and phishing attacks [32], and phishing/spam detection [32, 33].

Some studies on artificial intelligence and cyber security are as follows. In the study conducted by Aytan and Barışçı [35], artificial intelligence-based attack detection and analysis were performed in cyber defense. For this purpose, they tried to detect denial of service attacks and information scanning attacks using the "KDD Cup'99" data set and the machine learning methods in the Weka program. As a result, they achieved a success rate of 99%. Özdemir [36] investigated the impact of artificial intelligence and machine learning on cyber threat intelligence and examined how they can be integrated into applications related to cyber threat intelligence with case studies. Li et al. [37] conducted a study on how to improve real-time false alarm detection in network attacks by combining machine learning methods with deep learning to detect real alarms more accurately. They achieved successful results in the study. Liu et al. [38] conducted a review study focusing on methods that use machine learning techniques to model and detect hybrid cyber attacks in the industrial Internet of Things. They also discussed the difficulties and research trainings of analyzing industrial internet of things and cyber attacks and made some suggestions. Li [39] conducted a compilation study on cyber security and artificial intelligence. In this study, machine learning and deep learning methods are first summarized in terms of combating cyber attacks. Then, the attacks that artificial intelligence may be exposed to were classified.

The remainder of the study is organized as follows. In the second part of the study, the method of the research is mentioned. In the 3rd chapter, the findings are discussed, and in the last chapter, a general evaluation is made and suggestions are made.

II. METHOD OF THE RESEARCH

The aim of this study is to conduct a bibliometric analysis of studies involving the concepts of artificial intelligence and cyber security between 2002 and 2025 (available at the time of the search) in the light of different parameters. It is aimed that the bibliometric analysis results will guide and contribute to new studies in the field of artificial intelligence and cyber security. Within the scope of the study, the terms "artificial intelligence" and "cyber security" were searched on the Web of Science database using the conjunction "and" and selecting all categories.

Within the scope of the study, the contents obtained from the Web of Science database were examined within the framework of the following questions:

- What is the distribution of studies indexed in the Web of Science database on artificial intelligence and cyber security by category?
- What is the distribution of studies indexed in the Web of Science database on artificial intelligence and cyber security by year?
- Which authors are prominent in the studies indexed in the Web of Science database on artificial intelligence and cybersecurity, and what are the connections between them?
- What are the keywords used in studies indexed in the Web of Science database on artificial intelligence and cybersecurity, and what are the connections between them?
- What is the distribution of studies indexed in the Web of Science database on artificial intelligence and cybersecurity by country and the strength of the connections between these countries?
- What is the distribution of studies indexed in the Web of Science database on artificial intelligence and cybersecurity according to the most cited publications and the strength of the connection between these publications?

In studies where the keywords artificial intelligence and cyber security are used together, analysis by year is important in determining the increasing trend in these areas in recent years. In addition, determining the study areas on artificial intelligence and cyber security issues provides information to researchers who want to work interdisciplinary on this subject. Having a country analysis of the studies will reveal the relations between the countries and will also provide an idea about the prominent language and university connections in this regard. The author analysis conducted between the studies is important in terms of determining the authors who are the school in this field and revealing the cooperation between the publications. While the analyses will guide the studies to be conducted in this field, it is thought that the literature analysis will guide those who will work in this field.

Content indexed in Web of Science was used as the database. The keywords "artificial intelligence" and "cyber security" were used in the search dated 15.10.2024. In the search conducted using the AND conjunction, the All Fields field in Web of Science was selected and 1296 publications were reached. It was seen that these publications have many different categories, the oldest being 2002 and the newest being 2025, including 657 Proceeding Papers, 560 articles, 75 review articles, 24 early Access, 9 book chapters, 5 editorial material, 4 Retracted Publications, 2 data papers, 1 book, 1 book review, and 1 letter. The languages used in the studies were English, German, Chinese, Spanish and Turkish.

For the purpose of bibliometric analysis carried out on studies obtained from the Web of Science database and using the keywords "artificial intelligence" and "cyber security" together,

the Voswiever (version 1.6.20) program and the R studio programs "bibliometrix" package and the biblioshiny application were used. VOSviewer and R Studio are among the most widely used software in bibliometric analysis, offering important functions such as network analysis, clustering and visualization of citation relationships.

III. FINDINGS

Within the scope of the study, bibliometric analysis methods were applied to the studies indexed in the Web of Science database on artificial intelligence and cyber security in order to find answers to the research questions listed above. The categories of the data obtained as a result of the analysis are given in Figure 1.

Fig.1. Categories of publications containing the concepts of artificial intelligence and cybersecurity in the Web of Science database [40]

Among the categories with the most publications in the fields of artificial intelligence and cyber security, the first five places were taken by Computer Science Artificial Intelligence with 35.76%, Computer Science Information Systems with 30.31%, Electrical and Electronics Engineering with 27.70%, Computer Science Theory Methods with 26.094% and Computer Science Interdisciplinary Applications with 22.66%, respectively. Among the fields studied, there are also publications belonging to different categories such as Physics, Chemistry, Mathematics, Environmental Sciences and Telecommunications. General information about the data obtained from 1296 studies subject to bibliometric analysis is given in Table 1.

.

TABLE I
GENERAL INFORMATION ABOUT THE STUDIES

Time period	2002:2025
Sources (Magazines, Books, etc.)	719
Total number of publications	1296
Annual Growth Rate %	2,97
Average age of studies	2.71
Average number of citations per study	11.79
References	49394
Keywords (ID)	874
Authors	4023
Number of authors of single-authored studies	105
Number of single-authored studies	114
Co-authors per study	3.89
International co-authorships %	30.71

When Table 1 is examined, it is seen that 1296 publications published between 2002 and 2025 are included in 719 different sources. The total number of references for publications was determined as 49394. Other data obtained from the table include the information that 114 of these publications were

single-authored and that an average of 2.97% of new publications were produced annually.

The data obtained through the bibliometric analysis applied within the scope of the study were examined in terms of distribution and link strength according to the years of publication, fields of publication, countries with the most publications, universities with the most publications, most used keywords, most cited authors and most cited publications. Firstly, the distribution according to the years of publication was examined. The findings obtained in the study are given under subheadings.

Publications in the Web of Science database using the terms artificial intelligence and cyber security together were made between 2002 and 2025. Among the publication years, the highest number was reached in 2024 with 224. Figure 2 shows the distribution of publications by year.

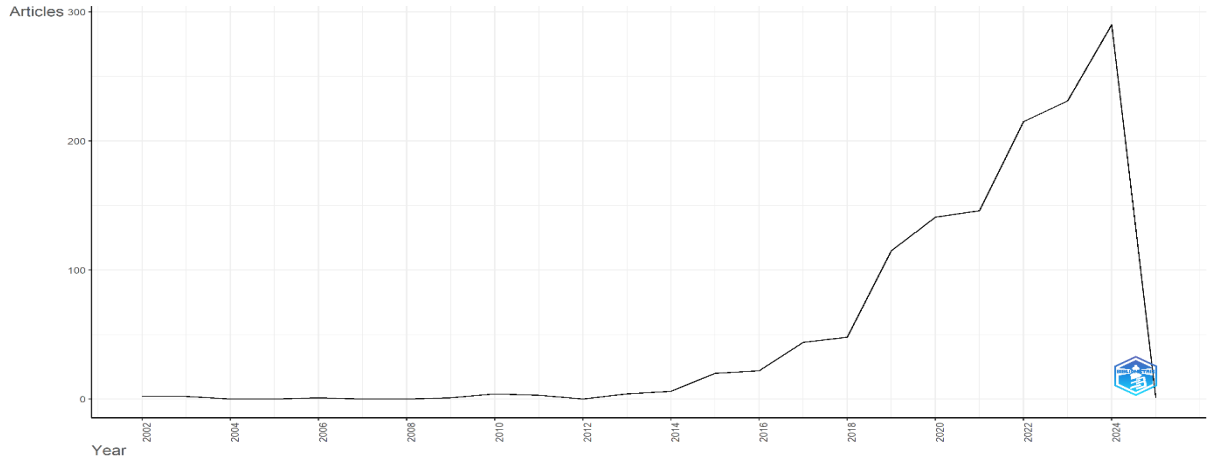

Fig.2. Distribution of publications by year

As Figure 2 shows, very little work has been done in the field between 2002 and 2014. In total, 23 studies were carried out between these years. It is observed that this area, where studies were very few until 2014, gained rapid momentum especially after 2019.

A. Author Profile and Network Analysis

A total of 4023 authors' works were obtained from the dataset obtained from the Web of Science database between the years 2002-2025. The five most influential authors working in the fields of artificial intelligence and cybersecurity over the years are Yang Zhang with 19 publications, Jinjin Li with 14 publications, Jingshi Yang with 14 publications, Yicheng Liu with 13 publications, and Yisen Wang with 11 publications, respectively.

The most relevant authors are presented in Figure 3.

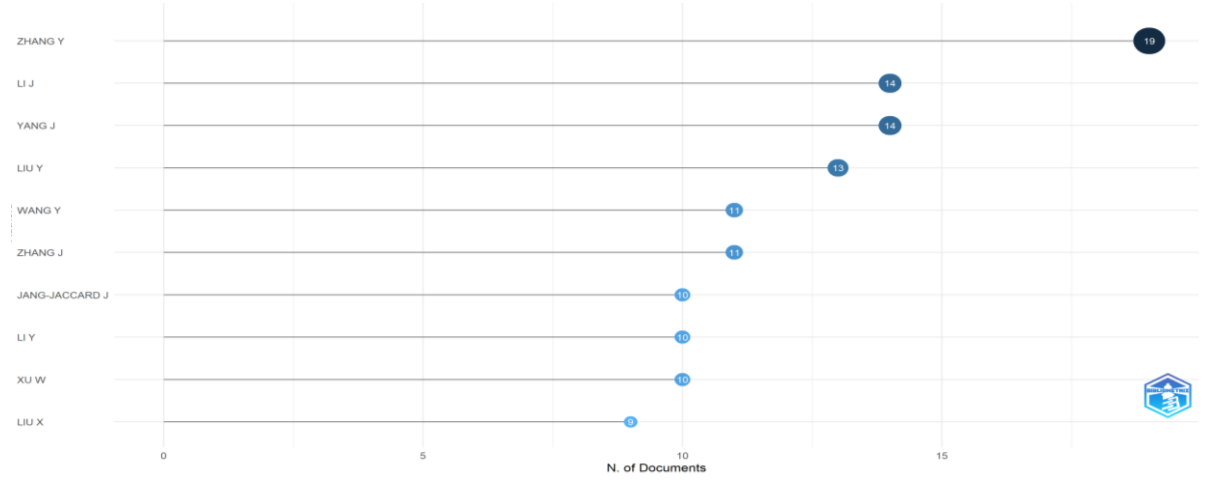

Fig.3. The most relevant authors and the number of publications they produced

When we look at the productivity status of the authors over the years, it is seen that Yang Zhang, Jinjin Li, Jingshi Yang, Yicheng Liu, Yisen Wang took the first places between 2015 and 2025, when the intensity of the studies increased. Figure 4 shows the productivity status of the authors.

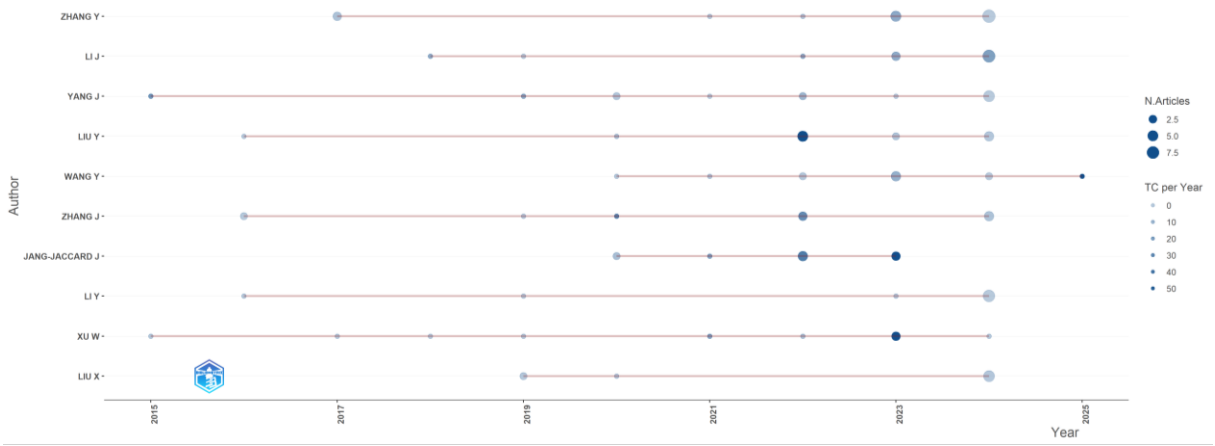

Fig.4. Productivity status of writers by year

B. *Keyword Analysis*

In publications obtained from the Web of Science database in the fields of artificial intelligence and cyber security, the most frequently used keywords by authors were cyber security with 344 repetitions, artificial intelligence with 238 repetitions, machine learning with 214 repetitions, deep learning with 133 repetitions, and internet of things with 50 repetitions. Another keyword analysis conducted within the scope of the study is to determine the usage density of author keywords that changes over the years. As a result of this analysis, when the studies conducted in recent years are examined, it is seen that the concepts of deep learning, artificial intelligence, internet of things, blockchain, and intrusion detection come to the fore, especially in 2022 and beyond. Figure 5 shows the network map of the change in author keywords in the publications in the dataset over the years

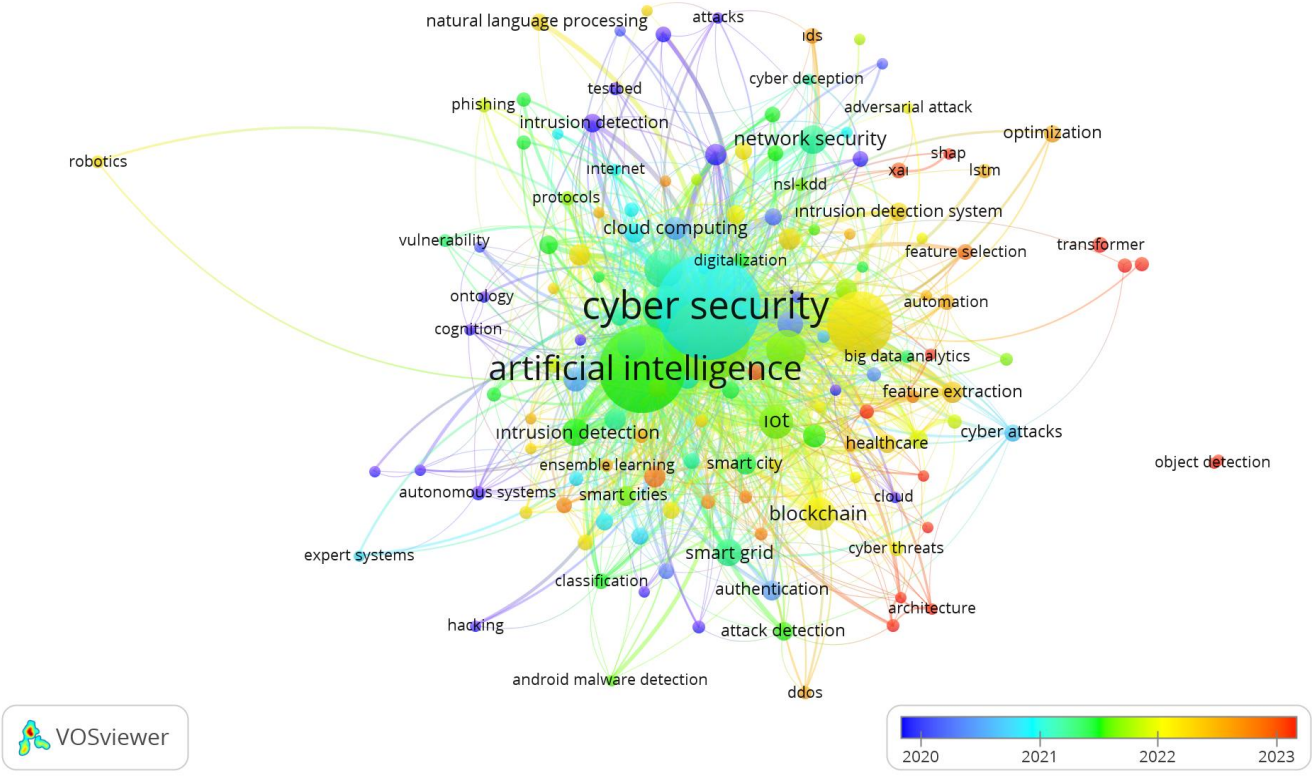

Fig.5. Most frequently used keywords and their links

In the visualization of the most frequently used keywords in the word cloud format obtained from the studies obtained from the Web of Science database, it is seen that the first five words are artificial intelligence, cyber security, attacks, intrusion detection and classification. Figure 6 shows the World cloud

obtained from the most frequently used keywords and prepared by the R-Studio program.

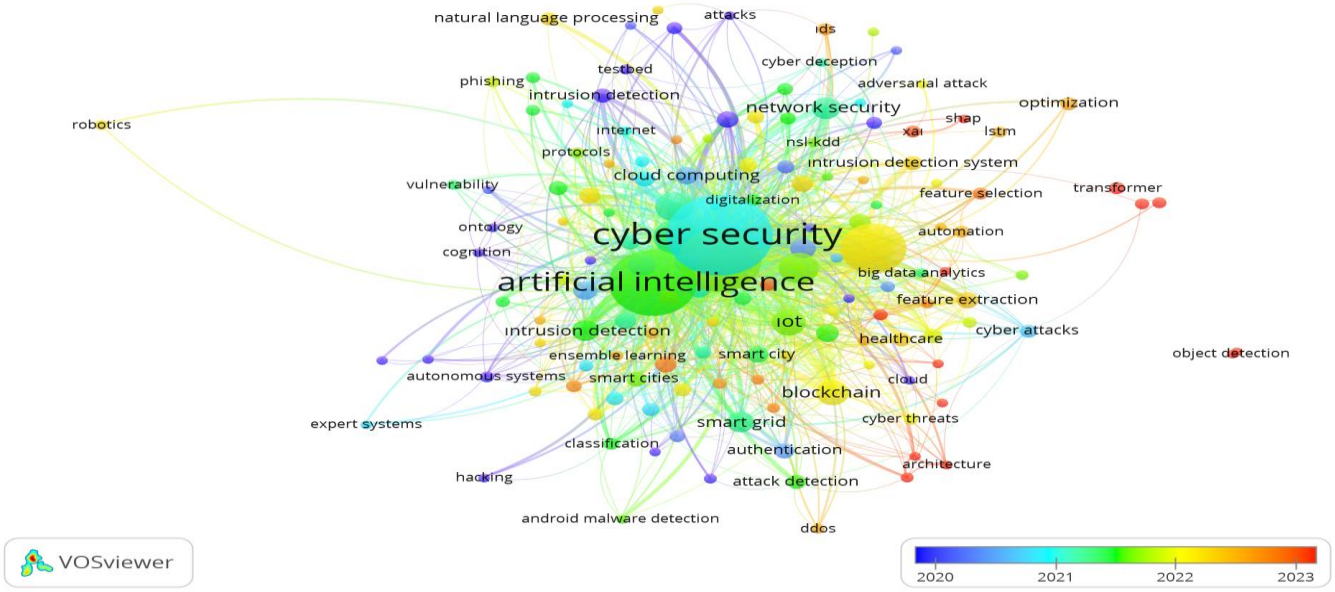

Fig.6. Keyword cloud

C. *Network Analysis of Countries*

It was determined that the data obtained from the Web of Science database included publications from 97 countries. Among the 62 countries that passed the threshold by meeting the conditions of at least 1 publication and 1 citation, it was determined that the countries with the most publications were China (282 publications), the USA (217 publications), India (125 publications), the UK (102 publications) and Saudi Arabia (96 publications), respectively. The top five most cited countries are the USA (3846 citations), the UK (3260 citations), India (2950 citations), China (2564 citations) and Australia (1832 citations). The top five countries in terms of total connection power are the United States, China, Saudi Arabia, India and Australia. Table 2 shows the publication numbers for each country.

TABLE II
NUMBER OF PUBLICATIONS, NUMBER OF CITATIONS AND TOTAL LINK STRENGTH OF COUNTRIES

Country	Number of Publications	Number of Citations	Total Link Strength
People's Republic of China	282	2564	18955
USA	217	3846	19063
India	125	2950	17445
England	102	3260	12990
Saudi Arabia	96	1241	18092
Australia	83	1832	13446
South Korea	66	799	7944
Italy	57	873	6499
Israel	50	496	3583
United Arab Emirates	41	447	8605
Canada	41	426	5743
Germany	41	375	4812
Pakistan	35	481	10653
Greece	35	297	3559
Spain	33	260	3811
France	31	305	2799
Malaysia	26	225	3995
Singapore	25	909	2135
Romania	24	62	387

According to the findings obtained from the data set, the countries are listed according to the number of publications in Table 2, which shows the number of publications, the number of citations and the strength of the connection between them. In order to make a bibliographic analysis of the publications according to their countries, the relationship between 62 countries that have a relationship between them was examined within the scope of the criteria of at least 1 work published and 1 citation. Figure 7 shows the analysis showing the bibliographic coupling of countries.

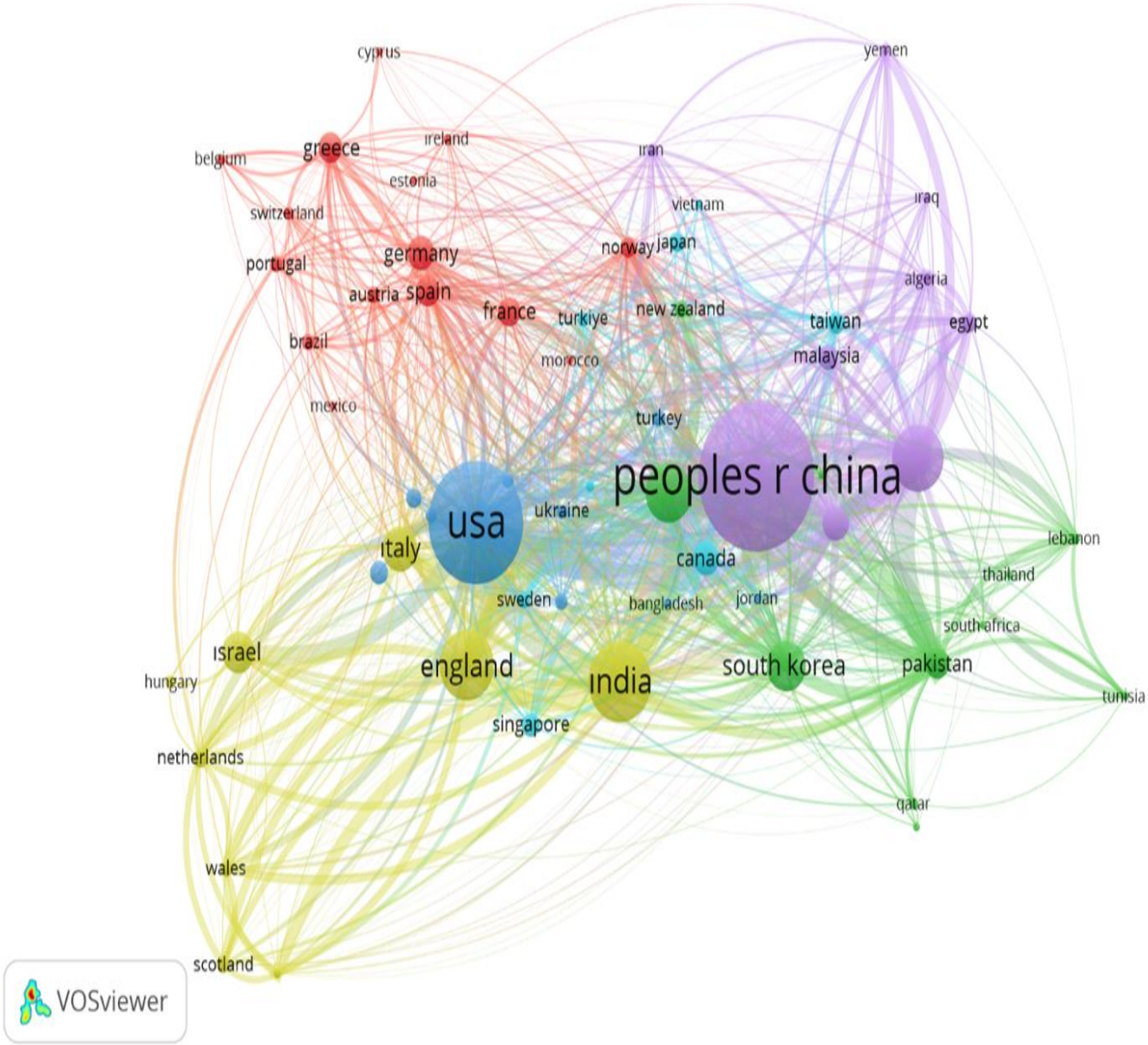

Fig.7. Network map showing bibliographic matching of countries

D. Citation Analysis

Author and source citation analysis was examined in order to perform citation analysis on the data set obtained from the Web of Science database. In order to perform author citation analysis, the criterion of having at least 1 publication and 1 citation was applied. Out of 4023 authors, 2964 authors passed the threshold value. Among the authors, Niti Upadhyay (470 citations), Zhon Lin Wang (405 citations), Jin Yang (341 citations), Julian Jan-Jaccard (312 citations) and Fadi Al-Turjman (296 citations) are at the top of the list. Figure 8 shows the network map of the most cited authors based on the findings from the dataset.

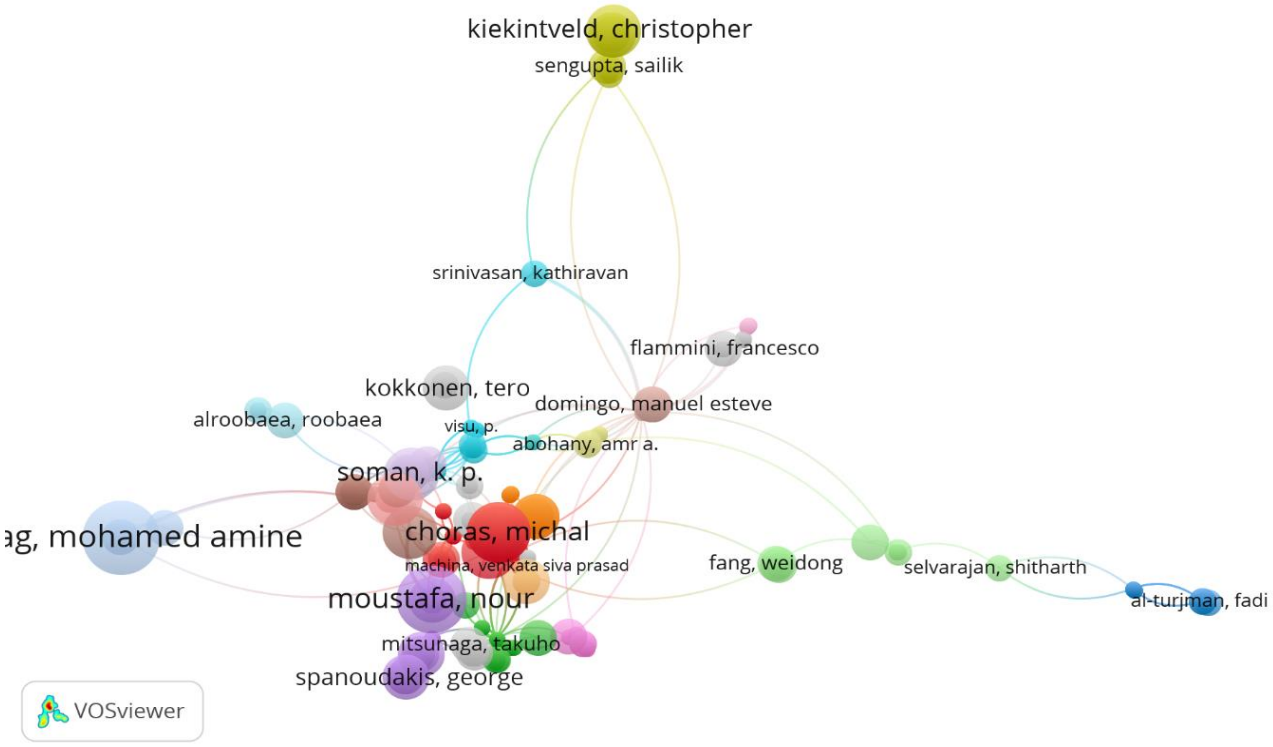

Fig.8. Network analysis showing authors' citation ties

Another analysis most frequently used in studies is the analysis of sources. When the analysis of the resources was examined, it was determined that the production was highest after 2018 and reached its highest values in 2024. Table 3 shows the data for the top ten sources with the most publications.

TABLE III
PUBLICATION NUMBERS OF SOURCES

Sources	Articles
Proceedings of the 3rd International Conference on Cybersecurity, Artificial Intelligence and Digital Economy 2024, CSAIDE 2024	115
IEEE Access	59
Electronic	24
Sensors	23
2023 IEEE Cybersecurity and Resilience, CSR International Conference	12
Computers and Security	12
Sustainability	12
2023 25th International Conference on Advanced Communication Technologies, ICACT	11
Applied Sciences-BASEL	11
Computers and Electrical Engineering	8

As a result of examining the sources in terms of bibliographic analysis, bibliographic match was revealed. Bibliographic matching on sources is defined as the citation of a common work by two independent sources as a result of the citation analysis. While examining the citation analysis of the sources, the criterion of having at least 1 publication and 1 citation was determined and 501 sources that passed the threshold value were listed. Figure 9 shows the network map showing the citation analysis of the sources.

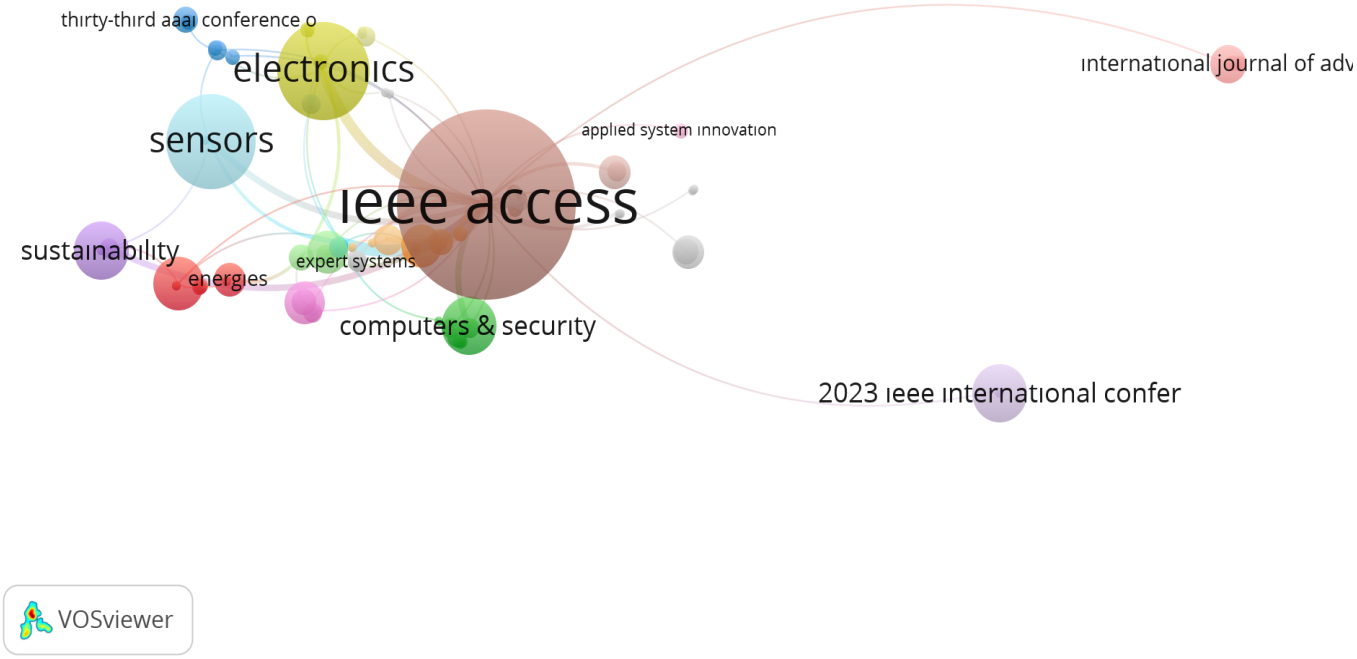

Fig.9. Citation network map of sources

E. Featured Trend Topics in The Field (Themes Analysis)

New fields of study and trending topics in the fields of cyber security and artificial intelligence have differentiated over the years. These topics have changed according to the prominent technological developments of the period. There are subject areas that have about to disappeared, as well as subject areas that feed a different subject in the new period and form the basis for its development. Identifying prominent themes and topics is important for researchers who want to work in this field to show current trends in the field. Min Cluster Frequency was selected as "5" for the Thematic map. Clustering Algorithm was selected as "Louvain". The selected algorithm is an algorithm that focuses on densities and prevents distributed clustering. Figure 10 presents a thematic map that provides a comprehensive analysis of academic studies in the field.

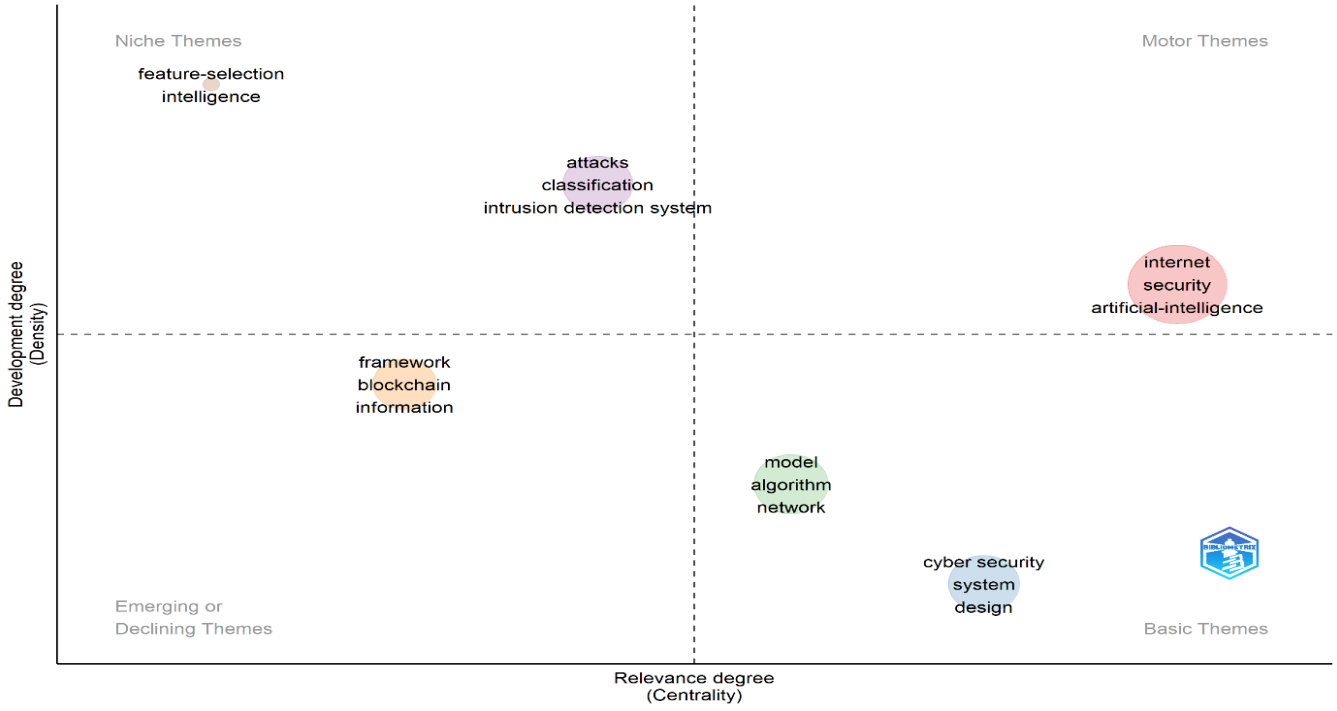

Fig.10. Agenda for future research (thematic map)

The X axis of the diagram represents network cluster centrality, which measures the degree to which clusters interact with each other and indicates the importance of a study theme. The Y-axis represents density, which is a measure of the internal connectivity of network clusters and a measure of theme growth.

Niche themes are defined as themes that cover a more specific area rather than a broad and general area While these themes were not directly related to the research area, they were developed and included in the field. Niche themes that stand out in the research area are categorized into two groups. The first set of prominent themes includes attacks, classification, intrusion detection system. The other cluster, which has not yet developed and attracted academic interest, consists of feature-selection and intelligence.

The motor themes have high centrality and high density. It includes important subject areas that shape the research field and contribute to its development. In other words, it means important and central topics in the field. The main cluster, which includes internet, security, artificial-intelligence, represents the leading motor themes in the field.

Emerging and declining themes have low centrality and low density. It represents themes that are likely to trend in the future and themes that are slowly fading into oblivion. In the diagram, the themes of framework, blockchain and information are in this group.

The basic themes have high centrality and low density. They represent interconnected topics that are more prominent in interdisciplinary studies. It is represented by two clusters in the diagram. The first cluster includes model, algorithm and network topics. The other cluster consists of cyber security, system and design topics, which are the leading and most fundamental topics in the research field.

Thematic Evolution is another analysis made while examining the issues in the study area. Themes that emerged and disappeared on selected important breakpoint dates are presented. Figure 11 shows thematic evolution, which shows past studies in this field and sheds light on future studies.

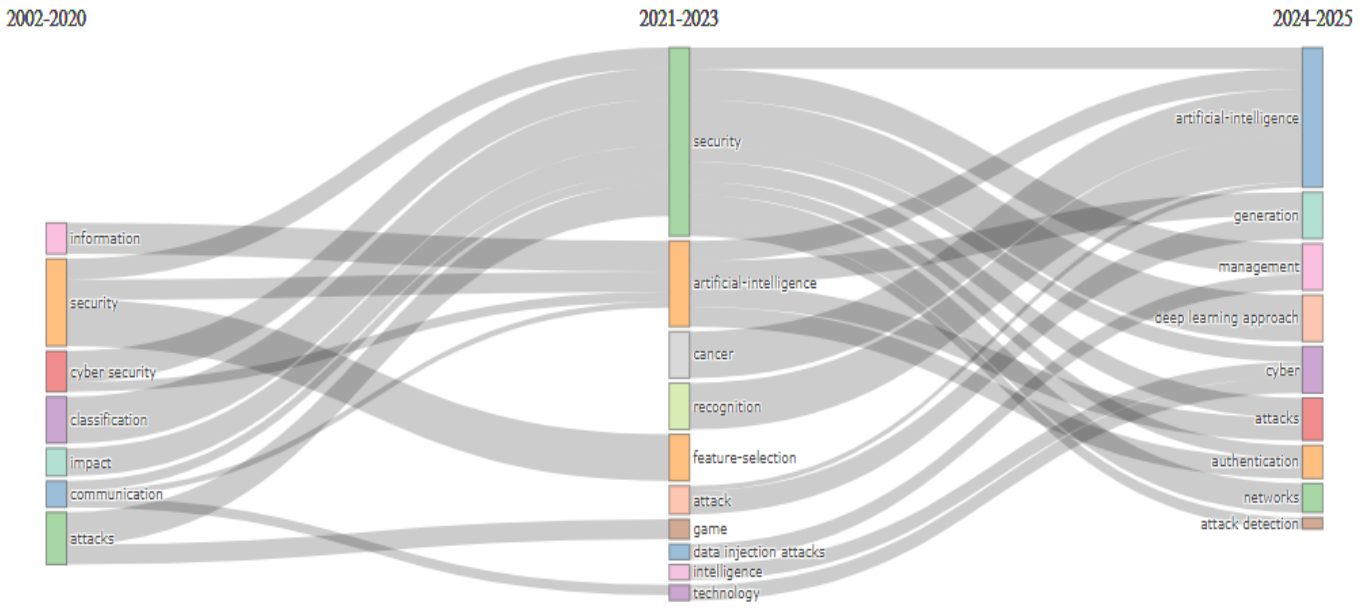

Fig.11. Thematic evolution of prominent topics in the research field

Among the parameters selected for the analysis, Min Cluster Frequency was set as 5, Clustering Algorithm as “Walktrap”, Min Weight Index as “0.1”, Number of Labels as “3”. The year 2020 was chosen as the breaking point in the diagram. This date was chosen because it is the year when the researches increased the most. After 2020, it is seen that the information field completely disappeared and fed the artificial intelligence subject area in the following period. Classification, impact, communication topics were combined under the security topic in the next period. The subject areas that are expected to remain important in the future are artificial intelligence, deep learning aproach, authentication, attack detection.

IV. CONCLUSION AND RECOMMENDATIONS

In today's digital world, artificial intelligence and cybersecurity have become increasingly integrated and complementary to each other. More effective solutions can be offered when combating threats in cyber security, By integrating these two areas. In this study, a bibliometric analysis was conducted on studies in the field of artificial intelligence and cyber security.

The Web of Science database was searched using the keywords "artificial intelligence" and "cyber security" using the conjunction "and" and selecting "all fields". A data set was created with the data obtained as a result of this search. The results of the bibliometric analysis conducted according to keywords, authors, countries and citations within the scope of the study are summarized below. The distribution by years of 1296 publications made between 2002 and 2025 (available at the time of the search) was examined. It was stated that the publications in the field of study increased after 2019 and the year 2024 stood out with 224 publications among the publication years. Studies have been prepared mostly in English. Among 4023 authors, the most influential authors were determined to be Yang Zhang, Jinjin Li, Jingshi Yang, Yicheng Liu, and Yisen Wang. According to the keyword analysis, the most frequently used keywords are cyber security, artificial intelligence, machine learning, deep learning and internet of things. Data obtained from the Web of Science database showed that studies were conducted in 97 countries. China (282 publications), USA (217 publications), India (125 publications), UK (102 publications) and Saudi Arabia (96 publications) are ranked as the top five countries. Another criterion taken into consideration when analyzing on a country basis is the number of citations. The most cited countries are the USA, China and India. The most commonly used sources in the studies were Proceedings of the International Conference on Cybersecurity, Artificial Intelligence and Digital Economy, IEEE Access, International Conference on Electronics, Sensors, Cybersecurity and Resilience.

The prominent study topics in the fields of cyber security and artificial intelligence were analyzed in the themes analysis section. In the topics examined in four groups as niche themes, motor themes, emerging and declining themes and basic themes, artificial-intelligence came to the fore in motor themes, while intrusion detections system, feature-selection were identified as niche themes. Cyber security was found as basic themes. When the study topics were analyzed according to years, it was determined that artificial intelligence, deep learning aproach, authentication, which was selected as the breaking point in 2020, are promising subject areas.

It is thought that the study will guide new researchers who will work in this field on the use of artificial intelligence in cyber security. In order to increase the effectiveness of the study, Voswiever (version 1.6.20) and R Studio programs were used together and the analysis results obtained from both programs were presented. The scope of the study can be expanded to include deep learning and cryptology fields and contribute to the literature. In addition, the study was conducted covering only the Web of Science database. The scope can be expanded by adding data from Scopus and Google Scholar databases in future studies.

REFERENCES

[1] H. Hoşgör, H. Güngördü. "Sağlıkta Yapay Zekanın Kullanım Alanları Üzerine Nitel Bir Araştırma.", European Journal of Science and Technology, Vol.35, 2022, pp. 395-407.

[2] F. Coşkun, H.D. Gülleroğlu. "Yapay zekânın tarih içindeki gelişimi ve eğitimde kullanılması.", Ankara University Journal of Faculty of Educational Sciences (JFES), Vol.54, No.3, 2021, pp.947-966.

[3] E. Gümüş, B. Medetoğlu, S. Tutar. "Finans ve bankacılık sisteminde yapay zekâ kullanımı: kullanıcılar üzerine bir uygulama.", Journal of Bucak Business Administration Faculty, Vol.3, No.1, 2020. pp.28-53.

[4] B. Kesici, M.S. Yıldız. "Kalite kontrol faaliyetlerinde yapay zekâ kullanımı ve bir otomotiv yan sanayisinde uygulanması.", Yalova Journal of Social Sciences, Vol.6, No.12, 2016, pp.307-323.

[5] E.Ö. Çizer, "Pazarlamada Yapay Zeka Uygulamaları." Individual, Society, Politics in the Digitalizing World, Congress Abstracts, İstanbul, Turkey, 26-27 May 2022.

[6] H. Güven, E.T.A. Güven. "Yapay Zekâ Uygulamalarının E-Ticarette Kullanımı.", International Journal of Management and Administration, Vol.7, No.13, 2023, pp.69-94.

[7] İ Terzi, M.M. Özgüven, Z Altaş, T. Uygun. "Tarımda Yapay Zeka Kullanımı.", International Erciyes Agriculture, Animal & Food Sciences Conference, Kayseri, Turkey, 24-27 April 2019.

[8] Z. Öğretmen Kotil. "Hukukta Yapay Zekâ Uygulamaları.", Artificial Intelligence Working Group, 2022, pp.1-12.

[9] C. Tiftik. "Insan kaynakları yönetiminde yapay zekâ teknolojileri ve uygulamaları.", IBAD Journal of Social Sciences, Vol.9, 2021. pp.374-390.

[10] R. Dirik, E. Taşkesen, Ö. Dirik. "Yenilenebilir Enerji Kaynaklarında Yapay Zekâ Kullanımı.", In International Conference on Recent Academic Studies, Vol.1, 2023, pp.28-35.

[11] N.S. Partigöç. "Afet risk yönetiminde yapay zekâ kullanımının rolü.", Journal of Information Technologies (JIT), Vol.15, No.4, 2022, pp.401-411.

[12] A. Tekin. "Yapay zeka kullanımının sanata etkileri.", Journal of Urban Academy, Vol.11 No.4, 2018, pp.692-702.

[13] M.Y. Başer, A. Olcay. "Akıllı turizmde yapay zekâ teknolojisi." Gaziantep University Journal of Social Sciences, Vol. 21, No.3, 2022. pp. 1795-1817.

[14] T.M. Erbir, O. Sevli. "Arama Motorlarında Yapay Zekâ Teknolojilerinin Kullanımı." 10th International Nardin Artuklu Scientific Researches Conference , Turkey, 2023.

[15] X. Liu, C. Li. (2023). *Yapay zeka ve çeviri*. Routledge Çeviri Teknolojisi Ansiklopedisi Routledge, 2023, p. 280-302.

[16] B. Anadolu. "Dijital hikâye anlatıcılığı bağlamında yapay zekânın sinemaya etkisi: Sunspring ve It's No Game filmlerinin analizi.", Journal of Erciyes Communication, Vol.1, 2019, pp.39-56.

[17] A. Efe. "Oyun Teorisi Perspektifinden Bilgisayar Oyunlarında Yapay Zekâ Kullanımı Üzerine Bir Değerlendirme.", Istanbul Gelisim University Journal of Social Sciences (IGUJSS), Vol. 11, No.1, 2024, pp.422-441.

[18] M.M. Mıjwıl, E. Sadıkoğlu, E. Cengiz, H. Candan. "Siber Güvenlikte Yapay Zekanın Rolü ve Önemi: Bir Derleme.", Journal of Data Science, Vol.5, No.2, 2022, pp.97-105.

[19] R. Von Solms, J. Van Niekerk. "From information security to cyber security.", Computers & Security, Vol.38, 2013, pp.97-102.

[20] A. Tekke, A. Lale. "Sosyal Medyada Etik, Bilgi Manipülasyonu ve Siber Güvenlik", Journal of Academic Inquiries (AID), Vol.16, No.2, 2021, pp. 44-62.

[21] N. De Bellis. "Bibliometrics and citation analysis: from the science citation index to cybermetrics.", scarecrow press, 2009.

[22] B. Godin. "On the origins of bibliometrics.", Scientometrics, Vol.68, No.1, 2006, pp.109-133.

[23] C. Chen. "Science mapping: A systematic review of the literature", Journal of Data and Information Science, Vol.2, 2017, pp. 1-40.

[24] N. Jan Eck, L. Waltman. "Software survey: VOSviewer, a computer program for bibliometric mapping.", Scientometrics, Vol.84, No.2, 2010, pp.523-538.

[25] Z.A. Polat, M. Alkan. "Jeodezi, jeoinformasyon ve arazi yönetimi dergisi'nin bibliyometrik analizi.", TMMOB Chamber of Surveying and Cadastre Engineers, Vol.15, 2015, pp.25-28.

[26] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M.A. Latif, F. Al-Turjman, L. Mostarda. "Cyber security threats detection in internet of things using deep learning approach.", IEEE access, Vol.7, 2019, pp.124379-124389.

[27] B.J. Radford, L.M. Apolonio, A.J. Trias, J.A. Simpson, *Network traffic anomaly detection using recurrent neural networks*, arXiv preprint arXiv:1803.10769, 2018.

[28] M.J.H. Faruk, H. Shahriar, M. Valero, F.L. Barsha, S. Sobhan, M.A. Khan, M. Whitman, A. Cuzzocrea, D. Lo, A. Rahman, F. Wu, "Malware detection and prevention using artificial intelligence techniques.", In 2021 IEEE international conference on big data (big data), 15-18 December 2021 (pp. 5369-5377). IEEE.

[29] M. Stampar, K. Fertalj. “Artificial intelligence in network intrusion detection.” In 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE. May 2015.
[30] F.M. Teichmann, S.R. Boticiu. “Adequate responses to cyber-attacks.”, International Cybersecurity Law Review, Vol.5, No.2, 2024, pp.337-345.
[31] S. More, A. Rohela. “Vulnerability assessment and penetration testing through artificial intelligence.”, International Journal of Recent Trends in Engineering Research, Vol.4, No.1, 2018, pp.217-224.
[32] M. Schmitt, I. Flechais. “Digital deception: generative artificial intelligence in social engineering and phishing.”, Artificial Intelligence Review, Vol.57, No.12, 2024, pp.1-23.
[33] İ. Yurtseven, S. Bagriyanik, S. Ayvaz. “A review of spam detection in social media.”, In 2021 6th International Conference on Computer Science and Engineering (UBMK), IEEE, September 2021.
[34] D.J. Dsouza, A.P. Rodrigues, R. Fernandes. *Multi-modal Comparative Analysis on Execution of Phishing Detection using Artificial Intelligence*. IEEE Access, 2024.
[35] B. Aytan, N. Barışçı. “Siber savunma alanında yapay zekâ tabanlı saldırı tespiti ve analizi.” In Proceeding of the 2nd International Symposium on Innovative Approaches in Scientific Studies, Samsun, December 2018.
[36] B. Özdemir. “Siber tehdit istihbaratında yapay zeka ve makine öğrenmesi.”, The Journal of Defence and Security Research, Vol.1, No.1, 2024, pp.75-96.
[37] S. Li, D. Qin, X. Wu, J. Li, B. Li, W. Han. “False alert detection based on deep learning and machine learning.”, International Journal on Semantic Web and Information Systems (IJSWIS), Vol.18, No.1, 2022, pp.1-21.
[38] Y. Liu, S. Li, X. Wang, L. Xu. “A review of hybrid cyber threats modelling and detection using artificial intelligence in IIoT.”, Computer Modeling in Engineering & Sciences, Vol.140, No.2, 2024.
[39] J.H. Li. “Cyber security meets artificial intelligence: a survey.” Frontiers of Information Technology & Electronic Engineering, Vol.19, No.12, 2018, pp.1462-1474.
[40] Web of Science. https://www.webofscience.com/wos/ woscc/analyze-results/b2364eca-c198-4339-b048-dc965c916cdd-4986caa2 (Access Date: 15. 10. 2024

BIOGRAPHIES

Songul Karakus received her undergraduate degree from Fırat University, Department of Computer Education and Instructional Technologies in 2010. She completed her master's degree at Fırat University, Department of Computer Education and Instructional Technologies. She started her doctoral studies at Fırat University Software Engineering Department. She completed her doctorate education in 2020. She is currently working as a faculty member at Bitlis Eren University Computer Engineering Department. Research regions; information security, machine learning, cyber security, software engineering.

Sevinc Ay received her undergraduate degree from Fırat University, Department of Software Engineering in 2016. She completed her master's degree at Fırat University, Department of Software Engineering. She started her doctoral studies at Fırat University Software Engineering Department. She completed her doctorate education in 2023. She is currently working as a Dr. Lecturer at Firat University Distance Education Center. Research regions; deep learning, machine learning, computer vision, image proccessing, video processing, object detection, object tracking, data science.