IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 23 May 2024, accepted 5 June 2024, date of publication 10 June 2024, date of current version 17 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3411632

SURVEY

Neural Networks Toward Cybersecurity: Domain Map Analysis of State-of-the-Art Challenges

RUSLAN SHEVCHUK[1,2], (Member, IEEE), AND VASYL MARTSENYUK[1]
[1]Department of Computer Science and Automatics, University of Bielsko-Biala, 43-309 Bielsko-Biała, Poland
[2]Department of Computer Science, West Ukrainian National University, 46009 Ternopil, Ukraine

Corresponding author: Ruslan Shevchuk (rshevchuk@ubb.edu.pl)

This work was supported by the European Union through the ERASMUS+ Project: The Future is in Applied Artificial Intelligence under Grant 2022-1-PL01-KA220-HED-000088359.

ABSTRACT The growing interest in applying neural networks for cybersecurity has prompted a substantial increase in related research. This paper presents a comprehensive bibliometric analysis of research on cybersecurity towards neural networks published in the Web of Science over the past two decades (2003–2023) using bibliometric methods and CiteSpace software. The analysis encompasses yearly publication trends, types of publications, and trends across various dimensions such as publishing sources, organizations, researchers, countries, and keywords. Additionally, timeline and burst detection analyses were conducted to identify significant topic trends and citations in the last two decades. It also outlines the latest trends, under-explored topics, and open challenges.

INDEX TERMS Neural network, cybersecurity, scientometric database, domain map analysis, CiteSpace.

I. INTRODUCTION

Cybersecurity is the complete package of all techniques and technologies responsible for defending networks, software, and data from potential cyberattacks [1]. As our world becomes increasingly interconnected, the potential for cyberattacks grows [2], [3], [4]. Traditional approaches to cybersecurity, such as signature analysis, incident detection, and firewalls are no longer sufficient to protect against the ever-evolving threat landscape. These methods rely on predefined signatures or rules to identify and block known threats. However, the rapidly evolving nature of cyber threats presents two key challenges that render traditional methods ineffective increasingly:

- Cybercriminals are constantly developing new attack methods (zero-day attacks) that exploit previously unknown vulnerabilities. Traditional methods, reliant on pre-defined signatures, are blind to these novel attacks, leaving systems vulnerable [5], [6].
- Even for known attack types, cybercriminals continuously modify their tactics, techniques, and procedures (TTPs) to evade detection. Traditional rule-based systems struggle to keep pace with these evolving patterns, leading to missed detections and security breaches [7], [8], [9].

Neural networks are a promising approach to cybersecurity [10], [11], [12], [13], [14]. They are machine learning models capable of being trained to discern patterns within datasets. These models possess the capability to learn and identify patterns within data, rendering them highly effective for tasks such as detecting malicious activities, implementing intrusion detection and prevention systems, and developing sophisticated firewall and encryption algorithms.

Neural networks address the limitations of traditional methods by offering several key advantages [6], [15], [16], [17], [18]:

- They excel at identifying subtle deviations in data, making them adept at detecting zero-day attacks and anomalous behavior indicative of malicious activity, regardless of prior encounters.
- They can learn from extensive datasets, including historical attack data and network traffic, enabling them to refine their threat detection models over time and

The associate editor coordinating the review of this manuscript and approving it for publication was Wanqing Zhao.

adapt to new attack vectors and evolving threat patterns, which is essential in the dynamic cybersecurity area.
- They can discern genuine threats from benign activities, thus reducing false positives and enhancing the efficiency of security systems.

The effectiveness of neural networks has been established across various cybersecurity applications [19], [20], [21], [22], [23], [24]. The use of neural networks in cybersecurity is still in its earlier stages, but the potential benefits are significant.

The application of neural networks in cybersecurity has been the subject of hundreds of published academic papers. Scholars are actively exploring the potential of neural networks in a diverse range of cybersecurity applications, such as detect malware with high accuracy [25], [26], [27], [28], [29], [30], [31], identify phishing [32], [33], [34], block unauthorized access to networks [35], protect data from theft [36], [37], etc. Analyzing existing research to extract important details and identify trends is crucial.

To comprehensively analyze the knowledge landscape surrounding neural networks and cybersecurity, this study employs bibliometric methods and visualization tools. The analysis delves into various aspects, including the total number of publications, their geographic distribution, prominent topics, associated terms, contributing authors, citation patterns, and institutional/regional collaboration networks. Notably, reference co-citation analysis is used to illuminate the foundational concepts, current research hotspots, and future trends within the field.

The main contributions of this paper are:

- We provide a thorough knowledge mapping and in-depth analysis of neural networks in cybersecurity research from 2003 to 2023 by investigating 2018 articles indexed in the Web of Science (WoS), offering a comprehensive understanding of global trends in the field.
- Utilizing CiteSpace 6.2.R7, we conduct various analyses, including collaboration networks, co-citation networks, references with citation bursts, keyword analysis, and cluster analysis. These analyses offer valuable insights into the current state of neural networks in cybersecurity research, highlighting key themes, influential authors, and emerging trends.
- We outline open research challenges and suggest areas for future investigation, aiming researchers toward addressing critical issues and advancing the field.

The structure of the remaining part of the paper is as follows: Section II will discuss relevant research surveys. Section III will provide details on the research methodology employed in this study. Section IV presents the findings of the bibliometric analysis, including insights from reference co-citation clustering, emerging research trends, and highly cited references. Section V presents open research challenges, highlights potential interdisciplinary approaches, and outlines technological developments that could influence future research. The final section provides the conclusions of this study.

II. RELATED WORK

This section delves into the current state-of-the-art research in this domain, highlighting relevant surveys that explore the challenges and opportunities of using neural networks for cybersecurity domain.

Numerous surveys have explored the application of neural networks in cybersecurity, focusing on various issues such as:
- Comparing neural network architectures that can be used for cybersecurity tasks [1], [11], [12], [38], [39], [40].
- Discussing the challenges of implementing neural networks in cybersecurity [1], [38]
- Applying neural networks to various cybersecurity areas [1], [10], [12], [39], [41], [42], [43].

Specifically, Pawlicki et al. [38] and Buczak and Guven [43] examine the challenges and considerations when implementing neural networks in intrusion detection systems (IDS).

Dasgupta et al. provide a broader perspective on machine learning for cybersecurity, encompassing the vulnerabilities of machine learning algorithms to attacks [41]. They offer a fundamental understanding of the security landscape of machine learning in cybersecurity.

Prajoy et al. delve into deep learning approaches for various cybersecurity applications, including malware detection, intrusion detection, and spam filtering [42]. They highlight the importance of large datasets for effective deep learning and the need for secure AI systems. It provides a comprehensive overview of specific applications of neural networks within cybersecurity.

Rodríguez et al. survey is the first complete review of deep learning methods for mobile and wireless network cybersecurity, and identifies the most effective approaches for different security challenges [12].

Berman et al. survey analyzes deep learning methods used in cybersecurity applications [11]. It provides a tutorial-style explanation of various deep-learning techniques and explores how they are used to address security challenges.

However, these surveys do not employ bibliometric methods to analyze research trends and patterns comprehensively. This gap is crucial because understanding the evolution of research, key contributors, and emerging trends can guide future investigations and innovations in the field.

III. RESEARCH METHODOLOGY

A. DATA COLLECTION

This study utilizes the WoS core collection, the world's leading citation database encompassing high-impact journals worldwide, as its primary data source [44]. To obtain publications about neural networks and cybersecurity, the following search term was used on February 7, 2024: Topic = "cybersecurity" or "cyber security" and "neural network." A total of 2070 papers were published in this domain between January 1, 1974, and February 1, 2024. These

include 1,301 articles, 691 proceeding papers, 75 reviews, and 4 others categorized as "others". Analysis suggests 2003 year as the starting point for publication papers activity in this area. To capture this growth, the second search encompassed 20 years, starting from 2003 and extending to 2023, yielding a total of 2018 published papers in the field.

The largest WoS categories of the selected papers in this files are presented in Table 1.

TABLE 1. The WoS categories with the highest number of papers.

Web of Science Categories	Record count	% of 2018
Computer Science Information Systems	850	40.246
Engineering Electrical Electronic	771	36.506
Telecommunications	481	22.775
Computer Science Theory Methods	477	22.585
Computer Science Artificial Intelligence	437	20.691
Computer Science Interdisciplinary Applications	209	9.896
Computer Science Hardware Architecture	166	7.860
Computer Science Software Engineering	164	7.765
Automation Control Systems	132	6.250
Engineering Multidisciplinary	119	5.634

Analyzing the distribution of publications across disciplines reveals the primary research areas and the concentration of expertise within the field of neural network applications in cybersecurity. As Table 1 shows, "Computer Science Information Systems" leads the pack with 850 records, representing 40.246% of the total 2018 publications in this domain. This is followed closely by "Engineering Electrical Electronic" with 771 records (36.506%) and "Telecommunications" with 481 records (22.775%).

B. SCIENTOMETRIC ANALYSIS METHODS

This study employs CiteSpace to visualize and analyze the knowledge structure and development trends in using neural networks for cybersecurity. CiteSpace is citation visualization analysis Java-based software developed by Chen, aiming to identify and summarize transformations or trends within a specific domain [45]. Our choice of CiteSpace is motivated by several factors [45], [46], [47]:

- CiteSpace excels at creating insightful visual representations of the knowledge domain, including co-citation networks and keyword burst charts. This aligns perfectly with our objective to explore the relationships between institutions, keywords, and cited references.
- CiteSpace's strength lies in its ability to generate insightful visual representations of the knowledge domain. These visualizations, including co-citation networks and keyword burst charts, can readily communicate complex relationships and trends.
- CiteSpace allows for time-sliced analysis, enabling us to track the evolution of research foci and collaborations over time. This is crucial for understanding the dynamic nature of research in this field.

In this research, we used version 6.2.R7 Advanced of CiteSpace [48]. Various node types, such as institutions, countries, keywords, references, and cited journals and terms, were chosen individually according to the analytical objectives. For analysis in CiteSpace, the following parameters were employed:

- Time Slices: One-year time slices were selected to provide a granular view of research trends over time. This allows for a more nuanced understanding of how the field has progressed.
- g-index: The g-index parameter was set to 25. The g-index is a metric that considers both the number of publications and their citations. Setting it to 25 ensures we focus on influential publications with a significant impact on the field.
- Top N and TopN%: We set Top N to 50 and TopN% to 10. Top N identifies the top 50 most frequently cited references, institutions, or keywords, while TopN% focuses on the top 10% of terms by citation frequency within a specific slice. This combination ensures we capture both highly influential entities and those experiencing rapid growth in citations.

To identify prominent actors and research foci, we will utilize CiteSpace's relationship graphs. These graphs will visualize interactions between countries, institutions, and frequently cited journals. This allows us to pinpoint leading contributors to the field and identify potential collaborations.

Co-citation network analysis, based on the methodologies developed by Small [49], will be employed to reveal research clusters and emerging trends. Co-citation analysis examines how frequently two publications are cited together. This helps us identify groups of highly interconnected research papers that share a common theme. By analyzing these clusters over time slices, we can track the evolution of research foci within the broader domain of neural networks and cybersecurity.

Furthermore, CiteSpace leverages Kleinberg's algorithm [50] to detect bursts in keyword citations. These bursts highlight entities experiencing an abrupt and significant increase in citations within a short timeframe. By identifying these keywords, we can pinpoint emerging research areas that are gaining rapid traction within the field.

While CiteSpace provides robust tools for research analysis, it's essential to recognize the limitations of the bibliometric approach, largely due to the reliance on WoS database [51], [52], [53], [54]:

- WoS indexes a significant portion of scientific literature, but it doesn't encompass everything. Many relevant journals, books, and conference proceedings may not be included in the database. - CiteSpace analyzes co-citation networks based on citations found in WoS. However, citation practices can be influenced by various factors, such as field-specific citation norms or language barriers. This can skew the analysis towards highly cited works within the WoS database, potentially underrepresenting emerging research areas or publications from under-resourced regions.
- Bibliometric analysis focuses on publications that have already gone through the peer-review process and been published. This inherently excludes ongoing research,

unpublished findings, or grey literature (e.g., technical reports, dissertations).
- Keyword analysis based on titles, abstracts, and article descriptions can provide a general understanding of research foci. However, it may miss the full depth and subtleties explored within the body of the research itself. Additionally, keyword analysis based on titles and abstracts excludes important information contained in books and deeper sections of articles.

IV. RESULTS AND DISCUSSIONS

A. PUBLICATIONS BY YEAR

As shown in the Figure 1, the number of citations and publications related to this field has steadily increased from 2003 to 2023, reflecting its growing importance.

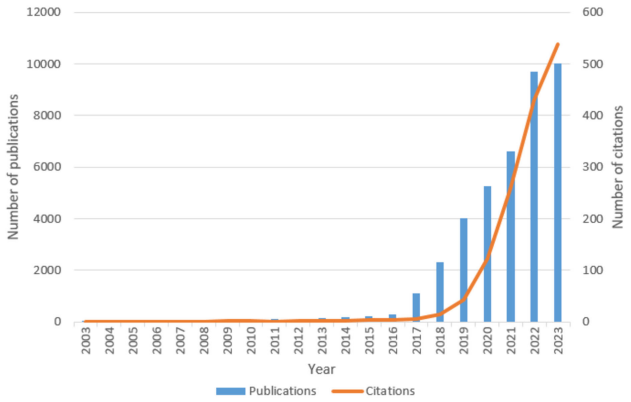

FIGURE 1. Number of citations and publications in the field of neural networks for cybersecurity from 2003 to 2023.

Figure 1 highlights a remarkable surge in publications concerning neural networks and cybersecurity, escalating from merely 3 articles in 2003 to 501 in 2023 – a 167-fold increase over two decades. This exponential growth, particularly pronounced after 2016, suggests a rapidly maturing field attracting significant interest. The year 2017 appears as a tipping point, demonstrating a sharp increase from 56 to 116 publications compared to the preceding year. While growth persists since then, the pace exhibits a degree of stabilization, potentially indicating a maturing research landscape.

Regarding the number of citations, it can be segmented into two distinct stages. The initial stage spans from 2003 to 2016, characterized by a relatively low number of citations. The subsequent stage demonstrates a notable upward trend, particularly from 2017 to 2023, marked by an exponential increase in citations. This growth culminates in a peak of 10,779 citations in 2023.

Several factors that contribute to this substantial growth:
- Escalating cybercrime: The relentless rise of cybercrime fuels the demand for effective defensive mechanisms. Neural networks, with their impressive learning and pattern recognition capabilities, emerge as a promising tool to address this challenge [38], [55], [56], [57], [58], [59].
- Technological advancements: Rapid advancements in artificial intelligence and machine learning, intertwined with neural network developments, propel interest in their application to cybersecurity [17], [60], [61], [62]. Increased sophistication and efficacy of these technologies further bolster their potential in this domain.
- Boosted investment: Growing awareness of the criticality of cybersecurity has led to increased investments in research and development [63], [64]. This surge in funding translates to additional resources for researchers, fostering exploration within this field and contributing to the publication boom.
- Heightened awareness: Enhanced public and organizational awareness regarding cyber threats fuels the demand for robust cybersecurity solutions [40], [65], [66]. This demand, in turn, drives research efforts and bolsters the number of publications in this rapidly evolving field.

B. KEY JOURNALS DRIVING RESEARCH TRENDS

In CiteSpace, the node type ''Cited Journal'' was chosen to identify the most influential journals in the field of neural networks for cybersecurity. As illustrated in Figure 2, this analysis yielded 999 nodes representing journals, with 6,422 connections (rows) and a density of 0.0129, indicating a relatively sparse network. The color bar legend in the lower left corner indicates the publication date of visualized items. Yellow shades represent more recent works, while older publications are represented by cooler colors. Additionally, journals experiencing citation bursts are highlighted with red rings. The top five most cited journals are ''IEEE Access,'' ''Lecture Notes in Computer Science,'' ''Computers & Security,'' ''IEEE Transactions on Industrial Informatics'' and ''IEEE Internet of Things Journal'' (Table 2). IEEE Access emerges as the most highly cited journal in this domain, accumulating a total of 1072 citations and demonstrating significant influence and impact. Additionally, a highly influential article from the arXiv.org preprint repository has garnered 595 citations, highlighting the potential contribution of preprints in this field.

C. THE MAJOR COUNTRIES AND INSTITUTIONS

The Figure 3 depicts a collaboration network among countries actively contributing to research in neural networks for cybersecurity. The analysis identifies researchers from 99 countries engaged in this field. The size of the circles represents the citation rate of each country's representatives (detailed citation counts are provided in Table 2). As illustrated in Figure 3, the size of the circles corresponds to the citation rate of each country. Accordingly, the top five most cited works originated from the United States (434 citations), China (415 citations), India (252 citations), Saudi Arabia (201 citations), and Australia (114 citations).

From 2003 to 2023, a total of 365 institutions have contributed to research in neural networks for cybersecurity,

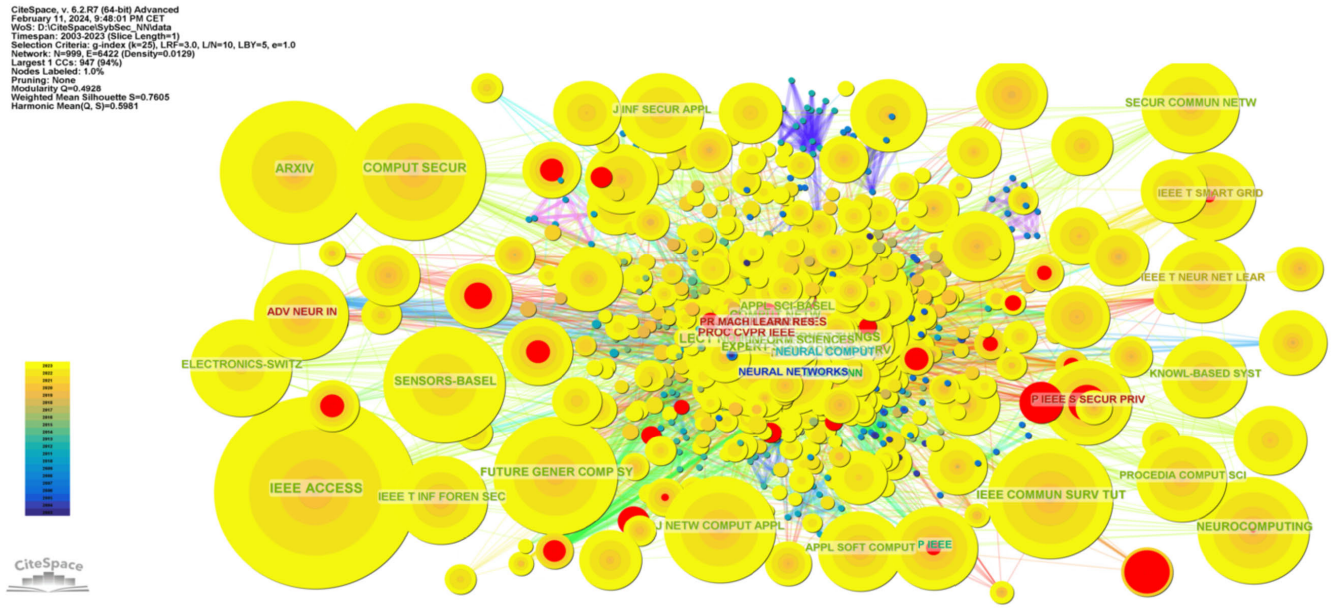

FIGURE 2. The cited journals cooperation network.

TABLE 2. Top countries, institutions and journals.

Rank	Countries	Number of Published Articles	Institutions	Number of Published Articles	Journals	Number of co-Citation Frequency
1	United States	434	Egyptian Knowledge Bank	49	IEEE Access	1072
2	China	415	University of Texas System	39	Lecture Notes in Computer Science	666
3	India	252	Chinese Academy of Sciences	37	arXiv.org	595
4	Saudi Arabia	201	King Abdulaziz University	31	Computers & Security	565
5	Australia	114	State University System of Florida	28	IEEE Transactions on Industrial Informatics	447
6	England	110	University of Texas at San Antonio	26	IEEE Internet of Things Journal	436
7	Canada	105	National Institutes of Technology	26	IEEE Communications Surveys & Tutorials	434
8	Pakistan	80	Princess Nourah bint Abdulrahman University	25	Future Generation Computer Systems	421
9	Republic of Korea	59	Prince Sattam bin Abdulaziz University	24	Sensors (Basel)	399
10	Italy	55	King Khalid University	23	Expert Systems with Applications	367

with a mapping density of 0.0095. This density suggests that the connections between institutions are not particularly close, indicating a low degree of cooperation, with institutions operating largely independently (Figure 4). The top five institutions in terms of publication output are the Egyptian Knowledge Bank (49), the University of Texas System (39), the Chinese Academy of Sciences (37), King Abdulaziz University (31), and the State University System of Florida (28).

D. MAPPING AND ANALYSIS OF AUTHORS

The results showed that 457 authors participated in 2018 articles in the WoS database. Figure 5 shows the author co-occurrence map. Al-wesabi, Fahd N and Hilal, Anwer Mustafa are the core authors in the field of neural networks for cybersecurity, and many other authors form a more extensive collaborative network with them. Interestingly, these authors have joint publications, and their article [67] in which proposed a novel AI-enabled multimodal fusion-based intrusion detection system for cognitive cyber-physical systems in Industry 4.0, is significant not only for its potential advancements in the field but also for its contribution to the body of knowledge through its citations and content.

Table 3 presents the top 10 authors with the highest number of publications, along with their affiliations, countries, and the year of their first publication. Table 3 reveals that four authors from Saudi Arabia have a significant number of publications. Vinayakumar Ravi has contributed 19 articles, with his first publication dating back to 2017. Based on the volume of published articles, he appears to possess

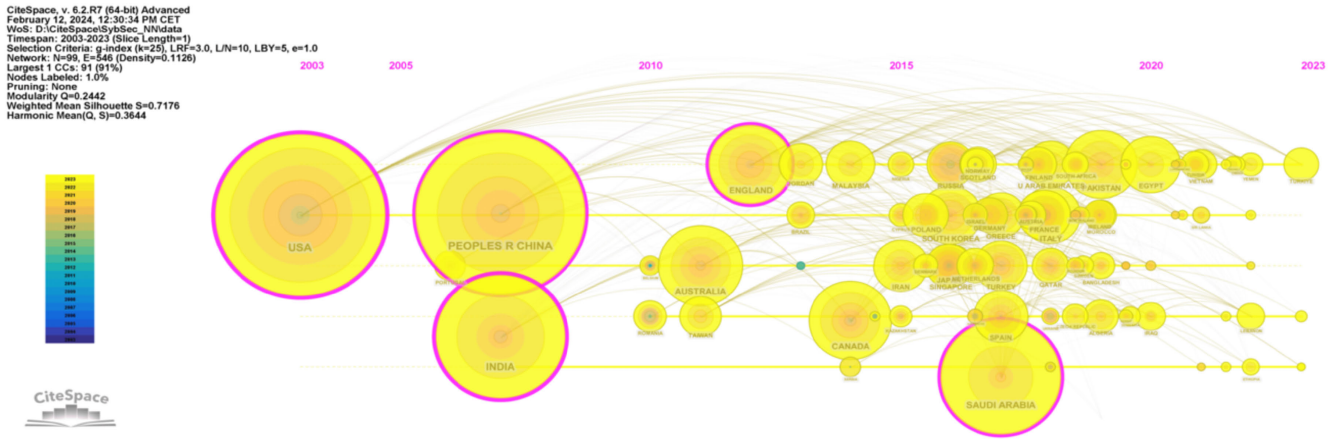

FIGURE 3. The cooperation network between countries.

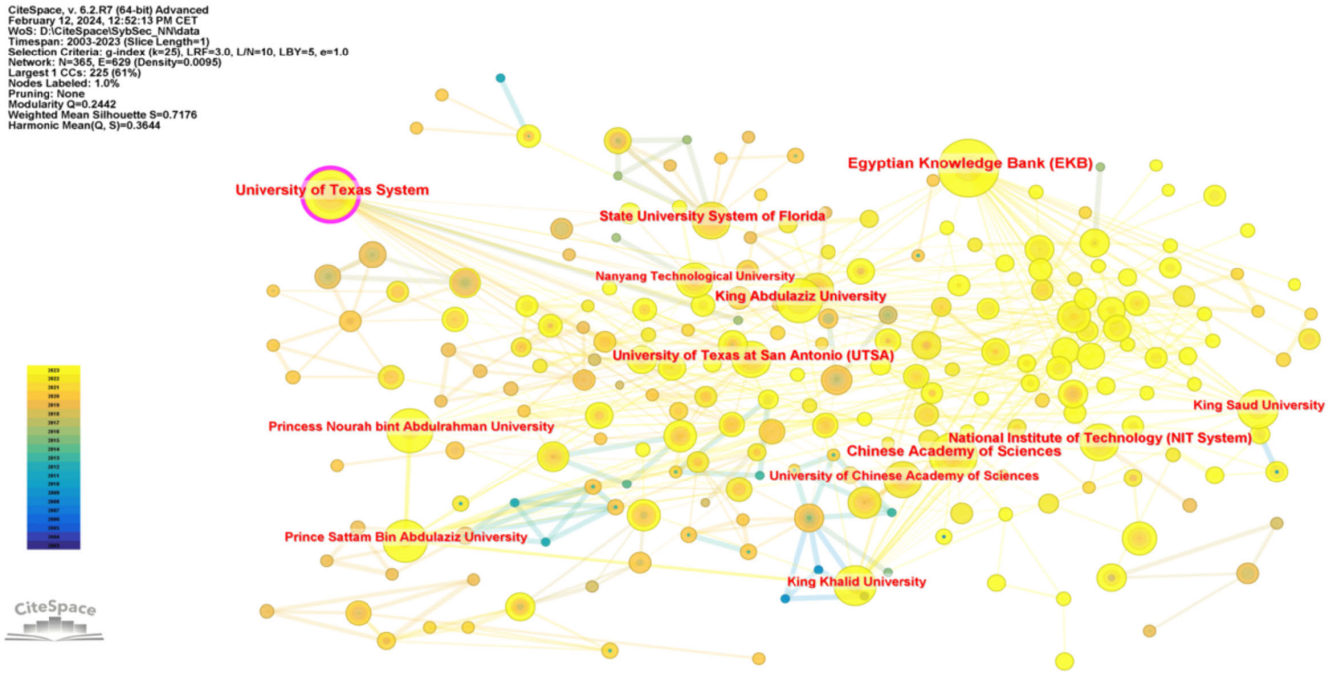

FIGURE 4. The institutional cooperation network.

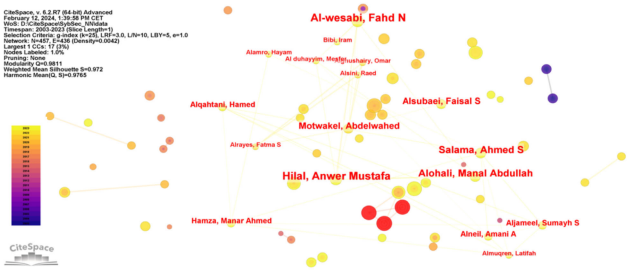

FIGURE 5. Author co-occurrence map.

extensive research experience in this field. Following closely, Poornachandran, Prabaharan, and Soman, K. P. rank second with 10 publications each, also beginning their contributions in 2017.

Table 4 presents the top 10 authors with the highest number of cited references, along with their affiliations, countries, and the year of their first publication.

E. KEYWORDS CO-OCCURRENCE ANALYSIS

To understand key research themes, we built a network based on the most frequent keywords. Each node represents a keyword, and the connecting lines show how often these keywords appear together in research papers. (Figure 6). Node size reflects keyword frequency, and line thickness indicates co-occurrence strength.

Figure 6 illustrates that the node representing ''deep learning'' is the most prominent in the network, appearing 531 times, followed by ''machine learning'' with 382 occurrences. ''Intrusion detection'' is observed 282 times, while

TABLE 3. Top 10 authors with the largest number of articles.

#	Author	Organization	Country	Publications	First published time
1	Vinayakumar, Ravi	Prince Mohammad Bin Fahd University	Saudi Arabia	19	2017
2	Poornachandran, Prabaharan	Amrita University	India	10	2017
3	Soman, K. P.	Amrita University	India	10	2017
4	Choo, Kim-Kwang Raymond	University of Texas System	USA	9	2019
5	Alazab, Mamoun	Charles Darwin University	Australia	8	2019
6	Ahmad, Jawad	University of Texas System	USA	8	2021
7	Aldhyani, Theyazn HH	King Faisal University	Saudi Arabia	8	2022
8	Al-wesabi, Fahd N	King Khalid University	Saudi Arabia	6	2022
9	Hilal, Anwer Mustafa	Prince Sattam Bin Abdulaziz University	Saudi Arabia	6	2022
10	Moustafa, Nour	University of New South Wales	Australia	6	2021

TABLE 4. Top 10 authors with the most cited references.

#	Author	Organization	Country	Citation Counts	First published time
1	Moustafa, Nour	University of New South Wales	Australia	199	2017
2	Hochreiter, Sepp	Technical University of Munich	Germany	177	2017
3	Vinayakumar, Ravi	Prince Mohammad Bin Fahd University	Saudi Arabia	172	2018
4	LeCun, Yann	New York University	USA	160	2017
5	Tavallaee, Mahbod	University of New Brunswick	Canada	146	2017
6	Goodfellow, Ian	Google Brain	USA	146	2017
7	Kingma, Diederik P.	Google Brain	USA	140	2017
8	Liu, Yang	Anhui University	China	126	2016
9	Wang, Wei	Huaqiao University	China	124	2019
10	Sharafaldin, Iman	Canadian Institute for Cybersecurity	Canada	123	2019

"cybersecurity" appears 249 times. Additionally, other keywords such as "neural networks," "internet," "algorithm," "optimization," "big data," and "internet of things" also demonstrate frequent occurrences.

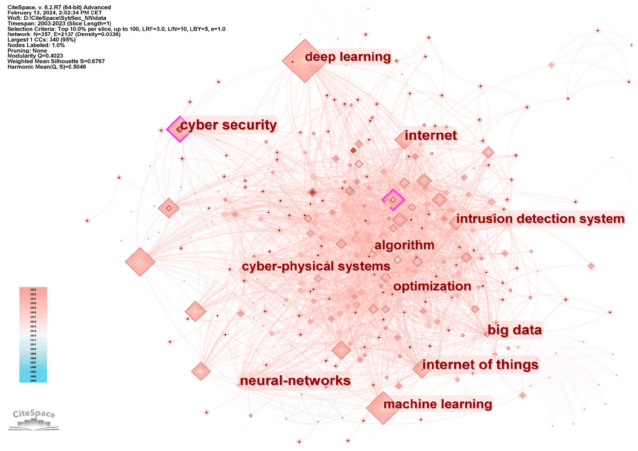

FIGURE 6. Network of keywords, output of the co-occurrence analysis.

Figure 7 presents the top ten keywords with the strongest citation bursts. The keyword "cybersecurity" exhibited the strongest citation burst, spanning from 2010 to 2019. Following closely, "data mining" experienced a burst starting in 2011 and concluding in 2020. Synonyms such as "neural networks" and "neural network" began to surge in 2015. "Deep neural networks," "big data," and "multi-cloud platforms" showed bursts in 2018. More recent burst keywords signify emerging research areas, including "smart cities" and "feature extraction."

Top 10 Keywords with the Strongest Citation Bursts

Keywords	Year	Strength	Begin	End	2003 - 2023
cyber security	2010	19.73	2010	2019	
data mining	2011	4.32	2011	2020	
neural networks	2013	5.43	2015	2019	
neural network	2013	9.06	2016	2018	
deep neural networks	2018	5.88	2018	2020	
big data	2015	4.38	2018	2019	
multi-cloud platforms	2018	3.28	2018	2018	
deep neural network	2019	3.46	2019	2019	
smart cities	2021	5.22	2021	2021	
feature extraction	2019	3.1	2021	2021	

FIGURE 7. Top keywords with the strongest citation bursts.

F. TERMS ANALYSIS

Figure 8 identifies the most important terms from the publication's abstracts. By analyzing the timeline on the graph, we can identify the specific points in time when these terms experienced a significant increase in their usage. As a result of clusterization, we have gotten the main 11 clusters to be analyzed.

Similar to how citation bursts signal increased scientific interest in a particular article, burst detection can also identify terms experiencing explosive growth in their usage, acting as indicators of emerging research trends. The top 30 keywords exhibiting the strongest such bursts during the period 2003-2021 are visualized in Figure 9. The strongest ones include artificial neural networks, increasing incidents, and cyber-attacks. During the years 2017-2018, there was

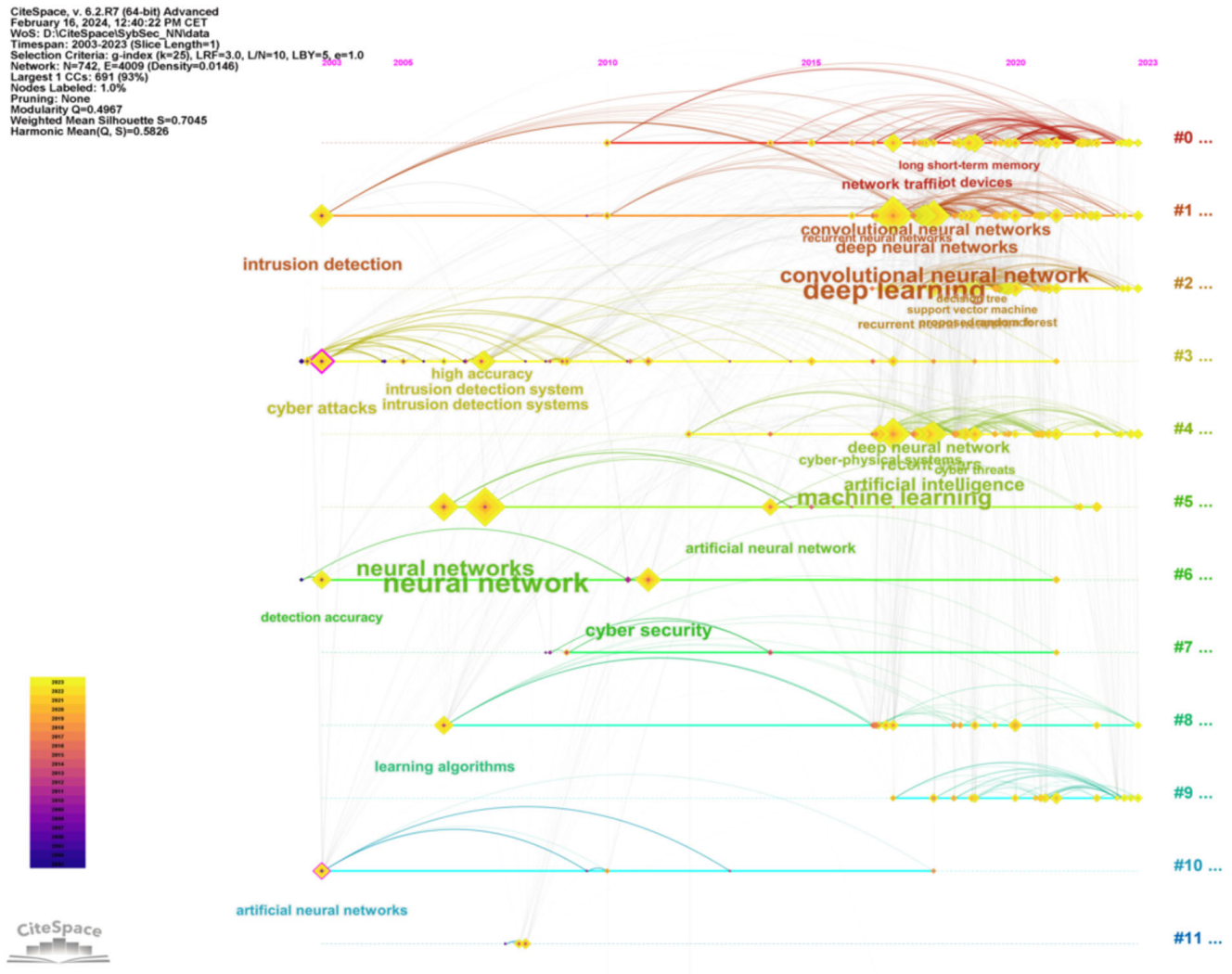

FIGURE 8. The temporal network view of term clusters.

a notable surge in the emergence of numerous keywords. Subsequently surged keywords include cyber security, big data, deep neural networks, recurrent neural networks, learning algorithms, etc.

As it follows from Figure 8, starting at early 2000th from applying multilayer perceptron to intrusion detection and cyberattacks, the extent has been shifted to deep learning problems with the models involving convolution neural networks and recurrent neural networks such as long-short term memory by 2015.

G. RESEARCH HOTSPOT ANALYSIS

To identify research hotspots in the field of neural networks for cybersecurity, CiteSpace was employed to generate co-citation networks and analyze reference citation bursts. The results are presented in three figures: Figure 10 depicts the cluster view of the network, Figure 11 illustrates the time-based view, and Figure 12 showcases reference citation bursts.

Figure 10 depicts the co-citation network, consisting of 842 nodes and 3327 connections, clustered into nine distinct categories: industrial internet (#0), network intrusion detection system (#1), anomaly-based intrusion detection (#2), effective malware classification (#3), industrial control systems (#4), smart grid (#5), convolutional neural network (#6), phishing detection (#8), and software vulnerability detection (#13). These categories are labeled based on their log-likelihood ratios (LLR) for optimal representation [68].

Each cluster visualizes individual publications as dots, with the most prominent publications labeled directly within the diagram.

Table 5 presents 9 clusters, organized by size, where larger sizes indicate more cited references within the cluster, reflecting its influence. Silhouette scores gauge cluster quality, with higher scores indicating greater homogeneity [69]. All clusters exhibit high credibility scores, with clusters #6, #8, and #13 achieving the highest Silhouette scores. Reflecting their recency, Cluster #0 features the most recent publications, averaging 2019. Conversely, clusters #8 and #13

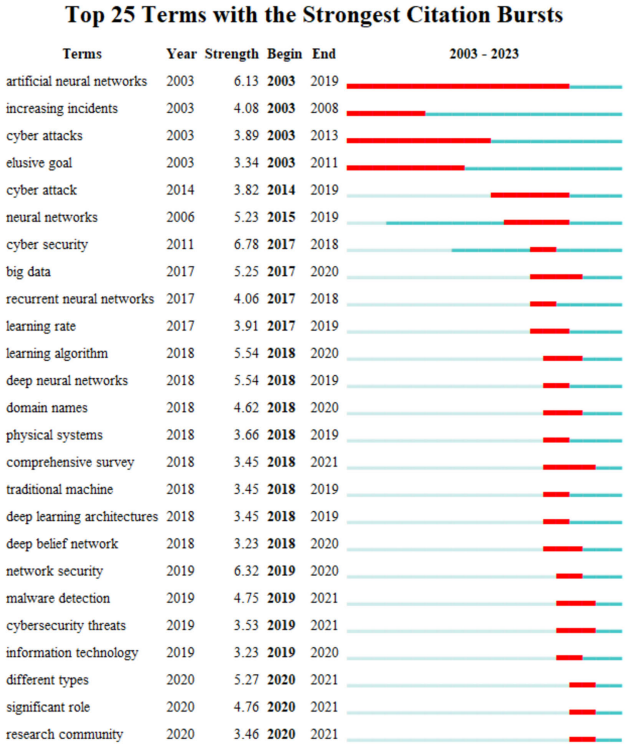

FIGURE 9. Top terms with the strongest citation bursts.

represent the least recent publications, averaging 2018 and 2017, respectively.

Figure 11 identifies the most influential publications within the timeframe, represented by red circles. These publications have the highest count of cited terms extracted from their bibliographic records. The graph's timeline allows you to pinpoint the specific years when these highly influential publications emerged.

A thorough analysis presented in Figure 12, considering both burst value (citation intensity) and burst duration, helps pinpoint emerging research trends shaping the field. The earliest identified citation burst references stem from the work of Srivastava et al. [70] and Kingma and Ba [71], which were published in 2014 and burst in 2017. This references attracted academic attention from 2017 to 2019. While 2017 witnessed the most intense surges in research interest for this field, He et al.'s 2016 paper [72] stands out as the only exception from the top 10 list, experiencing a burst in 2020. Two references, Goodfellow et al. [73] and Buczak and Guven [43], experienced a burst in 2017, which persisted until 2021, indicating their emergence as significant trends in the field. Additionally, the reference authored by Srivastava et al. [70] attained the highest strength value of 15.44 and has garnered 22,766 citations on Web of Science. This reference discusses techniques for enhancing neural networks by mitigating overfitting.

This analysis delves into three key clusters within the co-citation network, namely #0, #1, and #2. It specifically examines the cited references and citing articles associated with each cluster to gain insights into the research themes and interconnections within these distinct areas.

1) CLUSTER #0 - INDUSTRIAL INTERNET

Cluster #0 emerges as the largest cluster within the network, encompassing 129 references. Its silhouette value of 0.671 indicates a good level of cohesion within the cluster, suggesting strong thematic connections between the included references. The core references of this cluster revolves around using adaptive learning approaches to classify and identify malicious network traffic, particularly at the network edge [74], [75], [76], [77], [78]. This is critical due to the rapid growth of digital services and IoT devices, leading to diverse and evolving cyber threats that traditional methods struggle with. The key challenge highlighted in the articles is the sensitivity of existing solutions to subtle changes in network traffic features, resulting in misclassifications [79], [80], [81]. The cluster to explore the use of intrusion detection, which utilizes neural model for optimal separation of traffic samples belonging to different classes [82], [83]. Table 6 lists the most cited references and citing articles within Cluster #0 industrial internet.

The most cited reference within this cluster is by Koroniotis et al. [75], cited 545 times on WoS. This study proposes a novel dataset called Bot-IoT, containing both real and simulated IoT network data along with various attack scenarios. It also introduces a practical testing environment to address limitations in existing datasets, such as incomplete data capture, inaccurate labeling, and lack of representation for recent and complex attack patterns.

The second most cited reference is by Diro and Chilamkurti [76], cited 448 times on WoS. This work proposes a novel approach to exploring deep learning applications in cybersecurity, specifically focusing on social Internet of Things attack detection.

Three other highly cited references are surveys by Berman et al. [11], Meidan et al. [86], and Al-Garadi et al. [78].

Berman et al. comprehensively examine deep learning techniques for various cybersecurity applications like malware detection, spam filtering, and intrusion prevention [11].

Meidan et al. introduce a novel network-based anomaly detection method using deep autoencoders to address the growing threat of IoT-based botnet attacks [86]. Their method effectively identifies malicious traffic and showcases potential for improved IoT cybersecurity.

Al-Garadi et al. explore the application of machine learning and deep learning techniques for enhancing security in the expanding IoT landscape [78]. They delve into potential threats, attack surfaces, and ML/DL-based solutions, highlighting the opportunities and challenges in this emerging field.

These references collectively show how neural networks are shaping industrial IoT security by:

- Providing essential datasets for research and development [75].

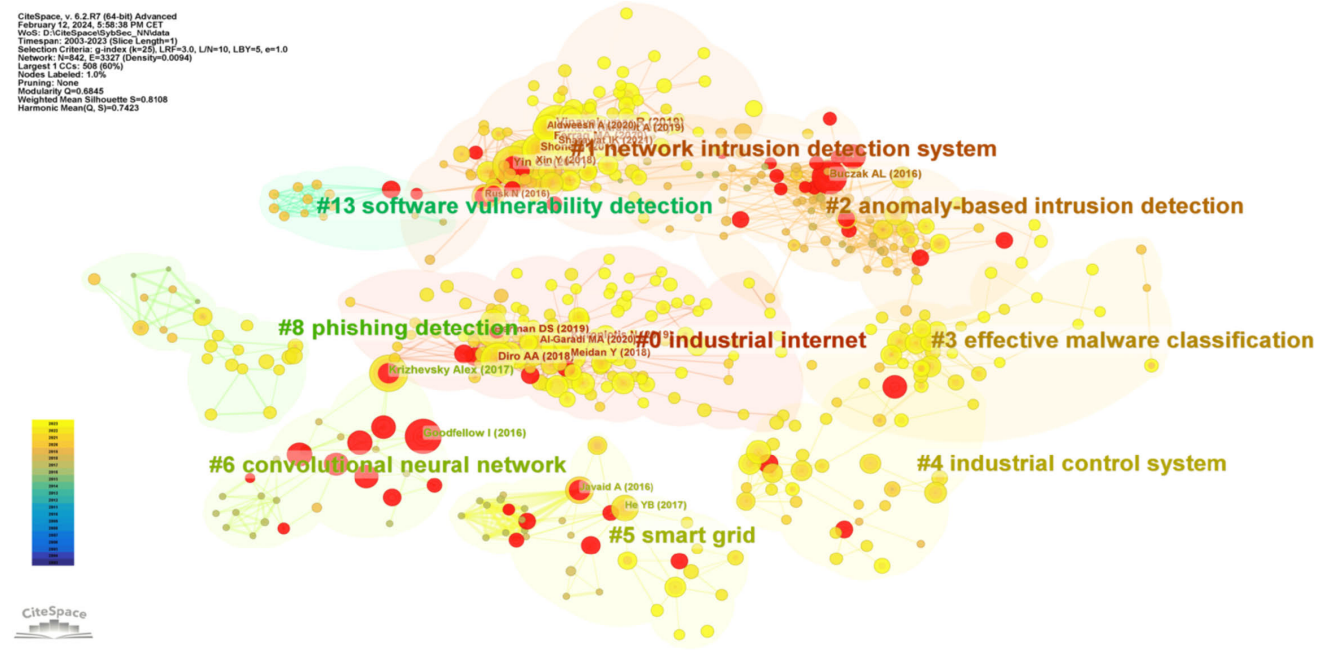

FIGURE 10. Clusters of the co-citation network.

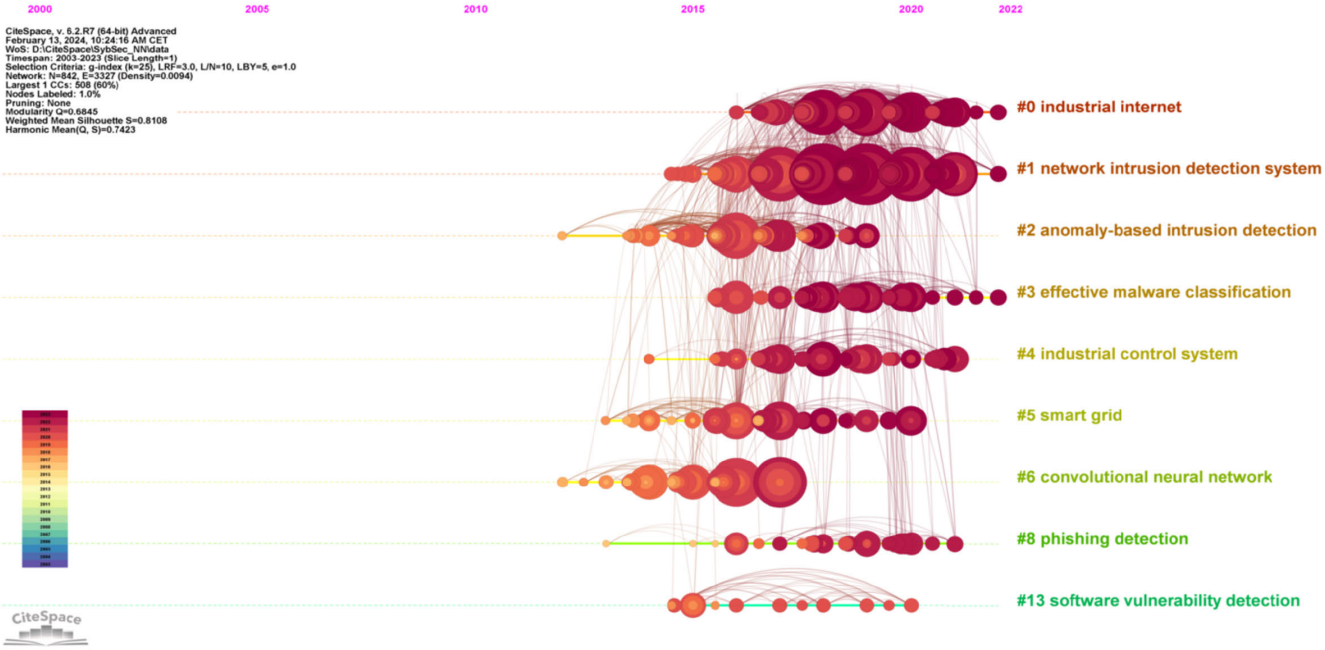

FIGURE 11. The temporal network view of the co-citation clusters.

- Exploring applications in specific IoT attack domains [76].
- Highlighting the broader role of neural networks in industrial IoT cybersecurity [11], [78], [86].

Their combined influence positions neural networks as a promising approach for securing industrial IoT networks and mitigating evolving threats in this critical infrastructure domain.

The citing articles authored by Muna et al. [74], Diro and Chilamkurti [76], Mirsky et al. [79], Alkadi et al. [80], and Alsaedi et al. [82] represent research fronts within Cluster #0.

2) CLUSTER #1 - NETWORK INTRUSION DETECTION SYSTEM

The second-largest cluster, #1, comprises 110 references with a silhouette value of 0.806. It delves into the realm of

TABLE 5. Summary of cluster analysis results.

Cluster ID	Size	Silhouette	Label (LSI)	Label (LLR)	Label (MI)	Average Year
0	129	0.671	iot network	industrial internet (427.58, 1.0E-4)	false data cyber-attack (2.25)	2019
1	110	0.806	intrusion detection system	network intrusion detection system (469.67, 1.0E-4)	false data cyber-attack (3.5)	2018
2	93	0.76	deep learning	anomaly-based intrusion detection (282.4, 1.0E-4)	false data cyber-attack (0.78)	2016
3	36	0.929	effective malware classification	effective malware classification (413.31, 1.0E-4)	false data cyber-attack (0.3)	2018
4	35	0.934	industrial control system	industrial control system (582.12, 1.0E-4)	physical network data (0.41)	2018
5	35	0.916	smart grid	smart grid (649.64, 1.0E-4)	false data cyber-attack (0.37)	2016
6	27	0.968	deep learning	convolutional neural network (240.5, 1.0E-4)	detecting domain generation algorithm (0.58)	2014
8	24	0.947	deep learning	phishing detection (322.03, 1.0E-4)	self-protected virtual sensor network (0.06)	2018
13	13	0.993	software vulnerability detection	software vulnerability detection (84.9, 1.0E-4)	deep learning (0.02)	2017

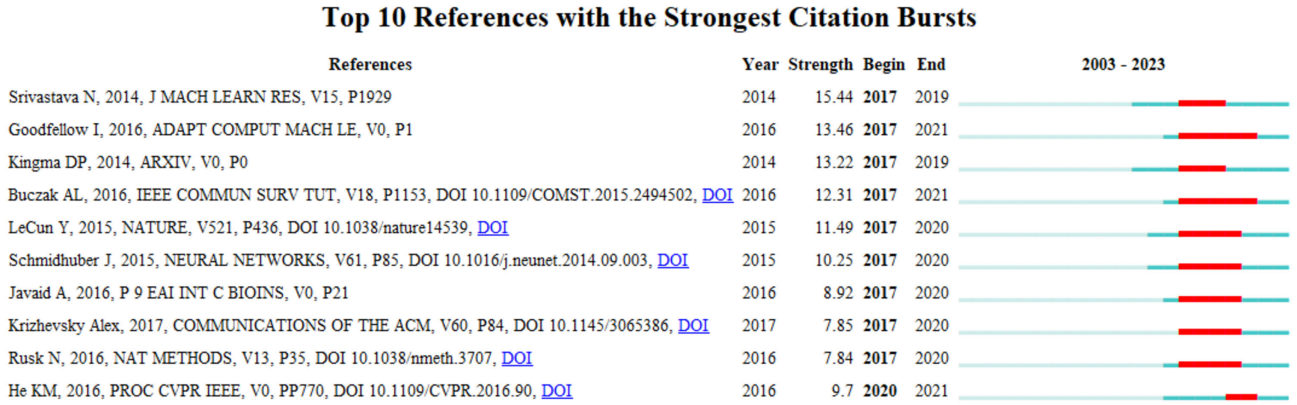

FIGURE 12. Top references with the strongest citation burst.

TABLE 6. References cited and articles citing in the Cluster #0 industrial internet.

Cited references	Citing articles
Koroniotis N, 2019, FUTURE GENER COMP SY, V100, P779, DOI 10.1016/j.future.2019.05.041 [75]	Rodriguez E, 2021, IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, V23, P36 DOI 10.1109/COMST.2021.3086296 [12]
Diro AA, 2018, FUTURE GENER COMP SY, V82, P761, DOI 10.1016/j.future.2017.08.043 [76]	Macas M, 2022, COMPUTER NETWORKS, DOI 10.1016/j.comnet.2022.109032 [84]
Berman DS, 2019, INFORMATION, V10, P0, DOI 10.3390/info10040122 [11]	Tsimenidis S, 2022, JOURNAL OF NETWORK AND SYSTEMS MANAGEMENT, DOI 10.1007/s10922-021-09621-9 [85]
Meidan Y, 2018, IEEE PERVAS COMPUT, V17, P12, 10.1109/MPRV.2018.03367731 [86]	Shaukat K, 2020, IEEE ACCESS, DOI 10.1109/ACCESS.2020.3041951 [1]
Al-Garadi MA, 2020, IEEE COMMUN SURV TUT, V22, P1646, 10.1109/COMST.2020.2988293 [78]	Lee S, 2021, JOURNAL OF NETWORK AND COMPUTER APPLICATIONS DOI 10.1016/j.jnca.2021.103111 [87]

network intrusion detection system (NIDS), leveraging neural networks to effectively identify and categorize various forms of network attacks. Table 7 lists the most cited references and citing articles within this cluster.

TABLE 7. References cited and articles citing in the #1 network intrusion detection system.

Cited references	Citing articles
Sharafaldin I, 2018, ICISSP: PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS SECURITY AND PRIVACY, V0, PP108, DOI 10.5220/0006639801080116 [88]	Gamage S, 2020, JOURNAL OF NETWORK AND COMPUTER APPLICATIONS, DOI 10.1016/j.jnca.2020.102767 [89]
Vinayakumar R, 2019, IEEE ACCESS, V7, P41525, DOI 10.1109/ACCESS.2019.2895334 [90]	Shaukat K, 2020, IEEE ACCESS, DOI 10.1109/ACCESS.2020.3041951 [1]
Yin CL, 2017, IEEE ACCESS, V5, P21954, DOI 10.1109/ACCESS.2017.2762418 [91]	Pawlicki M, 2022, NEUROCOMPUTING, V500, P13, DOI 10.1016/j.neucom.2022.06.002 [38]
Ferrag MA, 2020, J INF SECUR APPL, V50, P0, 10.1016/j.jisa.2019.102419 [92]	Capuano N, 2022, IEEE ACCESS, V10, P26, DOI 10.1109/ACCESS.2022.3204171 [10]
Shone N, 2018, IEEE TETCI, V2, P41, 10.1109/TETCI.2017.2772792 [93]	Tariq MI, 2020, MOBILE INFORMATION SYSTEMS, DOI 10.1155/2020/6535834 [94]

The most cited reference within this cluster, authored by Sharafaldin et al. [88], has been cited 545 times on WoS. The study assesses how well a wide array of network traffic features and machine learning algorithms perform, aiming to identify the most effective features for detecting specific attack categories.

The second most cited reference within Cluster #1 belongs to Vinayakumar et al., which explores the use of deep neural networks for IDS and proposed a framework to effectively monitor the network traffic and host-level events to proactively alert possible cyberattacks [90].

Yin et al. propose a deep learning approach for intrusion detection using recurrent neural networks [91]. The authors examine the model's performance in both binary and multiclass classification and analyze the impact of varying the number of neurons and different learning rates on the model's effectiveness.

Ferrag et al. survey deep learning approaches for intrusion detection in cybersecurity [92]. They review various deep learning models, such as recurrent neural networks and convolutional neural networks, and analyze their performance in binary and multiclass classification tasks using two real-world datasets (CSE-CIC-IDS2018 and Bot-IoT). Additionally, the study explores 35 cybersecurity datasets categorized by data type (network traffic, IoT traffic, etc.).

Shone et al. introduce a novel deep learning-based intrusion detection system using non-symmetric deep autoencoders for unsupervised feature learning and stacked network intrusion detection systems for classification, demonstrating promising results on benchmark datasets [93].

These articles collectively advanced the field by:

- Highlighting the importance of feature selection for effective neural network-based NIDS [88].
- Proposing new deep learning architectures and frameworks for NIDS [90], [91], [93].
- Surveying and comparing existing deep learning approaches for NIDS [92].

Notable contributions include studies by Gamage and Samarabandu [89], Shaukat et al. [1], Pawlicki et al. [38], Capuano et al. [10], and Tariq et al. [94].

The most cited reference in Cluster #1 show that neural networks have emerged as a promising approach for NIDS due to their ability to learn complex patterns in network traffic data.

3) CLUSTER #2 - ANOMALY-BASED INTRUSION DETECTION

There are 93 references cited in Cluster #2. Anomaly detection systems (ADS) have become increasingly important in various fields to identify and react to unusual, potentially harmful events. Overall, neural network-based ADS represent a promising direction for the field, offering significant potential for enhancing security and anomaly detection across diverse domains.

Table 8 presents the top five most cited references and citing articles within Cluster #2.

TABLE 8. References cited and articles citing in the Cluster #2 anomaly-based intrusion detection.

Cited references	Citing articles
Buczak AL, 2016, IEEE COMMUN SURV TUT, V18, P1153, DOI 10.1109/COMST.2015.2494502 [43]	Berman DS, 2019, INFORMATION, DOI 10.3390/info10040122 [11]
Kolias C, 2017, COMPUTER, V50, P80, DOI 10.1109/MC.2017.201 [95]	Mandavifar S, 2019, NEUROCOMPUTING, V347, P28, DOI 10.1016/j.neucom.2019.02.056 [96]
Moustafa N, 2016, INF SECUR J, V25, P18, DOI 10.1080/19393555.2015.1125974 [97]	Alom MZ, 2019, ELECTRONICS, DOI 10.3390/electronics8030292 [98]
Carlini N, 2017, P IEEE S SECUR PRIV, V0, PP39, 10.1109/SP.2017.49 [99]	Qiu J, 2021, ACM COMPUTING SURVEYS, DOI 10.1145/3417978 [100]
Papernot N, 2016, 1ST IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY, V0, PP372, 10.1109/EuroSP.2016.36 [101]	Shaukat K, IEEE ACCESS, DOI 10.1109/ACCESS.2020.3041951 [1]

The most frequently cited reference in Cluster #2 belongs to Buczak and Guven [43]. This review paper provides a comprehensive survey of machine learning and data mining techniques utilized in cyber analytics for intrusion detection.

The second most cited reference, authored by Kolias et al. [95], investigates the emerging threat of DDoS attacks launched using IoT devices, specifically focusing on the infamous Mirai botnet responsible for large-scale DDoS attacks in 2016.

Other highly cited references include works by Moustafa and Slay [97], Carlini and Wagner [99], and Papernot et al. [101].

The paper [97] addresses the limitations of existing benchmark datasets for NIDS evaluation and introduces the UNSW-NB15 dataset, which features modern attack scenarios, realistic normal traffic, and a balanced distribution of training and testing data. It also analyzes the complexity of UNSW-NB15 and demonstrates its superiority over KDD99, making it a valuable benchmark for evaluating NIDS performance.

The paper [99] challenges the effectiveness of defensive distillation, a method for enhancing neural network robustness against adversarial attacks. The authors introduce powerful attack algorithms that successfully fool both distilled and undistilled networks, highlighting the limitations of defensive distillation and setting a benchmark for future research in adversarial robustness.

Papernot et al. paper explores the vulnerability of deep learning models to adversarial samples - crafted inputs designed to cause misclassification [101]. They propose a novel method for generating such samples, achieving a 97% success rate in a computer vision task while modifying only a small portion of the input data. The work also introduces a ''hardness measure'' to assess the difficulty of attacking different types of samples and lays the groundwork for potential defenses based on distance metrics.

TABLE 9. Open research challenges, potential interdisciplinary approaches, and technological developments influencing future research.

Cluster ID	Open research challenges	Potential interdisciplinary approaches	Technological developments influencing future research
#0	- Identifying robust strategies to mitigate the impact of network traffic fluctuations on data classification. - Developing neural network architectures capable of continual learning and adaptation to evolving cyber threats. - Developing efficient countermeasures to protect machine learning-based IoT device identification from being undermined by adversarial attacks and threats. - Developing dynamic and up-to-date security measures to secure IoT systems focusing on addressing the heterogeneity of IoT networks and the quantity of devices that need to be secured. - Developing resilient and privacy-conscious neural network-based solutions for anomaly detection in industrial internet environments.	- Cyber-physical systems and industrial control. - Machine learning and data science. - Behavioral analysis and psychology.	- Advancements in edge computing will enable real-time anomaly detection and threat mitigation at the network edge, closer to data sources, improving efficiency and reducing response times. - Explainable AI techniques can help interpret the decision-making process of neural networks used for anomaly detection, leading to greater trust and transparency in security solutions. - Quantum computing has the potential to revolutionize anomaly detection by enabling faster and more complex pattern recognition within neural network models.
#1	- Training NIDS to detect evolving attack patterns and maintain their effectiveness in a dynamic threat environment is crucial. - Selecting the optimal configuration, including hyperparameters, for neural networks used in NIDS, is essential to minimize error and enhance performance. - Balancing the computational cost of training neural networks with the need for high detection accuracy is critical for practical NIDS implementations. - Improving the detection precision, particularly for low-frequency attacks, and maintaining stable detection performance amidst fluctuating network traffic.	- Network traffic analysis and neural networks. - Software engineering and neural networks.	- Advancements in network function virtualization and software-defined networking will enable more flexible and scalable deployment of neural network-based NIDS solutions within virtualized network environments. - The increasing availability of high-performance computing resources will allow the training of the more complex neural network models for NIDS, potentially leading to higher detection accuracy and the ability to handle larger datasets. - Neuromorphic computing hardware specifically designed to mimic the human brain has the potential to significantly improve the efficiency of neural network-based NIDS, enabling real-time intrusion detection on high-speed networks.
#2	- Further research is needed on optimization strategies for neural networks in anomaly detection. Additionally, there is required to be explored the applicability of hybrid methods, which combine neural networks with other techniques across various network environments. - Anomaly-based IDSs built on neural networks are susceptible to adversarial attacks, where attackers manipulate data to evade detection. - Many anomaly-based IDSs have been evaluated using outdated datasets that may not accurately reflect the complexities of contemporary network traffic. Research is needed to develop datasets incorporating sophisticated data patterns and low-footprint stealth attacks presented in modern networks.	- Statistical analysis and neural networks - Psychology and neural networks.	- Blockchain technology has the potential to create secure and transparent data repositories for training and sharing neural network models used in anomaly-based intrusion detection, fostering collaboration and improving model performance. - Federated learning techniques can enable training neural network models for anomaly-based intrusion detection on distributed datasets without compromising data privacy. This is crucial for scenarios where sensitive network traffic data cannot be centralized.

Cluster #2 also encompasses research exploring various aspects of DDoS attacks and related security challenges. Notable examples include studies by Ding et al. [102], Vinayakumar et al. [90], Biggio and Roli [103] and Ding et al. [104].

These references collectively show how neural network-based ADS is evolving. Their combined influence highlights the ongoing development of neural networks for more secure and effective ADS systems.

V. OPEN CHALLENGES AND FUTURE DIRECTIONS

Based on the analysis of articles in three key clusters (#0, #1, and #2) in the subsection IV-G Table 9 has been developed. This table presents open research challenges, highlights potential interdisciplinary approaches, and outlines technological developments that could influence future research.

Findings presented in Table 9 underscore the importance of interdisciplinary collaboration and integrating emerging technologies like edge computing, explainable AI, quantum computing, blockchain, and federated learning to address challenges and advance research in neural networks for cybersecurity.

VI. CONCLUSION

This study conducted a comprehensive bibliometric analysis of research related to neural networks for cybersecurity using the WoS publication database from 2003 to 2023. A total of 2,018 relevant articles were obtained and imported into CiteSpace 6.2.R7 Advanced for co-citation network analysis and keyword citation burst detection. This method enabled the exploration of the latest research trends, hotspots, and potential future directions in the field. Additionally, the study identified core journals, key contributing countries, and leading institutions within this research domain.

Firstly, this study analyzes the publication numbers and countries involved. It is found that the number of publications and citations related to neural networks and cybersecurity has been rapidly increasing since 2016, indicating a significant interest among researchers in utilizing neural networks for cybersecurity purposes. A map of collaborations and transnational networks in the field of neural networks for cybersecurity revealed that researchers from 99 countries are actively engaged in this domain. Research output is dominated by the United States, with the highest number of published articles in the field. Based on publication numbers, the United States and China are the leading countries in the field of neural networks for cybersecurity, surpassing other countries by a significant margin. India ranks third with 252 publications, followed by Saudi Arabia, Australia, England, Canada, Pakistan, the Republic of Korea, and Italy.

Secondly, the study examines the most productive authors and institutions. Poornachandran Prabaharan, Soman K. P., and Ravi Vinayakumar have published the most quantities of articles related to neural networks and cybersecurity. Amrita University in India boasts three of the top 10 most productive authors. In turn, four of the top 10 productive institutions are

located in the United States, the remaining ones span diverse locations including Saudi Arabia, Egypt, and China.

Thirdly, the analysis delves into the co-occurrence of keywords, indicating prevalent topics and hotspots in articles concerning neural networks and cybersecurity. Keywords such as ''deep learning'', ''machine learning'', ''intrusion detection'', ''cybersecurity'', and ''neural networks'' were among the most frequently occurring. Additionally, terms like ''internet'', ''algorithm'', ''optimization'', ''big data'', and ''internet of things'' demonstrated frequent co-occurrences with other keywords, suggesting heightened attention in these areas. The keyword ''cybersecurity'' exhibited the strongest citation burst held in 2010. Then ''data mining'' emerged as the next burst keyword, initiated in 2011. Keywords like ''neural networks'', ''neural network'', ''deep neural networks,'' ''big data,'' ''multi-cloud platforms,'' ''smart cities,'' and ''feature extraction'' emerged as prominent research topics, experiencing significant citation bursts within the analyzed timespan.

Fourth, by identifying open research challenges, interdisciplinary approaches, and technological advancements in key clusters, this study underscores the importance of collaboration across disciplines and the integration of emerging technologies like edge computing, explainable AI, quantum computing, blockchain, and federated learning to further the development of the field.

This study is subject to limitations inherent to the data source, WoS. Although our research has access to most indexes in the WoS core collection, it excludes Book Citation Indexes [53]. Additionally, while WoS boasts extensive coverage and high-quality data, it might not be exhaustive or entirely up-to-date. Furthermore, limitations in non-English publication coverage within certain fields [54] could introduce minor biases in our analysis due to relying solely on WoS data.

REFERENCES

[1] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, ''A survey on machine learning techniques for cyber security in the last decade,'' *IEEE Access*, vol. 8, pp. 222310–222354, 2020.
[2] T. Bailey, A. D. Miglio, and W. Richter, ''The rising strategic risks of cyberattacks,'' *McKinsey Quart.*, vol. 2, pp. 17–22, Jan. 2014.
[3] M. Ulsch, *Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks*. Hoboken, NJ, USA: Wiley, 2014.
[4] R. S. Deora and D. Chudasama, ''Brief study of cybercrime on an internet,'' *J. Commun. Eng. Syst.*, vol. 11, no. 1, pp. 1–6, 2021.
[5] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, ''Machine learning and deep learning methods for cybersecurity,'' *IEEE Access*, vol. 6, pp. 35365–35381, 2018.
[6] S. Ali, S. U. Rehman, A. Imran, G. Adeem, Z. Iqbal, and K.-I. Kim, ''Comparative evaluation of AI-based techniques for zero-day attacks detection,'' *Electronics*, vol. 11, no. 23, p. 3934, Nov. 2022.
[7] D. Sykes, A. Grivas, C. Grover, R. Tobin, C. Sudlow, W. Whiteley, A. Mcintosh, H. Whalley, and B. Alex, ''Comparison of rule-based and neural network models for negation detection in radiology reports,'' *Natural Lang. Eng.*, vol. 27, no. 2, pp. 203–224, Mar. 2021.
[8] H. Lai and M. Nissim, ''A survey on automatic generation of figurative language: From rule-based systems to large language models,'' *ACM Comput. Surv.*, vol. 56, no. 10, pp. 1–34, Oct. 2024.
[9] F. Yi, B. Jiang, L. Wang, and J. Wu, ''Cybersecurity named entity recognition using multi-modal ensemble learning,'' *IEEE Access*, vol. 8, pp. 63214–63224, 2020.
[10] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, ''Explainable artificial intelligence in CyberSecurity: A survey,'' *IEEE Access*, vol. 10, pp. 93575–93600, 2022.
[11] D. Berman, A. Buczak, J. Chavis, and C. Corbett, ''A survey of deep learning methods for cyber security,'' *Information*, vol. 10, no. 4, p. 122, Apr. 2019.
[12] E. Rodríguez, B. Otero, N. Gutiérrez, and R. Canal, ''A survey of deep learning techniques for cybersecurity in mobile networks,'' *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1920–1955, 3rd Quart., 2021.
[13] M. Choraś and M. Pawlicki, ''Intrusion detection approach based on optimised artificial neural network,'' *Neurocomputing*, vol. 452, pp. 705–715, Sep. 2021.
[14] E. A. Sukhvinder Singh Dari, ''Neural networks and cyber resilience: Deep insights into AI architectures for robust security framework,'' *J. Electr. Syst.*, vol. 19, no. 3, pp. 78–95, Jan. 2024.
[15] P. Dixit and S. Silakari, ''Deep learning algorithms for cybersecurity applications: A technological and status review,'' *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100317.
[16] C. Yinka-Banjo and O.-A. Ugot, ''A review of generative adversarial networks and its application in cybersecurity,'' *Artif. Intell. Rev.*, vol. 53, no. 3, pp. 1721–1736, Mar. 2020.
[17] I. H. Sarker, ''Deep cybersecurity: A comprehensive overview from neural network and deep learning perspective,'' *Social Netw. Comput. Sci.*, vol. 2, no. 3, p. 154, May 2021.
[18] I. Al-Turaiki and N. Altwaijry, ''A convolutional neural network for improved anomaly-based network intrusion detection,'' *Big Data*, vol. 9, no. 3, pp. 233–252, Jun. 2021.
[19] V. Sundararaj, S. Muthukumar, and R. S. Kumar, ''An optimal cluster formation based energy efficient dynamic scheduling hybrid MAC protocol for heavy traffic load in wireless sensor networks,'' *Comput. Secur.*, vol. 77, pp. 277–288, Aug. 2018.
[20] V. Sundararaj, ''Optimal task assignment in mobile cloud computing by queue based ant-bee algorithm,'' *Wireless Pers. Commun.*, vol. 104, no. 1, pp. 173–197, Jan. 2019.
[21] A. Davis, S. Gill, R. Wong, and S. Tayeb, ''Feature selection for deep neural networks in cyber security applications,'' in *Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS)*, Sep. 2020, pp. 1–7.
[22] M. Alazab and M. Tang, *Deep Learning Applications for Cyber Security*. Cham, Switzerland: Springer, 2019.
[23] V. Ford and A. Siraj, ''Applications of machine learning in cyber security,'' in *Proc. 27th Int. Conf. Comput. Appl. Ind. Eng.*, Oct. 2014, pp. 1–6.
[24] A. Yushko, R. Shevchuk, M. Leszczynska, O. Yashchyk, and T. Yurchyshyn, ''Shielding web application against cyber-attacks using SIEM,'' in *Proc. 13th Int. Conf. Adv. Comput. Inf. Technol. (ACIT)*, Sep. 2023, pp. 393–396.
[25] S. Tobiyama, Y. Yamaguchi, H. Shimada, T. Ikuse, and T. Yagi, ''Malware detection with deep neural network using process behavior,'' in *Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, Jun. 2016, pp. 577–582.
[26] J. Yan, Y. Qi, and Q. Rao, ''Detecting malware with an ensemble method based on deep neural network,'' *Secur. Commun. Netw.*, vol. 2018, pp. 1–16, Jan. 2018.
[27] S. Jha, D. Prashar, H. V. Long, and D. Taniar, ''Recurrent neural network for detecting malware,'' *Comput. Secur.*, vol. 99, Dec. 2020, Art. no. 102037.
[28] R. Alotaibi, I. Al-Turaiki, and F. Alakeel, ''Mitigating email phishing attacks using convolutional neural networks,'' in *Proc. 3rd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Mar. 2020, pp. 1–6.
[29] A. AlEroud and G. Karabatis, ''Bypassing detection of URL-based phishing attacks using generative adversarial deep neural networks,'' in *Proc. 6th Int. Workshop Secur. Privacy Anal.*, Mar. 2020, pp. 53–60.
[30] D. Li, Q. Li, Y. Ye, and S. Xu, ''A framework for enhancing deep neural networks against adversarial malware,'' *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 1, pp. 736–750, Jan. 2021.
[31] S. I. Imtiaz, S. U. Rehman, A. R. Javed, Z. Jalil, X. Liu, and W. S. Alnumay, ''DeepAMD: Detection and identification of Android malware using high-efficient deep artificial neural network,'' *Future Gener. Comput. Syst.*, vol. 115, pp. 844–856, Feb. 2021.
[32] L. Halgaš, I. Agrafiotis, and J. R. Nurse, ''Catching the Phish: Detecting phishing attacks using recurrent neural networks (RNNs),'' in *Proc. 20th Int. Conf. Inf. Secur. Appl.*, Jeju Island, South Korea. Cham, Switzerland: Springer, 2019, pp. 219–233.

[33] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Predicting phishing websites based on self-structuring neural network," *Neural Comput. Appl.*, vol. 25, no. 2, pp. 443–458, Aug. 2014.

[34] A. S. Bozkir, F. C. Dalgic, and M. Aydos, "GramBeddings: A new neural network for URL based identification of phishing web pages through N-gram embeddings," *Comput. Secur.*, vol. 124, Jan. 2023, Art. no. 102964.

[35] S. Mukkamala, G. Janoski, and A. Sung, "Intrusion detection using neural networks and support vector machines," in *Proc. Int. Joint Conf. Neural Netw.*, 2002, pp. 1702–1707.

[36] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, "Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1606–1615, Apr. 2018.

[37] B. F. Goldstein, V. C. Patil, V. C. Ferreira, A. S. Nery, F. M. G. França, and S. Kundu, "Preventing DNN model IP theft via hardware obfuscation," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 2, pp. 267–277, Jun. 2021.

[38] M. Pawlicki, R. Kozik, and M. Choraś, "A survey on neural networks for (cyber-) security and (cyber-) security of neural networks," *Neurocomputing*, vol. 500, pp. 1075–1087, Aug. 2022.

[39] A. Drewek-Ossowicka, M. Pietrołaj, and J. Rumiński, "A survey of neural networks usage for intrusion detection systems," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 1, pp. 497–514, Jan. 2021.

[40] J.-H. Li, "Cyber security meets artificial intelligence: A survey," *Frontiers Inf. Technol. Electron. Eng.*, vol. 19, no. 12, pp. 1462–1474, Dec. 2018.

[41] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: A comprehensive survey," *J. Defense Model. Simul., Appl., Methodol., Technol.*, vol. 19, no. 1, pp. 57–106, Jan. 2022.

[42] P. Podder, S. Bharati, M. R. H. Mondal, P. K. Paul, and U. Kose, "Artificial neural network for cybersecurity: A comprehensive review," 2021, *arXiv:2107.01185*.

[43] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.

[44] C. Birkle, D. A. Pendlebury, J. Schnell, and J. Adams, "Web of science as a data source for research on scientific and scholarly activity," *Quant. Sci. Stud.*, vol. 1, no. 1, pp. 363–376, Feb. 2020.

[45] J. Li and C. Chen, *CiteSpace: Text Mining and Visualization in Scientific Literature*. Beijing, China: Capital University of Economics and Bus. Press, 2016, pp. 149–152.

[46] Y. Mei, Z. Shihui, and Z. Wanlan, "The analysis of knowledge base, theme evolution and research hotspot of ideological and political theory course in colleges and universities based on CiteSpace," in *Proc. 2nd Int. Conf. Artif. Intell. Educ. (ICAIE)*, Jun. 2021, pp. 460–467.

[47] F. Feng, L. Zhang, Y. Du, and W. Wang, "Visualization and quantitative study in bibliographic databases: A case in the field of university–industry cooperation," *J. Informetrics*, vol. 9, no. 1, pp. 118–134, Jan. 2015.

[48] *Citespace 6.2.r7*, Citespace, 2024. [Online]. Available: https://citespace.podia.com/

[49] H. Small, "Co-citation in the scientific literature: A new measure of the relationship between two documents," *J. Amer. Soc. Inf. Sci.*, vol. 24, no. 4, pp. 265–269, Jul. 1973.

[50] J. Kleinberg, "Bursty and hierarchical structure in streams," in *Proc. 8th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Jul. 2002, pp. 91–101.

[51] Z. Xu, Y. Zhu, Y. Hu, M. Huang, F. Xu, and J. Wang, "Bibliometric and visualized analysis of neuropathic pain using web of science and CiteSpace for the past 20 years," *World Neurosurgery*, vol. 162, pp. e21–e34, Jun. 2022.

[52] Z. Shen, W. Ji, S. Yu, G. Cheng, Q. Yuan, Z. Han, H. Liu, and T. Yang, "Mapping the knowledge of traffic collision reconstruction: A scientometric analysis in CiteSpace, VOSviewer, and SciMAT," *Sci. Justice*, vol. 63, no. 1, pp. 19–37, Jan. 2023.

[53] W. Liu, "The data source of this study is web of science core collection? Not enough," *Scientometrics*, vol. 121, no. 3, pp. 1815–1824, Dec. 2019.

[54] M.-A. Vera-Baceta, M. Thelwall, and K. Kousha, "Web of science and scopus language coverage," *Scientometrics*, vol. 121, no. 3, pp. 1803–1813, Dec. 2019.

[55] A. V. Mbaziira and D. R. Murphy, "An empirical study on detecting deception and cybercrime using artificial neural networks," in *Proc. 2nd Int. Conf. Compute Data Anal.*, Mar. 2018, pp. 42–46.

[56] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, "Comprehensive review of cybercrime detection techniques," *IEEE Access*, vol. 8, pp. 137293–137311, 2020.

[57] S. Dilek, H. Çakır, and M. Aydın, "Applications of artificial intelligence techniques to combating cyber crimes: A review," 2015, *arXiv:1502.03552*.

[58] O. Kovalchuk, M. Kasianchuk, M. Karpinski, and R. Shevchuk, "Decision-making supporting models concerning the internal security of the state," *Int. J. Electron. Telecommun.*, vol. 10, pp. 301–307, Dec. 2022.

[59] O. Kovalchuk, M. Karpinski, S. Banakh, M. Kasianchuk, R. Shevchuk, and N. Zagorodna, "Prediction machine learning models on propensity convicts to criminal recidivism," *Information*, vol. 14, no. 3, p. 161, Mar. 2023.

[60] H. Chaudhary, A. Detroja, P. Prajapati, and P. Shah, "A review of various challenges in cybersecurity using artificial intelligence," in *Proc. 3rd Int. Conf. Intell. Sustain. Syst. (ICISS)*, Dec. 2020, pp. 829–836.

[61] M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L. F. Capretz, and S. J. Abdulkadir, "Detecting cybersecurity attacks in Internet of Things using artificial intelligence methods: A systematic literature review," *Electronics*, vol. 11, no. 2, p. 198, Jan. 2022.

[62] X. Jiang, J. Fan, Z. Zhu, Z. Wang, Y. Guo, X. Liu, F. Jia, and C. Dai, "Cybersecurity in neural interfaces: Survey and future trends," *Comput. Biol. Med.*, vol. 167, Dec. 2023, Art. no. 107604.

[63] M. Haris Uddin Sharif and M. Ali Mohammed, "A literature review of financial losses statistics for cyber security and future trend," *World J. Adv. Res. Rev.*, vol. 15, no. 1, pp. 138–156, Jul. 2022.

[64] V. Garg, "Covenants without the sword: Market incentives for cybersecurity investment," in *Proc. 49th Res. Conf. Commun., Inf. Internet Policy*, 2021, pp. 1–17.

[65] A. Alruwaili, "A review of the impact of training on cybersecurity awareness," *Int. J. Adv. Res. Comput. Sci.*, vol. 10, no. 5, pp. 1–3, 2019.

[66] L. Zhang-Kennedy and S. Chiasson, "A systematic review of multimedia tools for cybersecurity awareness and education," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–39, Jan. 2022.

[67] M. A. Alohali, F. N. Al-Wesabi, A. M. Hilal, S. Goel, D. Gupta, and A. Khanna, "Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment," *Cognit. Neurodyn.*, vol. 16, no. 5, pp. 1045–1057, Oct. 2022.

[68] H. Zheng, H. Wang, and J. Hu, "Cluster analysis of regulatory sequences with a log likelihood ratio statistics-based similarity measure," in *Proc. IEEE 7th Int. Symp. Bioinf. BioEng.*, Oct. 2007, pp. 1220–1224.

[69] K. R. Shahapure and C. Nicholas, "Cluster quality analysis using silhouette score," in *Proc. IEEE 7th Int. Conf. Data Sci. Adv. Anal. (DSAA)*, Oct. 2020, pp. 747–748.

[70] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, "Dropout: A simple way to prevent neural networks from overfitting," *J. Mach. Learn. Res.*, vol. 15, no. 1, pp. 1929–1958, 2014.

[71] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," 2014, *arXiv:1412.6980*.

[72] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 770–778.

[73] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[74] M. Al-Hawawreh, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial Internet of Things based on deep learning models," *J. Inf. Secur. Appl.*, vol. 41, pp. 1–11, Aug. 2018.

[75] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Gener. Comput. Syst.*, vol. 100, pp. 779–796, Nov. 2019.

[76] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Gener. Comput. Syst.*, vol. 82, pp. 761–768, May 2018.

[77] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet Things*, vol. 7, Sep. 2019, Art. no. 100059.

[78] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.

[79] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," 2018, *arXiv:1802.09089*.
[80] O. Alkadi, N. Moustafa, B. Turnbull, and K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9463–9472, Jun. 2021.
[81] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, "Dïot: A federated self-learning anomaly detection system for IoT," in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2019, pp. 756–767.
[82] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020.
[83] M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, "A hybrid deep learning model for efficient intrusion detection in big data environment," *Inf. Sci.*, vol. 513, pp. 386–396, Mar. 2020.
[84] M. Macas, C. Wu, and W. Fuertes, "A survey on deep learning for cybersecurity: Progress, challenges, and opportunities," *Comput. Netw.*, vol. 212, Jul. 2022, Art. no. 109032.
[85] S. Tsimenidis, T. Lagkas, and K. Rantos, "Deep learning in IoT intrusion detection," *J. Netw. Syst. Manage.*, vol. 30, no. 1, pp. 1–40, 2022.
[86] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, Jul. 2018.
[87] S.-W. Lee, H. Mohammed Sidqi, M. Mohammadi, S. Rashidi, A. M. Rahmani, M. Masdari, and M. Hosseinzadeh, "Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review," *J. Netw. Comput. Appl.*, vol. 187, Aug. 2021, Art. no. 103111.
[88] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," *ICISSp*, vol. 1, pp. 108–116, Jan. 2018.
[89] S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: A survey and an objective comparison," *J. Netw. Comput. Appl.*, vol. 169, Nov. 2020, Art. no. 102767.
[90] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.
[91] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.
[92] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102419.
[93] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 2, no. 1, pp. 41–50, Feb. 2018.
[94] M. I. Tariq, N. A. Memon, S. Ahmed, S. Tayyaba, M. T. Mushtaq, N. A. Mian, M. Imran, and M. W. Ashraf, "A review of deep learning security and privacy defensive techniques," *Mobile Inf. Syst.*, vol. 2020, pp. 1–18, Apr. 2020.
[95] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.
[96] S. Mahdavifar and A. A. Ghorbani, "Application of deep learning to cybersecurity: A survey," *Neurocomputing*, vol. 347, pp. 149–176, Jun. 2019.
[97] N. Moustafa and J. Slay, "The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," *Inf. Secur. Journal: A Global Perspective*, vol. 25, nos. 1–3, pp. 18–31, Apr. 2016.
[98] M. Z. Alom, T. M. Taha, C. Yakopcic, S. Westberg, P. Sidike, M. S. Nasrin, M. Hasan, B. C. Van Essen, A. A. S. Awwal, and V. K. Asari, "A state-of-the-art survey on deep learning theory and architectures," *Electronics*, vol. 8, no. 3, p. 292, Mar. 2019.
[99] N. Carlini and D. Wagner, "Towards evaluating the robustness of neural networks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 39–57.
[100] J. Qiu, J. Zhang, W. Luo, L. Pan, S. Nepal, and Y. Xiang, "A survey of Android malware detection with deep neural models," *ACM Comput. Surveys*, vol. 53, no. 6, pp. 1–36, Nov. 2021.
[101] N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, and A. Swami, "The limitations of deep learning in adversarial settings," in *Proc. IEEE Eur. Symp. Secur. Privacy*, Mar. 2016, pp. 372–387.
[102] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018.
[103] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2018, pp. 2154–2156.
[104] Y. Ding, S. Chen, and J. Xu, "Application of deep belief networks for opcode based malware detection," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2016, pp. 3901–3908.

RUSLAN SHEVCHUK (Member, IEEE) received the M.S. degree in computer systems and networks and the Ph.D. degree in computer systems and components from Ternopil National Economic University, Ukraine, in 2003 and 2008, respectively. He is currently an Assistant Professor with the Department of Computer Science and Automatics, University of Bielsko-Biala, Poland, and an Assistant Professor with the Department of Computer Science, West Ukrainian National University, Ukraine. His research interests include information security, cryptographic transformations, and cyber-physical systems.

VASYL MARTSENYUK received the master's degree in applied mathematics and the Ph.D. and D.Sc. degrees in systems analysis and decision making from the Taras Shevchenko National University of Kyiv, Ukraine, in 1993, 1996, and 2005, respectively, and the Dr.Hab. degree, in 2015. From 1997 to 2015, he was a Professor, the Chair of the Medical Informatics Department, and the Vice-Rector of Ternopil State Medical University, Ukraine. He received the title of a Professor of technical sciences in Poland, in 2015. He joined the Department of Computer Science and Automatics, University of Bielsko-Biala, Poland, as a Professor, in 2015, where he has been the Head of the Department, since 2023. Since 2020, he has been coordinating EU-funded projects on big data and artificial intelligence. His research interests include artificial intelligence, big data, cyber-physical systems, and medical informatics.