Results in Control and Optimization 10 (2023) 100204

Contents lists available at ScienceDirect

Results in Control and Optimization

journal homepage: www.elsevier.com/locate/rico

A bibliometric analysis of cyber security and cyber forensics research

Deepak Sharma [a], Ruchi Mittal [b], Ravi Sekhar [c], Pritesh Shah [c,*], Matthias Renz [a]

[a] Department of Computer Science, Christian-Albrechts-University Kiel, Kiel, 24118, Germany
[b] Department of Computer Science, Ganga Institute of Technology and Management, Bahadurgarh-Jhajjar Road Kablana, Jhajjar, 124104, Haryana, India
[c] Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune, 412115, India

ARTICLE INFO

Keywords:
Anomaly detection
Cyber security
Cyber forensics
Cyber attack
Malware detection
Machine learning
Deep learning
Bibliometry

ABSTRACT

Cybersecurity is one of the most important concerns associated with ever expanding internet based technologies, products, services and networks. If cybersecurity is prevention then cyber forensics is the cure. Both are equally important pillars of digital security. This paper presents an extensive bibliometric analysis of cybersecurity and cyberforensic research published in Web of Science during the past decade (2011–2021). The analysis included yearly publications, publication types and trends across different verticals such as publishing sources, organizations, researchers, countries and keywords. Full counting method was used for citation analysis, whereas fractional counting method was implemented to analyze co-citation, co-author collaborations as well as keyword co-occurrences across all these verticals. Furthermore, timeline and burst detection analyses were carried out to unravel significant topic trends and citations in the last decade. The study presents bibliometric results in terms of the authors, organizations, countries, keywords, sources and documents with the highest collaborative link strengths worldwide in the field of cybersecurity and forensics. Latest trends, under-investigated topics and future directions are also presented.

1. Introduction

Cyberattacks on the host computer's information and services are hostile operations that aim to interrupt, degrade, deny or corrupt essential information and services. Cybersecurity refers to the various defense mechanisms employed to safeguard against such attacks. Cyber forensics refers to the science of data recovery and attack tracing after an attack event. A lot of time and effort is required by conventional security software to identify and categorize potential/new threats and encode these categorizations in order to detect such attacks in the future. Using machine learning techniques, this time-intensive procedure may be made more efficient. Therefore, various machine learning techniques were created to identify assaults more rapidly and accurately [1].

Cyber security and forensics is a serious issue across all industries and sectors because of the prevalence and rapid expansion of computer systems and internet capabilities. Higher education is also increasingly facing such dangers. There have been reports of data breaches at universities as a result of cyber-attacks. Higher education users employ portable gadgets that allow them to be extremely mobile. These gadgets enable students to become acclimated to networking, allowing them to connect to the unsecured networks at any time and from any device. As a result of the openness and simple access to data and information, cyber security is particularly difficult to implement in higher educational institutions [2]. Inadequate cyber security exposes higher education to

* Corresponding author.
E-mail addresses: deepak.btg@gmail.com (D. Sharma), ruchi.mittal138@gmail.com (R. Mittal), ravi.sekhar@sitpune.edu.in (R. Sekhar), pritesh.ic@gmail.com (P. Shah), mr@informatik.uni-kiel.de (M. Renz).

https://doi.org/10.1016/j.rico.2023.100204
Received 10 October 2022; Received in revised form 5 December 2022; Accepted 17 January 2023
Available online 20 January 2023

risks, and the existence of numerous sorts of academic research data has made educational institutions a desirable target for cyber criminals [3]. This implies that higher education institutions, such as universities, are now vulnerable to cyber security threats [4]. Because most colleges embrace open access and an information-sharing culture, they become more susceptible. This is a concerning condition for higher education, as cyber dangers such as hacking have the potential to interrupt academic operations. Hackers distribute useful information from colleges, and they may readily sell this knowledge since data has become a commodity [3]. Universities' online systems are a possible target for cyber security concerns such as hacking [3]. This is because university systems include sensitive personal information about students and employees, as well as a wealth of intellectual property created by scholars. The university community's culture of open communication and collaboration, which includes students, administrative personnel, professors, and research groups, makes the system even more exposed to challenges [5,6].

Data security and forensics are some of the most important aspects of data science, ever growing in importance year after year as most firms, large and small, acquire massive volumes of relevant data [7]. Cyber criminals target sensitive data of governments, military, national intelligence, security agencies, financial institutions, corporations, businesses, hospitals, agriculture and many more [8]. Data used by well-known organizations such as Microsoft and Google to get perspectives for their decision-making and to better comprehend the relationships between present and next-generation technologies is also a prime target [9].

1.1. Motivation, importance and benefits of the current study

The motivation of the current study is to provide deep and meaningful insights into firstly, the most significant contributors and collaborations in the field of cybersecurity and cyber forensics over the past decade and secondly, to reveal the most crucial research areas, timeline trends of topic clusters, keywords and scientific papers. Based on the above mentioned analyses, the current study aims to provide directions for further research in this rapidly emerging field. The importance of this study is evident from the critical roles that cybersecurity and cyber forensics play in ensuring the safety and reliability of all our digital information and transactions. Any compromise in this regard may lead to the sensitive information/functionality breaches leading to severe and irreparable losses. Hence, this study is important in terms of its bibliometric analysis based contribution to the field of cybersecurity and cyber forensics as a whole. As far as the benefits of this work are concerned, firstly the recognition of the most impactful researchers, institutions, nations, journals and their mutual collaborations in this field is of immense benefit to the entire scientific research community. Secondly, the temporal evolution of the research themes, topics and keywords over the past decade benefits the researchers to direct their investigations into niche and less investigated areas. This study points out some important future/emerging areas to benefit the upcoming researchers in this field.

2. Related work and data collection

The following subsections present a brief review of the related bibliometric/review studies followed by the details of data source, data collection and data preprocessing adopted in the current work.

2.1. Bibliometric analysis and related work

Bibliometric analysis supplements traditional literature evaluations by objectively assessing a study area's trends and prospects [10–13]. This analysis is valuable for highlighting the evolution of a particular field of study over several years or even decades [14]. There are a variety of approaches for reviewing scientific research advancements in a specific topic [15]. Evaluative and relational reviews are the primary categories of these methodologies [16]. The evaluative reviews are used for quantitatively studying the absolute research impacts of research publications, authors, organizations, and countries. Various productivity variables, such as the number of journals, publications per year, number of citations and more are included in this analysis [17]. Expert judgments on research impact indicators in a particular field can also be used to undertake qualitative evaluative reviews [18]. On the other hand, the relational review techniques concentrate on the inter-relationships between the evaluative measures stated above. The number of collaborative outputs, collaborative links and related link strengths are used to quantify and express these inter-relationships. Citations-based connections, co-occurrences, and co-citations-based analyses are other useful relational metrics [19]. Linkages between co-authors are crucial indications of information transfer between various research groups [20]. Understanding research links among prolific writers and organizations requires evaluation of citation linkages [21]. The breadth of collaborations/co-citations across geographies is also determined by connection strengths [22].

The current study incorporates evaluative and relational techniques for a balanced bibliometric analysis of cybersecurity and cyber forensics research. Bibliometric surveys [12] give information on the evolution of a research field over one or more decades. These analyses typically yield vital information about individual authors' research outputs and their affiliated organizations' research outputs [23], collaboration and citation networks among documents, authors, organizations, and places [24], trending topics and keywords [18], top publishing journals, inter-journal linkages [25,26] and more. Data visualization tools are critical for successfully presenting study results and arriving at actionable conclusions quickly [27]. VoSviewer and CiteSpace were used in the current study for quantitative data analysis and visualization of cybersecurity/forensic research published in the Web of Science (WoS) from 2011 to 2021. Based on the bibliometric analysis of collaboration/citation data, VoSviewer creates author and journal network maps. It can also generate keyword maps that demonstrate the relationships between numerous co-occurring phrases in a study topic [28]. CiteSpace is basically a Java program that visualizes citation networks [29], co-authorship relationships, time series analysis of major subjects, and citation/reference bursts [30].

Recent bibliometric studies on cybersecurity aspects include Jalali et al. [31], who conducted bibliometric analysis of cybersecurity in healthcare domain. This study considered about 472 publications indexed in Web of Science and PubMed databases. Rahim [32] analyzed cybersecurity research in higher education using bibliometry. Makawana and Jhaveri [33] applied bibliometry to analyze the impact of machine learning techniques in cybersecurity. Elango et al. [34] redefined cybersecurity keywords through a bibliometric analysis and clustering of the associated search terms. Azambuja and Almeida [35] analyzed cybersecurity publications in industry 4.0 domain. Rehman et al. [36] analyzed 100 top cited articles dealing with information security in business enterprises using bibliometry. Shukla and Gocchait [37] conducted a short bibliometric analysis of cybersecurity research published in Web of Science. Nakhodchi and Dehghantanha [38] applied bibliometric tools to analyze Web of Science published research on deep learning in cybersecurity implements. The authors included the bibliometric analyses of research areas, continents, countries, institutions, authors, keywords and terms. Gill et al. [39] conducted a bibliometric analysis into mobile forensics research. Kusuma et al. [40] conducted a bibliometric study on digital forensics research in Indonesia. Baldwin et al. [41] conducted a bibliometric analysis of cloud forensics research. Gokhale et al. [42] analyzed digital image forensics research using bibliometry. Gou et al. [43] used bibliometric mapping to analyze research on system dynamics safety and security. Thakur and Purandare [44] applied bibliometry to analyze cyber attacks carried out on financial institutions since 2016. The authors considered publications from the Scopus and Web of Science Core Collection databases and included the year and number of publications, citations and keywords in their analyses. Yarovenko [45] also applied bibliometric analysis to identify cyber frauds in financial systems. The author used VOSviewer software to analyze relevant research articles published during 2017 to 2022. Bolbot and Musharraf [46] investigated research developments in maritime cybersecurity using bibliometric analysis. Cojocaru and Cojocaru [47] conducted a bibliometric analysis of cybersecurity research published by Moldovan investigators. Their study included over 68,000 articles published during 2008–2018 and sourced from Web of Science and Scopus databases. Goyal [48] conducted a bibliometric study of blockchain technology in cyber forensics including analyses of research institutions, countries, authors, funding agencies, keywords and journals. Ismayilova [49] used bibliometry to analyze various aspects of articles addressing information security concerns. The author determined the most productive authors, journals, countries in this field. Citation based network maps among various nations were also constructed.

The preceding brief review indicates that most of the above mentioned studies were focused on bibliometric analysis of cybersecurity in relatively narrower domains such as healthcare, higher education, machine learning, keywords, industry 4.0, business enterprises, mobile forensics, digital forensics, financial institutions, maritime security and system dynamics. Hence, an in-depth, comprehensive bibliometric examination of cybersecurity and cybersecurity is required for the period of past ten years. The current effort attempts to close this research gap by giving academics multi-dimensional insights into current and future developments in this promising sector.

2.2. Data source, collection and pre-processing

The Web of Science (WoS) repository was chosen as the research database for the current study's bibliometric analysis. This database contains a comprehensive collection of high-quality, high-impact research papers published in the world's most famous publications. It contains a database of publications published in indexed journals since 1990. The Emerging Science Citation Index (ESCI), Science Citation Index Expanded (SCIE), Social Sciences Citation Index (SSCI), Arts and Humanities Citation Index (AHCI), Conference Proceedings Citation Index—Social Sciences and Humanities (CPCI-SSH) and Book Citation Index—Social Sciences and Humanities (CPCI-SSH) are all part of the WoS core collection. BCI-SSH (Book Citation Index—Science), CPCI-S (Conference Proceedings Citation Index—Science) and BCI-S (Book Citation Index—Science) are also included in WoS. The WoS document search string in the current study was composed as follows - ((((online AND fraud) OR (anomaly) OR (malware) AND detection) OR (cyber AND (forensics OR attack))) AND ((machine OR deep) AND learning)) for a period of one decade, from 2011 to 2021. For the search terms mentioned above, the search parameters were set to 'full record and cited references'. This search was conducted in January 2022, which yielded 9152 research papers extracted from the database in plain text form. The search resulted in precise document entries that matched the cybersecurity and forensics related keywords well.

3. Publication structure analysis

This section explains how the searched publications were distributed according to publication years, kinds, source titles, cybersecurity and forensic study topics and trends. In addition, the top cybersecurity and forensic research contributing nations, organizations, authors, and nationalities and their corresponding publication counts are also presented. All the results presented in this section were obtained directly from the Web of Science filtered analysis options, that were applied on the entire document corpus extracted using the search string mentioned in the previous section.

3.1. Year on year publication analysis

Fig. 1 depicts the progression of WoS research articles in the field of cyber security and forensics year on year. The x-axis indicates the publishing years from 2011 through 2021, while the y-axis depicts the number of WoS publications. The actual publication counts have been highlighted on the top of yearly publication bars. From 2011 to 2017, the number of cyber forensic publications gradually increased. Since 2018, these figures have increased aggressively, reflecting a growing interest and demand in cybersecurity and forensic research. Compared to prior years, the number of publications from 2019 and 2021 increased significantly. The number of cybersecurity and forensic papers published in WoS in 2021 more than quadrupled the number of manuscripts published during the initial years of the past decade.

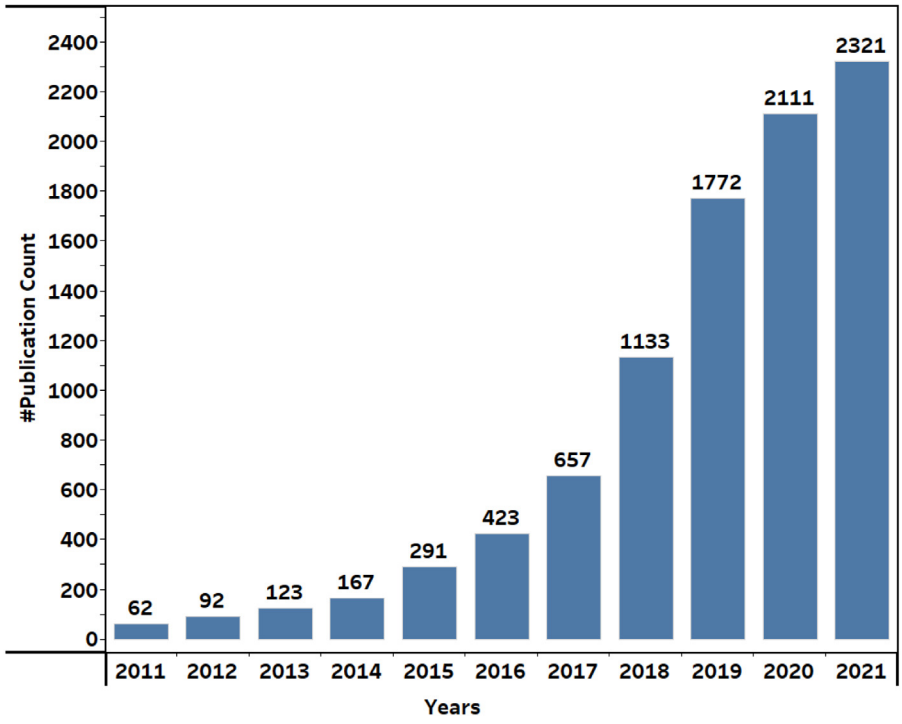

Fig. 1. Annual publication in the field of cyber security and forensics from 2011 to 2021.

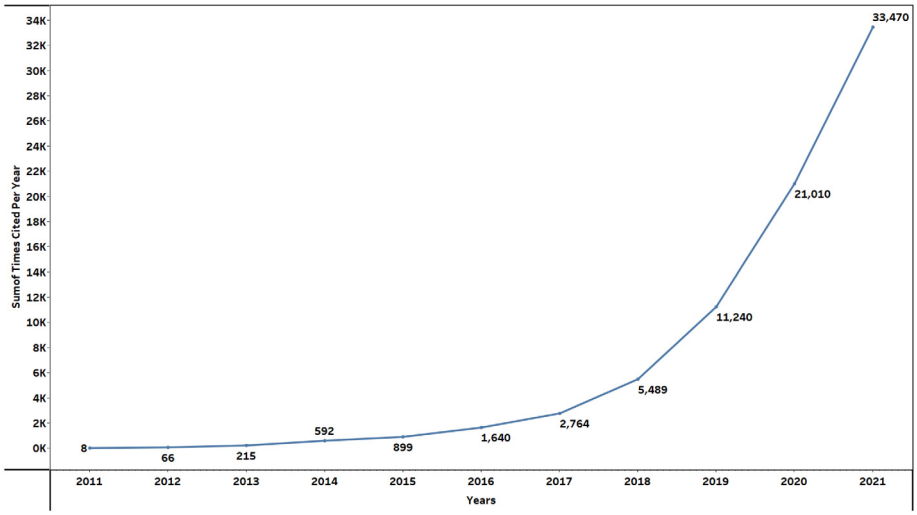

Fig. 2. Sum of citations (total citations) received by the cybersecurity and forensic related WoS publications per year.

With the growth of social networking and the internet usage, cybercrime has increased, necessitating research efforts in cyber security and forensics at a faster rate. Hence, academics' interest in this evergreen issue is expected to continue in the future. This is clearly evident in Fig. 2. This figure shows an exponential rise in the citations received by the cybersecurity and forensic related WoS publications. The following subsection gives details of the different types of WoS publications in this field.

3.2. Publication type

The WoS database search yielded a total of 9152 cybersecurity and forensic publications, which included research articles, conferences, review papers, early access documents and more. Fig. 3 depicts all these categories of publications and their corresponding counts. Research papers account for a significant portion of all publications (4685). The second-largest group of

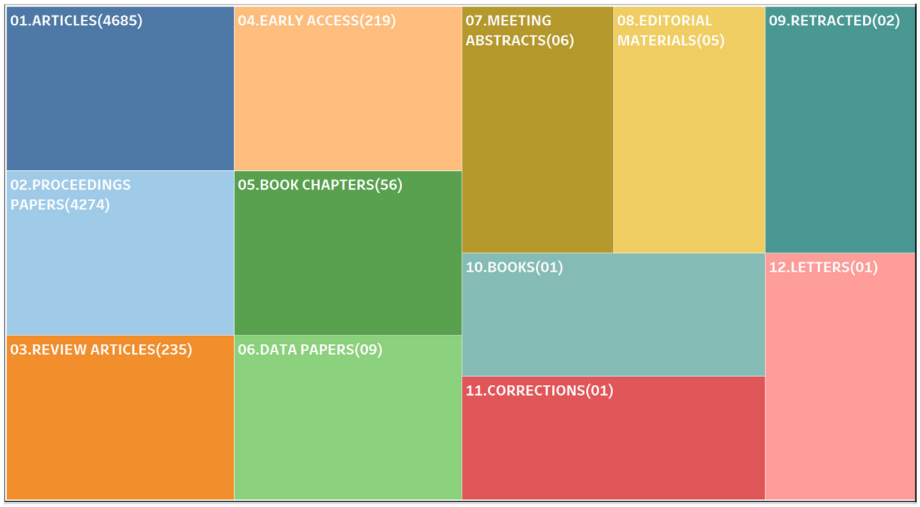

Fig. 3. The top 12 categories of a total of 9152 cyber-security and forensic publications of the WoS database.

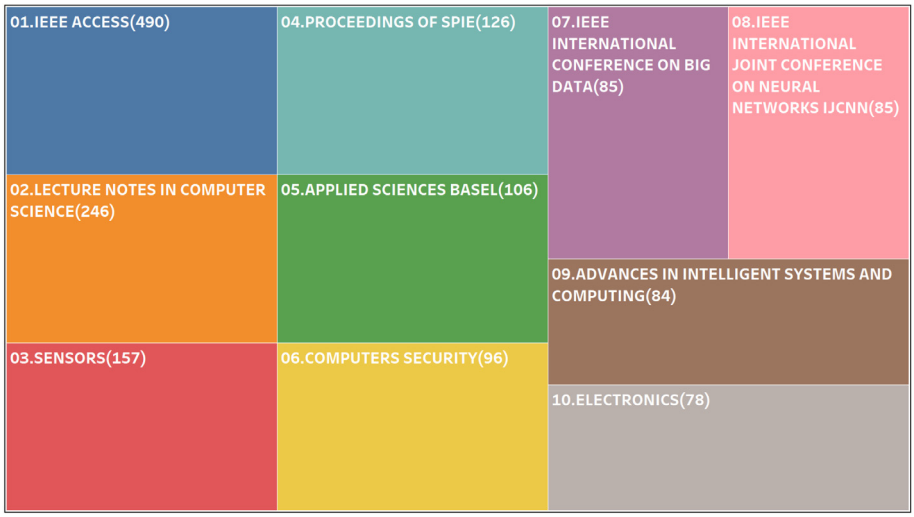

Fig. 4. The top 10 source title of a total of 9152 cyber-security and forensic publications of the WoS database.

cybersecurity and forensic publications is proceedings papers (4274), while review articles (235) make up 0.2 percent of the total corpus. On the other hand, book chapters (56) and early access papers (219) formed 0.02 and 0.23 percents of the total documents. Letters, corrections, editorials, data papers, reprints and other publishing categories made up less than 0.25 percent of the exported database.

3.3. Publication source

This subsection focuses on the top sources publishing cybersecurity and forensic research and indexed in WoS. Fig. 4 depicts these sources as well as the number of articles published in them. As per source-wise distribution analysis, the journal 'IEEE Access and LNCS' published the most articles (736), accounting for 6.39 percent of all published content in the topic of cybersecurity and forensic composites. With 157 (4.67 percent) publications, the 'Sensors Journal' was identified as the third highest publishing source. From 2011 and 2021, the journals 'Proceedings of SPIE' 'Applied Science BASEL', Computer Security', and 'IEEE international conference on Big Data' published the fourth (126), fifth (106), sixth (96) and seventh most cybersecurity and forensic papers. The remaining journals that emerged among the top ten publishers were 'IEEE conference on neural networks' (eighth), Advances in intelligent system and computing' (ninth), and Electronic journal' (tenth). As many as 85, 85, 84 and 78 articles were published in these conferences/journals (respectively) during the surveyed period. The following subsection presents the top organizations worldwide whose members have published maximum articles in WoS.

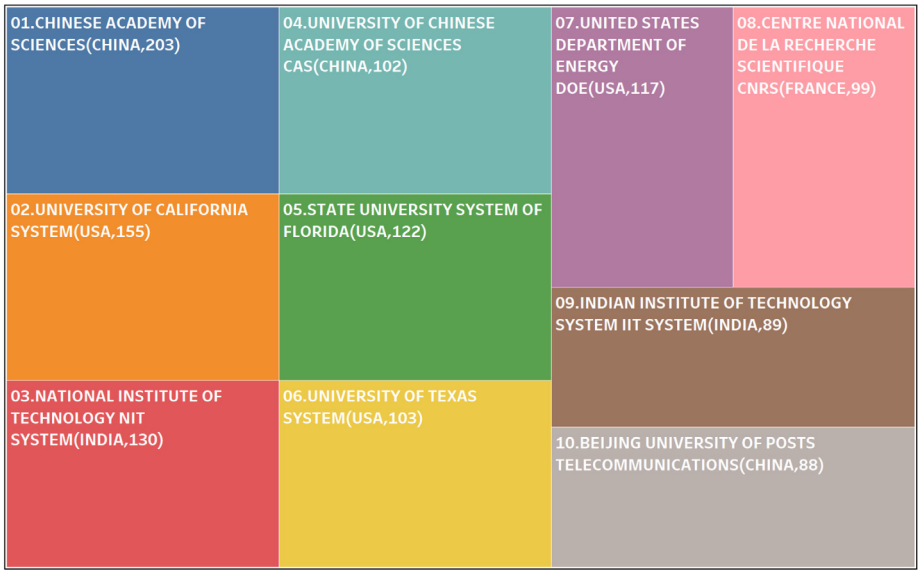

Fig. 5. The top 10 organizations of a total of 9152 cyber-security and forensic publications of the WoS database.

Table 1
The 10 most productive authors in the field cyber-security and forensic.

Author	Organization	Country	Record
Wang, Yong	Beijing Inst Technol, Sch Software, Beijing	China	40
Kim, Jonghyun	ETRI, Informat Secur Div, Daejeon	South Korea	35
Liu, Yang	Nanyang Technological University	Singapore	33
Li, Jing	Henan University of Technology, Zhengzhou	China	33
Zhang, Jun	Swinburne University of Technology,	Australia	32
Zhang, Yi	Natl Univ Def Technol, Coll Comp, Hunan	China	31
Alazab, Mamoun	Charles Darwin Univ, Casuarina, NT	Australia	28
Wang, John	PFP Cybersecur, Spring Hill, Vienna	USA	28
Wang, Zi	New York Inst Technol, Dept Comp Sci, New York	USA	28
Elovici, Yuval	Ben Gurion Univ Negev, Cyber Secur Res Ctr Malware Lab, Beer Sheva	Israel	27

3.4. Productive organizations and researchers

This subsection analyzes the top ten organizations publishing cybersecurity and forensic-domain articles in Web of Science during 2011–2021. Fig. 5 shows that the Chinese Academy of Science (China) published maximum WOS papers (203) in the field of cybersecurity and forensics. The second-highest number (155) of WoS articles was contributed by the University of California during 2011–2021. The National Institute of Technology NIT System, India, followed it with 130 publications. The University of Chinese Academy of Science, China, bagged the fourth position with 102 publications, whereas the State University of Florida published 122 articles. Researchers at the University of Texas systems published 103 articles on cybersecurity and forensics. These were followed by the United state department of energy DOE and the Centre National de la Recherche Scientifique CNRS, France, with 117 and 99 publications respectively. Finally, the Indian Institute of Technology, India, and Bejing University Post Telecommunication arrived ninth and tenth. Their researchers published 89 and 88 WoS papers on cybersecurity and forensics, respectively. This analysis showcases that the Chinese, USA and Indian authors have contributed significantly to the cybersecurity and forensic research over the past decade.

Table 1 shows the list of top ten researchers with maximum WoS publications in cybersecurity and forensics. Of these top ten authors, three are from China and two from USA and Australia, respectively. There is one author each from South Korea, Singapore and Israel.

3.5. Countries trends

This subsection highlights the top ten nations contributing WoS articles in cybersecurity and forensics — USA, Peoples Republic of China, India, England, Australia, South Korea, Canada, Italy, Germany and Japan. Fig. 6 depicts the publication output trends of these nations 2011 onward. It is evident that the researchers from the USA contributed the maximum research papers every year till 2020. In 2021 there has been a dip in the USA publication output. Thus, the Chinese research output, which was consistently second

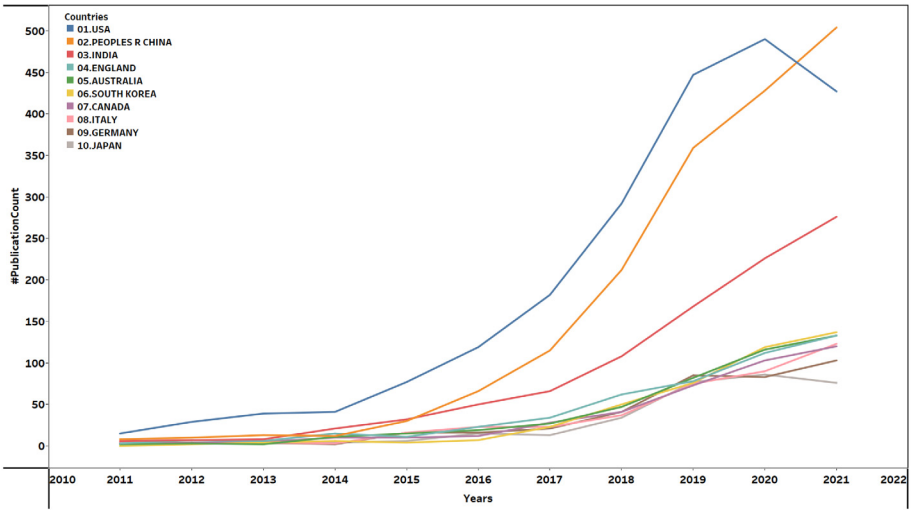

Fig. 6. Publication count trends of countries of a total of 9152 cyber-security and forensic publications of the WoS database.

highest till 2020, claimed the top position in 2021 (1757 WoS papers). The third most significant contributions to cybersecurity and forensic research came from India. The Indian researchers performed almost at par with their Chinese counterparts till 2015 (74 papers), afterwards, the publication gap between the two countries increases where the publication count of Chinese researchers overtake the Indian publication count. Still, the Indian researchers maintained their third position in terms of WoS papers published every year, till 2021 (968 WoS total papers). Among the other nations making it to the top ten contributors, South Korea, Australia and England published almost similar number of WoS papers throughout the timeline considered in the current work. They are followed by Canadian, Italian and German researchers. All of the top ten countries are progressively increasing their research outputs over the years except for USA and Japan, wherein a downward trend has begun in the last couple of years.

3.6. Popular research areas

This section showcases the most important topical areas in which cybersecurity and forensic issues/solutions have been addressed by researchers. Fig. 7 shows that most WoS articles addressed the cybersecurity and forensic applications in the area of computer science' (6285 articles), followed by 'engineering' with 3948 papers. The third most investigated area is cybersecurity and forensic aspects in 'telecommunication' with 1898 papers, which is a rapidly emerging area with increasing coverage and speed of telecommunications based services in developing economies. Next in line is the topic of automation control systems' with 343 WoS articles, highlighting the emerging importance of cybersecurity and forensic features in connected industrial systems for smart manufacturing. These topics are followed by cybersecurity and forensic research in physics and chemistry domains with 348 and 280 WoS papers respectively, indicating an interesting trend generally not very evidently visible in contemporary research. About 270 WoS articles were tagged under 'instrumentation', showing the cybersecurity and forensic research in the domain of device level automation and control instrumentation. Another 244 WoS articles focused on cybersecurity and forensics in 'imaging science and photographic technologies', indicating importance of data security during event recording, image capturing, storage, transmission and analyses. Applications of cybersecurity and forensic in general science and technology areas were covered in 227 WoS articles, whereas 210 papers addressed cybersecurity and forensic threats in the processing and proliferation of different kinds of advanced materials.

Fig. 8 shows the WoS publication trends of the research areas mentioned above. It is evident that cybersecurity and forensics in computer sciences is the most significantly trending area since 2011. Over the past decade there is no other research area that has been addressed for cybersecurity and forensic investigations as 'computer science'. Cybersecurity and forensic research trend in computer sciences witnessed maximum growth during 2017 to 2019. Thereafter, researchers' interest in this area seems to be hitting a plateau. It seems that researchers have reached a saturation point in this field and new breakthroughs are awaited to grow this trend further. The next most trending cybersecurity and forensic research areas are 'engineering' and 'telecommunications'. These two areas have also been continuously growing in their respective publication trends over the past decade, although at a lower rate than 'computer science'. However, research trends in 'telecommunications' have taken a dip since 2020. This phenomenon may be related to Covid-19 related slow downs imposed on the growth of telecommunications networks throughout the world. The remaining research areas featuring in the top ten list, viz. 'physics', 'chemistry', 'instruments instrumentation', 'imaging science photographic technology', 'science technology other topics' and 'materials science' witnessed marginal growth over the past decade, with interests picking up only during the last couple of years. More cybersecurity and forensic research is expected to be conducted in these emerging areas in future. Cybersecurity and forensic publications in 'automation control systems' appears to be stagnant and needs to be focused more by the research community.

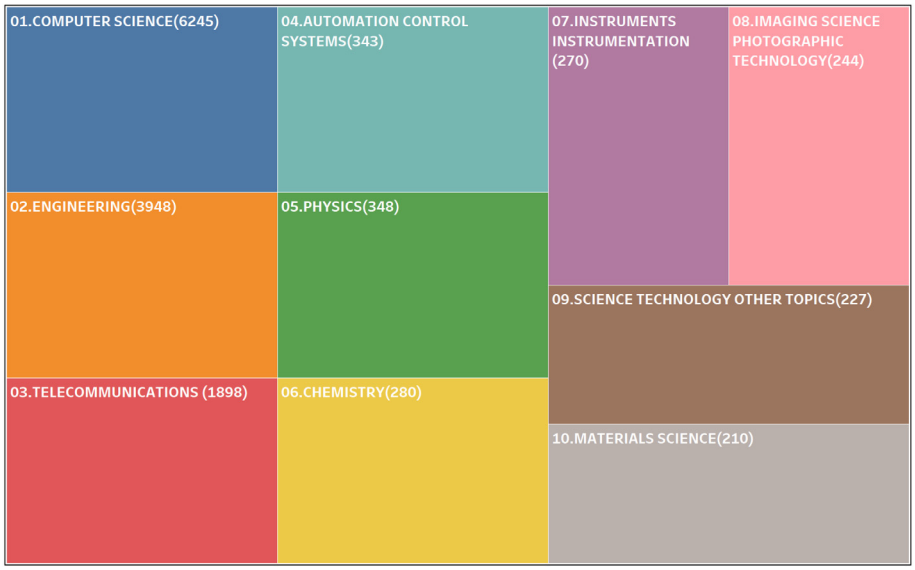

Fig. 7. Top research areas of a total of 9152 cyber-security and forensic publications of the WoS database.

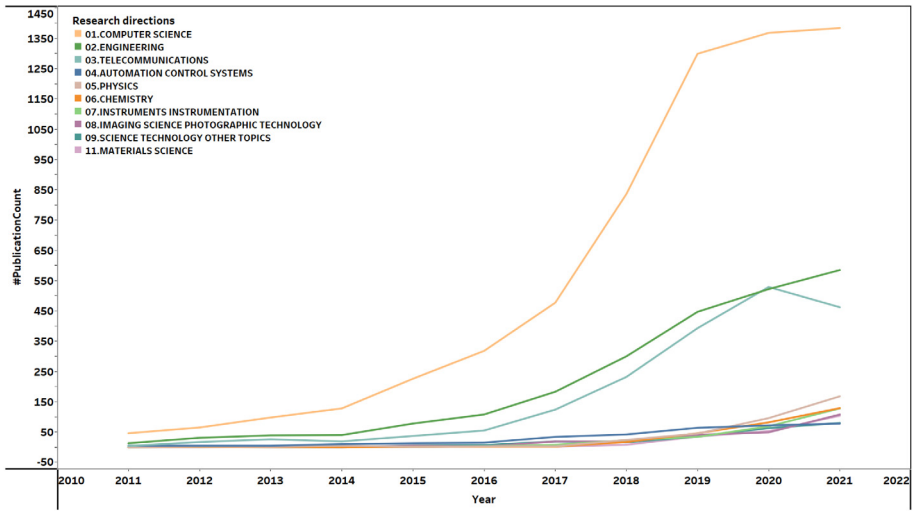

Fig. 8. Publication count trends of research areas of a total of 9152 cyber-security and forensic publications of the WoS database.

3.7. Web of science indexed publications and categories

This section depicts the distribution of cybersecurity and forensic related research articles available under leading Web of Science indices. Fig. 9 shows the number of papers published and indexed in the WoS corpus indices. Most of the WoS publications (4258) have been published under the Conference Proceedings Citation Index. Conference publications are important to showcase early results obtained in research projects and obtain valuable feedback from the scientific community on the same. The second-highest number of articles have been published under the Science Citation Index Expanded (4220), which is quite popular and is a well known identifier of its indexed journals as publishers of good quality of research. The Emerging Sources Citation Index (ESCI) and the Social Sciences Citation Index (SSCI) include 624 and 195 cybersecurity and forensic related articles respectively. The ESCI index includes journal titles that are rapidly emerging titles featuring quality research outputs. On the other hand, the SSCI indexed publication numbers indicate the articles published in journals addressing social science related topics. This shows the wide scope of cybersecurity and forensic research much beyond science and technology domains. Similarly, 57 articles were indexed in the Conference Proceedings Citation Index—Social Science and Humanities. The Book Citation Index—Science included 56 cybersecurity and forensic related articles, whereas the Book Citation Index - Social Science and Humanities comprised of only 7 articles and held the seventh position in the top ten indices list. Finally, the pure Arts and Humanities Citation Index included only 6 published

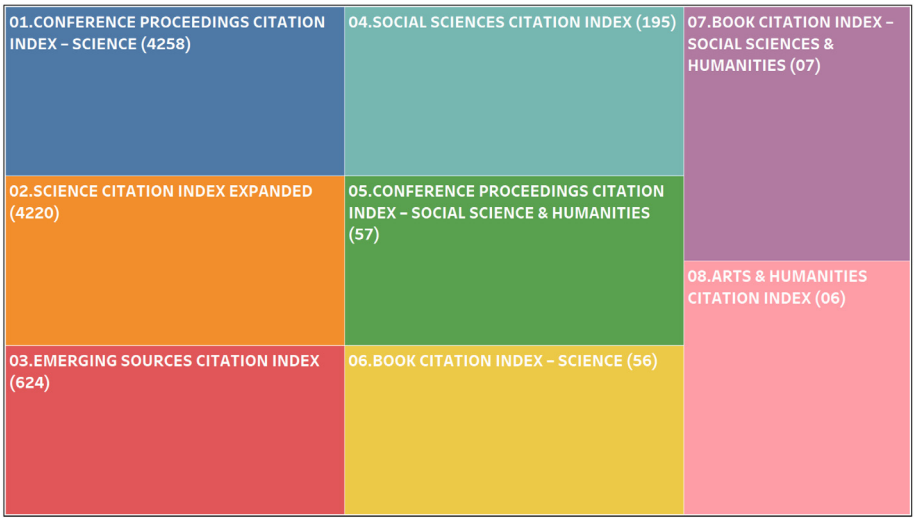

Fig. 9. Web of Science Indexes of a total of 9152 cyber-security and forensic publications of the WoS database.

articles related to cybersecurity and forensic. Hence, there is more scope for cybersecurity and forensic research applications in arts, humanities and social science domains.

Fig. 10 depicts the cybersecurity and forensic related publications classified by Web of Science under different categories. The analysis results indicate that the leading number of publications (3195) are categorized under 'Engineering Electrical Electronic' indicating a large number of articles focusing on the electrical and electronics engineering related aspects of cybersecurity and forensic. However, six of the top ten WoS categories specify computer science related areas, indicating that vast majority of the articles focused on cybersecurity and forensic aspects in computer science applications. These areas titled 'Computer Science Information Systems', 'Computer Science Theory Methods', 'Computer Science Artificial Intelligence', formed the second (3027 papers), third (2383 papers), fifth (1869 papers), sixth (730 papers), seventh (712 papers) and eighth (679 papers) most popular WoS categories respectively. The remaining significant category in the WoS top ten included 'telecommunication' with 1898 articles at the fourth position. The last two spots in the WoS top ten were occupied by the 'automation control systems' with 343 papers and 'engineering multidisciplinary' with 302 papers.

Fig. 11 depicts the publication trends of the above mentioned WoS categories during 2011–2021. It is evident that the category of 'Engineering Electrical Electronic' maintained a higher rate of climb over the past decade as compared to all other categories. It was surpassed briefly by the 'Computer Science Information Systems' during 2019–2020. In 2021, it regained its top spot as the category with the maximum publications related to cybersecurity and forensic, seconded by 'Computer Science Information Systems', which seems to have hit a plateau after 2020. The next three categories with significant publication trends are 'Computer Science Theory Methods', 'Telecommunications' and 'Computer Science Artificial Intelligence'. These three categories witnessed growth in annual publications till 2019–2020, post which these trends started dipping. This is an interesting phenomenon, given that the cybersecurity and forensic aspects are closely related to computer science theory methods as well as with the applications of various artificial intelligence techniques. The remaining five WoS categories did not register any substantial research attention till 2017, post which the annual number of published articles started picking up pace. These research categories offer maximum opportunities for carrying out novel cybersecurity and forensic investigations.

4. Co-authorship analysis

Collaboration breeds quality research outputs. Inter-departmental, inter-institutional and international collaborations are deemed necessary for facilitating useful exchange of new ideas and approaches to existing issues for mutual benefits. Following subsections details upon bibliometric analysis of various collaborative research aspects pertaining to the topic of cybersecurity and forensics. VOS viewer software was used for extracting and analyzing these results.

4.1. Co-authorship analysis based on authors

This subsection presents co-authorship analysis of cybersecurity research publishing authors during the past decade. VoS search yielded a total of 20 827 such authors. The co-authorships among these researchers were analyzed using fractional counting method with a threshold of minimum 5 published documents and 10 citations per author. Fractional counting has been established as a better methodology in bibliography as compared to full counting due to its equal emphasis on lowly cited and highly cited references representing the same article [50]. In the current analysis, documents co-authored by more than 25 researchers were

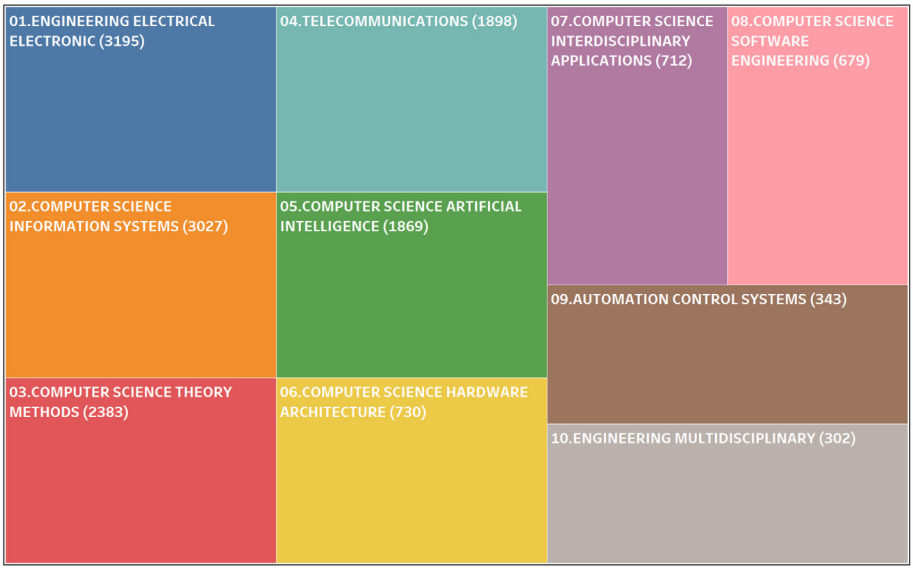

Fig. 10. Web of Science Category of a total of 9152 cyber-security and forensic publications of the WoS database.

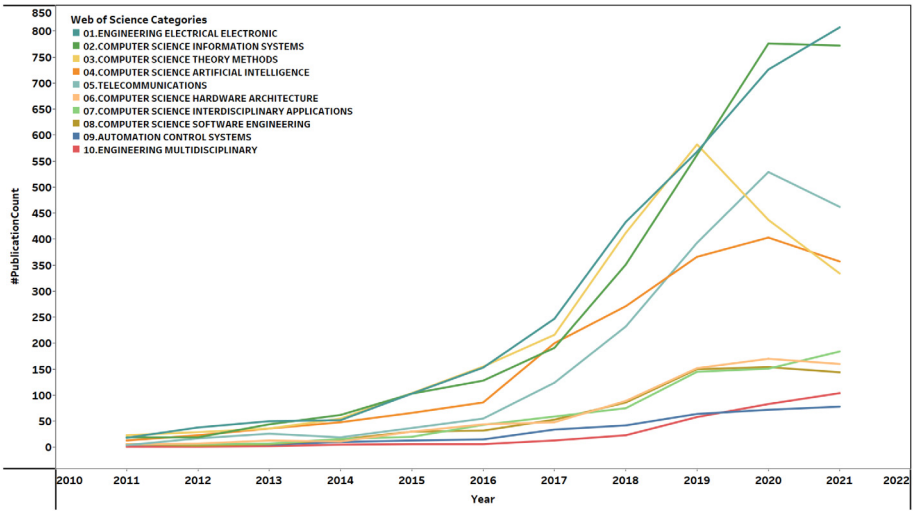

Fig. 11. Web of Science Trend of a total of 9152 cyber-security and forensic publications of the WoS database.

Table 2
The top 10 researchers with maximum TLS values.

Rank	Author	Country	P	Links	TLS
1	Zhang, Y	China	97	158	82.00
2	Li, Y	China	87	147	79.00
3	Wang, J	USA	87	145	76.00
4	Wang, Y	China	83	121	74.00
5	Wang, Z	USA	73	118	67.00
6	Zhang, X	Australia	69	130	64.00
7	Liu, Y	Singapore	75	145	63.00
8	Wang, X	China	68	112	62.00
9	Li, Z	Singapore	64	93	61.00
10	Zhang, J	Australia	68	92	61.00

not considered. Only 900 met the above mentioned criteria. Of these, 788 were found to form the largest network of co-authors. From this set of 788, the top ten organizations with highest co-authorship based TLS values are listed in Table 2. In this table, 'P'

Table 3
The top 13 organizations with the maximum TLS.

Rank	Organization	Country	P	Links	TLS
1	Chinese Academy Science	China	159	100	142.00
2	University of Chinese Academy of Sciences	China	101	47	98.00
3	King Saud University	Saudi Arabia	64	59	48.00
4	Deakin University	Australia	62	45	45.00
5	Tsinghua University	China	67	57	45.00
6	Nanyang Technological University	Singapore	68	55	42.00
7	Beijing University of Posts and Telecommunications	China	84	36	37.00
8	University of New South Wales	Australia	46	41	34.00
9	Shanghai Jiao Tong University	China	56	35	33.00
10	Qatar University	Qatar	39	28	32.00
11	The University of Texas at San Antonio	USA	48	40	32.00
12	University of Sydney	Australia	35	37	30.00
13	University of Illinois at Urbana-Champaign	USA	40	41	28.00

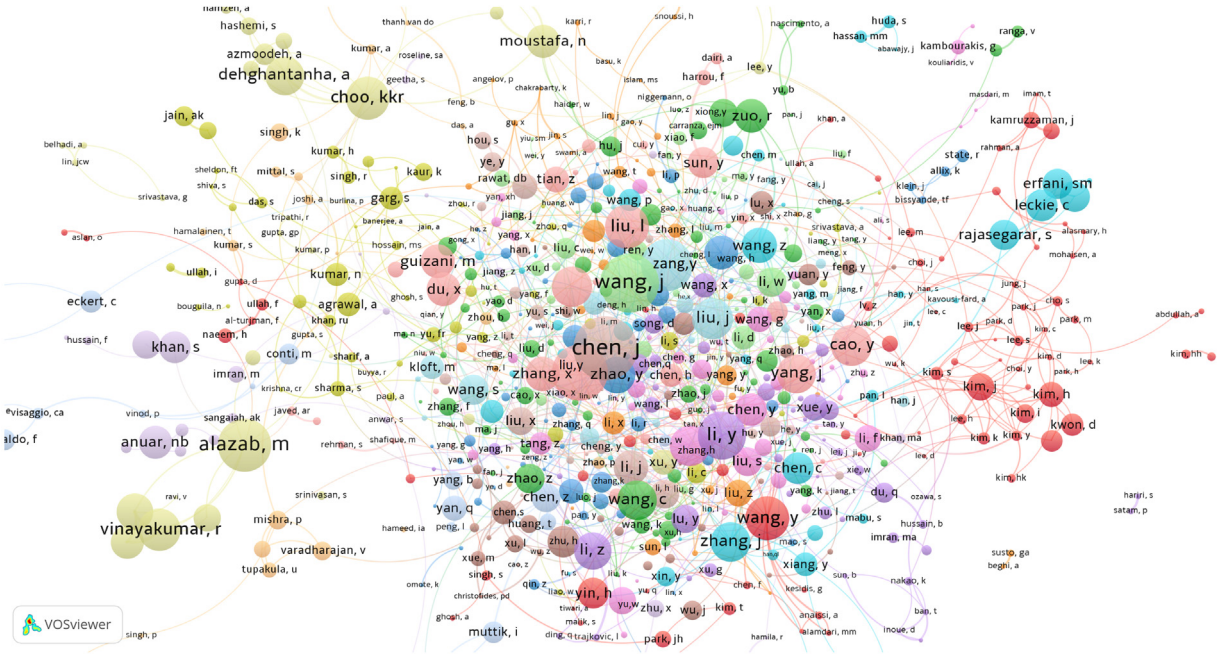

Fig. 12. Co-authorship network based on authors in the field of cyber-security and forensic (WoS) . (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

shows the number of cybersecurity and forensic papers published by the respective researchers in WoS. 'Links' indicates the number of co-author collaborations of a particular author with other researchers. Herein, if 'n' researchers co-authored an article, then the strength of link among each pair of co-authors was computed as 1/n. TLS indicates the sum of such link strengths of an author with all other co-authors over all published papers. The co-authorship based TLS is always a whole number (not a fraction) because the sum of fractional link strengths of a single author in any published article will always be one. Hence, the total co-authorship link strength of an author over all published articles will be equal to the number of such published articles (P). However, this phenomenon is not evident in Table 3, wherein the TLS is always a whole number but is always much lesser than the actual number of publications (P). This observation indicates that there are some published articles wherein there are no co-authors. It may also mean that some published articles included co-authors having less than 5 cybersecurity and forensic publications and/or 10 WoS citations themselves, thus getting omitted from the current analysis and not getting counted as co-authors. For instance, in case of the topmost TLS author Zhang Y, publications are 97 whereas TLS is 82. Hence, there are 15 articles authored by Zhang Y which either did not include any co-author or had such co-authors that have less than a total of 5 publications and/or 10 citations (individually). Similar observations may be made in case of TLS of other researchers as well. It is evident from Table 2 that among the top ten researchers with maximum TLS, four are from China. Australia, Singapore and USA are represented by two researchers each. Thus, the top ten list comprises of cyber security and forensic researchers from just four countries. It may be noted that Wang, Z (USA) has higher TLS (67) as compared to Zhang, X (Australia, TLS 64) inspite of having lesser number of co-author links (118 as compared to 130 of Zhang, X). This observation indicates that Wang, Z has more publications per co-author as compared to Zhang, X.

Fig. 12 shows the collaboration network map of cyber security and forensic researchers with their respective inter-linkages. This map highlights various network groups in different colors. The respective link strengths are depicted by corresponding thicknesses

Table 4
The top 13 countries with the maximum TLS.

Rank	Country	P	Links	TLS
1	USA	2157	68	768.00
2	China	1757	58	609.00
3	England	482	62	343.00
4	Australia	456	56	260.00
5	India	968	52	228.00
6	Saudi Arabia	271	50	201.00
7	Canada	407	47	193.00
8	Italy	400	52	183.00
9	Germany	378	50	173.00
10	France	268	45	142.00
11	Pakistan	202	39	142.00
12	South Korea	428	42	135.00
13	Spain	268	47	115.00

of links shown in the figure. The figure shows top TLS authors such as Wang Y (red node), Zhang J (blue node), Li Y (purple node), Wang J (light green node), Wang Z (blue node) and others in closely connected co-author networks.

4.2. Co-authorship analysis based on organizations

This subsection presents co-authorship analysis of cybersecurity research publishing organizations during the past decade. VoS search yielded a total of 6338 such organizations. The co-authorships among these institutions were analyzed using fractional counting method with a threshold of minimum 5 published documents and 10 citations per organization. Documents co-authored by more than 25 organizations were not considered. Only 798 organizations were found to satisfy these criteria. Of these, 757 were found to form the largest network of interconnected organizations. From this set of 757, the top ten organizations with highest co-authorship based TLS values are listed in

Table 3. In this table, 'P' shows the number of cybersecurity and forensic papers published by the respective organizations in WoS. 'Links' indicates the number of co-author collaborations of a particular institution with other organizations. Herein, if 'n' organizations co-authored an article, then the strength of link among each pair of co-authored organization was computed as 1/n. TLS indicates the sum of such link strengths of an organization with all other co-author institutions over all published papers. The co-authorship based TLS of organizations is always a whole number (not a fraction) because the sum of fractional link strengths of a single organization in any published article will always be one. Hence, the total co-authorship link strength of an organization over all published articles will be equal to the number of such published articles (P). However, this phenomenon is not evident in Table 3, wherein the TLS is always a whole number but is always much lesser than the actual number of publications (P). This observation indicates that there are some published articles wherein there are no co-authors from other organizations. It may also mean that some published articles included co-authors from only such organizations that had less than 5 cybersecurity and forensic publications and/or 10 WoS citations themselves, thus getting omitted from the current analysis and not getting counted as co-author organizations. For instance, in case of the topmost TLS organization Chinese Academy Science, publications are 159 whereas TLS is 142. Hence, there are 17 articles authored by the researchers of Chinese Academy Science which either did not include a co-author from any other organization or had co-authors from such organizations that had less than a total of 5 publications and/or 10 citations (individually). Similar observations may be made in case of TLS of other organization as well. Table 3 is also dominated by the Chinese organizations, claiming the first, second, fifth, seventh and ninth spots. The list also consists of three Australian universities and two institutions affiliated to the USA. There is one institutional representation each for Saudi Arabia, Singapore and Qatar.

Fig. 13 shows the collaboration network map of worldwide institutions involved in cyber security and forensic research, with their respective inter-linkages. Different colors are used in this figure to depict distinct research network groups. Relative thicknesses of connecting links depict respective link strengths among organizations. Organizations such as Chinese Academy Science, Beijing University of Posts and Telecommunications and the Tsinghua University are connected together in co-authorship linkages depicted in green color. Similarly, King Saud University is connected to Deakin University, University of Sydney and University of New South Wales in the brown colored co-authorship network. Many universities of the USA are connected in the red colored network, whereas the Nanyang Technological University forms an important node of the pink colored co-author network with Korea University, Seoul National University and others.

4.3. Co-authorship analysis based on countries

This subsection presents co-authorship analysis of cybersecurity research publishing nations during the past decade. VoS search yielded a total of 124 such nations. The co-authorships among these nations were analyzed using fractional counting method with a threshold of minimum 5 published documents and 10 citations per country. Documents co-authored by more than 25 nations were not considered. Only 79 countries were found to satisfy these criteria. Of these, the top ten cited sources with highest TLS values are listed in Table 4. Herein, if 'n' nations co-authored an article, then the strength of link among each pair of co-authored nation was computed as 1/n (due to the citing article). For instance, if ten nations co-authored an article, then the link strengths among

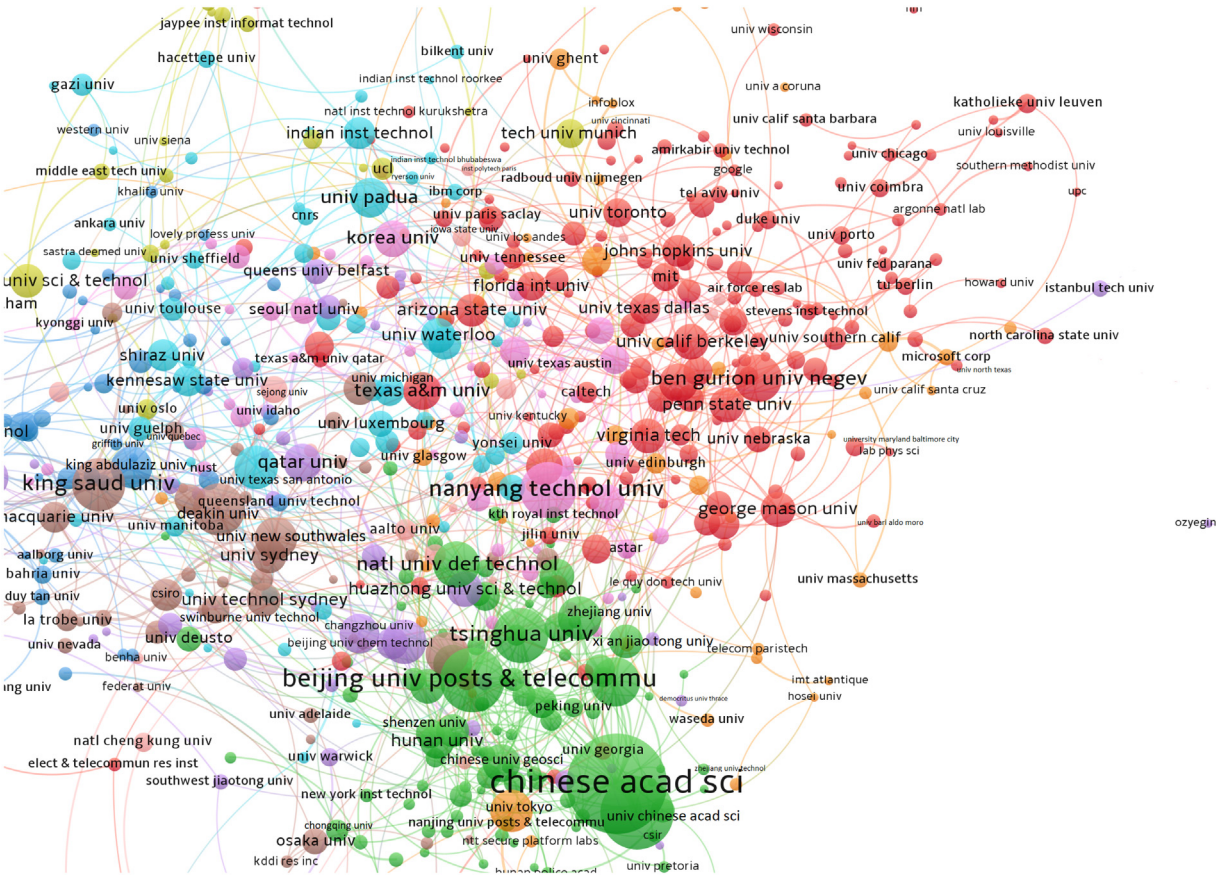

Fig. 13. Co-authorship network based on organizations in the field of cyber-security and forensic (WoS). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

each of them would be 1/10. TLS indicates the sum of such link strengths of a nation with all other co-author nations over all published papers. The co-authorship based TLS of nations is always a whole number (not a fraction) because the sum of fractional link strengths of a single nation in any published article will always be one. Hence, the total co-authorship link strength of a nation over all published articles will be equal to the number of such published articles (P). However, this phenomenon is not evident in Table 13, wherein the TLS is always a whole number but is always much lesser than the actual number of publications (P). This observation indicates that there are some published articles wherein there are no co-authors from other countries. It may also mean that some published articles included co-authors from only such countries that had less than 5 cybersecurity and forensic publications and/or 10 WoS citations themselves, thus getting omitted from the current analysis and not getting counted as co-author nations. For instance, in case of the topmost TLS country USA, publications are 2157 whereas TLS is only 768. Hence, there are 1389 articles authored by USA researchers and, either did not include a co-author from any other nationality or had co-authors from such nations that had less than a total of 5 publications and/or 10 citations (individually). Similar observations may be made in case of TLS of other countries as well.

The Table 4 shows the top thirteen nations with the maximum TLS metrics in the field of cybersecurity and forensic WoS publications. This list is topped by the USA and China with 2157 and 1757 publications during 2011–21, with 768 and 609 TLS respectively. India produced the third most publications (968) but claimed only the fifth highest TLS spot. This observation reveals comparatively lesser international co-author linkages of Indian authors as compared to those of researchers from England and Australia, which have higher TLS values in spite of lower publication outputs as compared to India. Hence, Indian authors can focus on enhancing international co-author linkages in proportion to their publication outputs. A similar observation can be made in case of the publication numbers and TLS of Saudi Arabia versus those of Canada, Italy and Germany. The Saudi Arabian authors produced only 271 articles, but included many more international co-authors per paper as compared to the researchers from Canada, Italy and Germany. Similar observation may be made in case of Pakistan, South Korea and Spain.

Fig. 14 shows the collaboration network map of the countries involved in cyber security and forensic research, with their respective inter-linkages. Different colors are used in this figure to depict distinct research network groups. Relative thicknesses of connecting links depict respective link strengths among different countries. The figure shows nations like USA, China, Singapore,

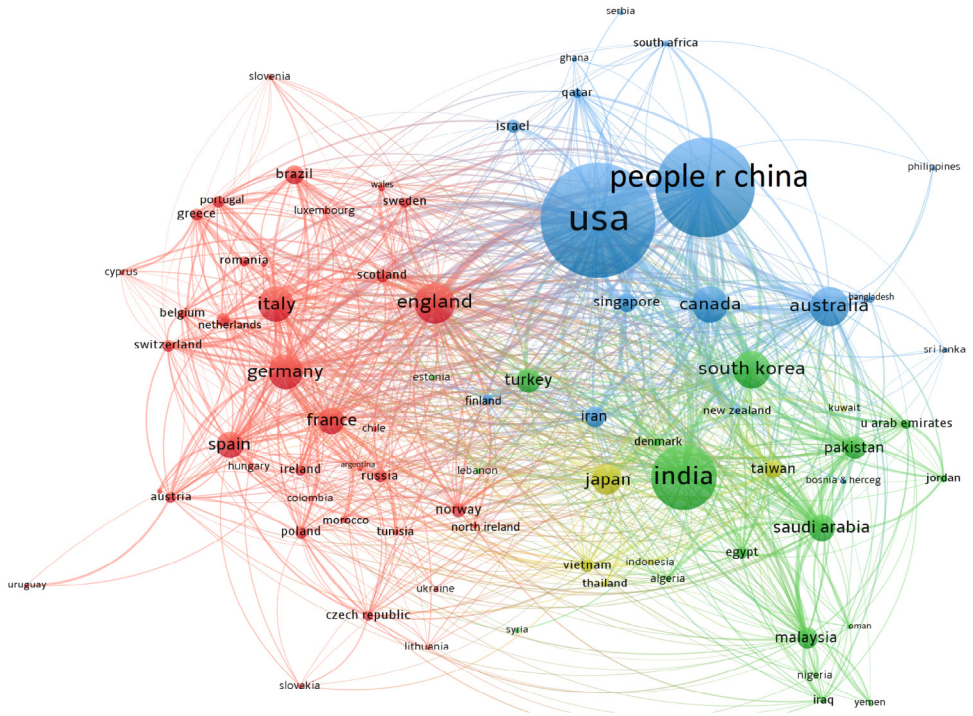

Fig. 14. Co-authorship network based on countries in the field of cyber-security and forensic (WoS). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Table 5
The top 13 keywords with the maximum co-occurrence TLS values for author Keywords.

Rank	Keyword	P	Links	TLS
1	Machine learning	2990	458	2707.00
2	Anomaly detection	2007	424	1823.00
3	Deep learning	1514	416	1393.00
4	Malware detection	553	224	530.00
5	Intrusion detection	465	299	443.00
6	Malware	435	258	423.00
7	Security	360	289	352.00
8	Feature extraction	340	308	337.00
9	Classification	275	194	268.00
10	Internet of things	256	230	249.00
11	Cyber security	263	221	247.00
12	Cybersecurity	220	214	217.00
13	Intrusion detection system	222	187	210.00

Canada and Australia connected together in blue-colored co-author networks. Similarly, India, South Korea, Saudi Arabia, Malaysia, Pakistan and Turkey form the green colored network. The red colored network is mostly formed by European nations such as Germany, England, France, Spain, Italy, Norway and others. Japan and Taiwan form the fewer nodes of the yellow colored network.

5. Co-occurrence analysis

This section gives details of the analyses carried out on the co-occurrences of various keywords mentioned in the cybersecurity and forensic articles published in the WoS.

5.1. Co-occurrence analysis based on author keywords

This subsection presents co-occurrence analysis of the keywords quoted by authors in cybersecurity research publications during the past decade. VoS search yielded a total of 15 515 such keywords. The co-occurrences among these keywords were analyzed using fractional counting method with a threshold of minimum 10 occurrences per keyword. Only 465 keywords were found to satisfy this criterion. Of these, the top ten c-occurring keywords with highest TLS values are listed in Table 5. This table showcases

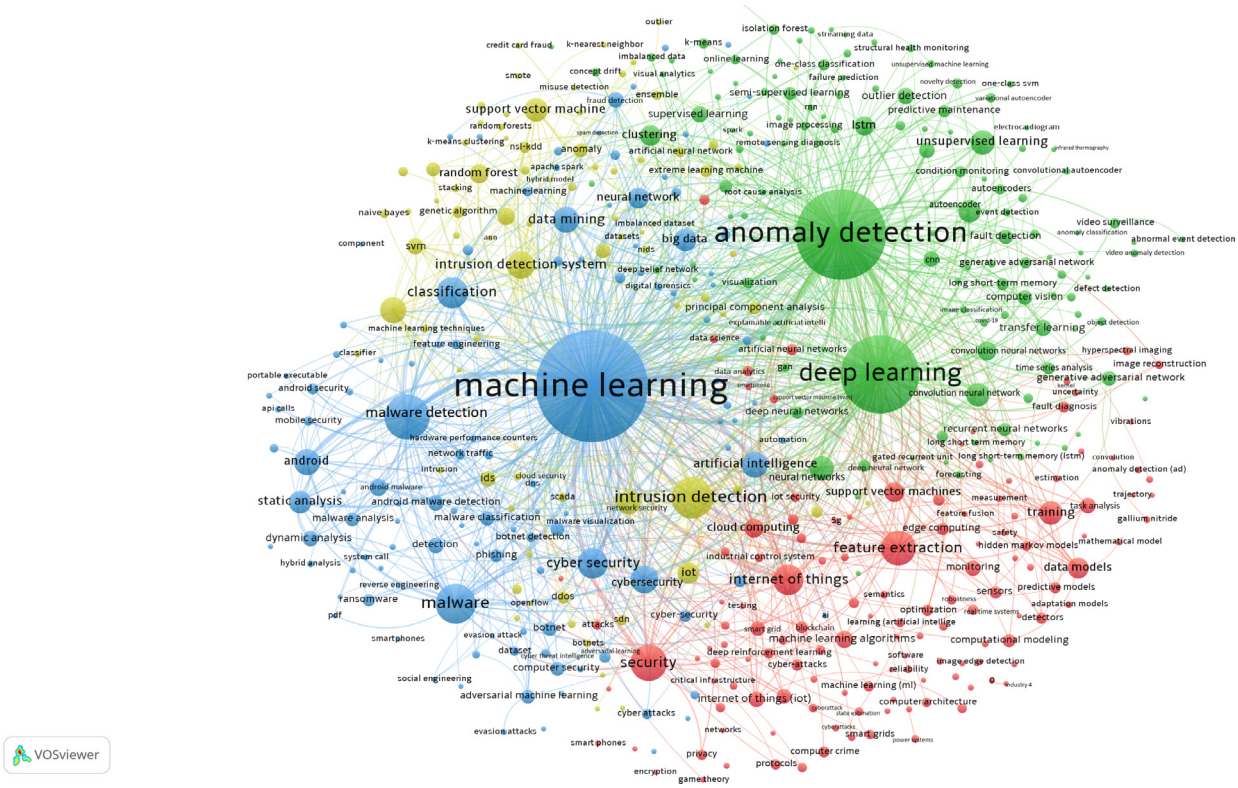

Fig. 15. Co-occurrence network of author keywords in the field of cybersecurity and forensics (WoS). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

the top thirteen keywords mentioned by researchers in their cybersecurity and forensics related research articles published in WoS. The list shows that the keyword 'machine learning' appeared in 2990 published articles (P). 'Machine learning' co-occurred with 458 other cyberforensic author-keywords in these articles. The TLS of 'machine learning' is 2707, which is the sum of the number of times 'machine learning' has co-occurred with each of the 458 other keywords (having minimum 10 occurrences). Herein, if 'n' author-keywords co-occurred an article, then the strength of link among each pair of co-occurred keywords was computed as 1/n (due to the citing article). For instance, if ten keywords co-occurred in an article, then the link strengths among each of them would be 1/10. TLS indicates the sum of such link strengths of a keyword with all other co-occurring keywords over all published papers. The co-occurrence based TLS of keywords is always a whole number (not a fraction) because the sum of fractional link strengths of a keyword in any published article will always be one. Hence, the total co-occurrence link strength of a keyword over all published articles will be equal to the number of such published articles (P). However, this phenomenon is not evident in Table 13, wherein the TLS is always a whole number but is always lesser than the actual number of publications (P). This observation indicates that there are some published articles wherein no other cybersecurity keyword has been mentioned by the authors. It may also mean that in some published articles only such cybersecurity keywords co-occurred that had less than 10 occurrences themselves, thus getting omitted from the current analysis and not getting counted as co-occurred keywords. For instance, in case of the topmost TLS keyword 'machine learning', publications are 2990 whereas TLS is 2707. Hence, there are 283 articles that mentioned this keyword and, either did not include any other cybersecurity WoS keyword or mentioned such keywords that had less than a total of 10 occurrences themselves (individually). Similar observation may be made in case of other author keywords as well. It may be noted in Table 5 that the fifth ('intrusion detection') and the thirteenth ('intrusion detection system') keywords are similar. Fourth ('malware detection') and sixth ('malware') keywords are also similar to each other. The eleventh ('cyber security') and twelfth ('cybersecurity') keywords are exactly the same, except for the styling of the terminology. The top five keywords indicate the focus of most research articles — anomaly/malware/intrusion detection using machine/deep learning. It may be observed from this list that generally, higher number of occurrences correspond with higher TLS of the keywords. However, 'cybersecurity' has higher links (214) and TLS (217) despite appearing in lesser publications (220) as compared to 'intrusion detection system' (occurrences 222, links 187 and TLS 210).

Fig. 15 shows the co-occurrence network of author keywords in the field of cybersecurity and forensics. Author defined cybersecurity keywords such as 'machine learning', 'classification', 'malware detection', 'feature selection', 'data mining' and 'malware' co-occur together, with their co-occurrence networks depicted in blue color in Fig. 15. Similarly, the keywords 'anomaly detection', 'deep learning', 'model' and 'neural networks' form prominent nodes of the red colored co-occurrence network. The green

Table 6
The top 13 keywords with the maximum co-occurrence TLS values for all keywords.

Rank	Keyword	P	Links	TLS
1	Machine learning	2990	654	2844.00
2	Anomaly detection	2436	629	2308.00
3	Deep learning	1514	607	1456.00
4	Classification	761	531	738.00
5	Intrusion detection	660	457	646.00
6	Malware detection	604	345	581.00
7	Security	555	456	545.00
8	Malware	477	362	464.00
9	Feature extraction	340	440	338.00
10	Model	309	435	300.00
11	Intrusion detection system	288	309	282.00
12	Cyber security	273	332	263.00
13	Internet	264	356	260.00

colored co-occurrence network is composed of author-keywords such as ‘security’, ‘intrusion detection’, ‘intrusion detection system’, ‘internet of things’, ‘attacks’, ‘cybersecurity’ and more.

5.2. Co-occurrence analysis based on all keywords

This subsection presents co-occurrence analysis of the all keywords identified by WoS in cybersecurity research publications during the past decade. VoS search yielded a total of 18 708 such keywords. The co-occurrences among these keywords were analyzed using fractional counting method with a threshold of minimum 10 occurrences per keyword. Only 666 keywords were found to satisfy this criterion. Of these, the top ten c-occurring keywords with highest TLS values are listed in Table 6. This table showcases the top thirteen keywords indexed by WoS in cybersecurity and forensics related research publications. The list shows that the keyword ‘machine learning’ appeared in 2990 published articles (P). It co-occurred with 654 other cyberforensic WoS indexed-keywords in these articles. The TLS of ‘machine learning’ is 2844, which is the sum of the number of times this keyword has co-occurred with each of the 654 other keywords (having minimum 10 occurrences). Herein, similar to the case of author specified keywords, if ‘n’ WoS indexed-keywords co-occurred an article, then the strength of link among each pair of co-occurred keywords was computed as 1/n (due to the citing article). TLS indicates the sum of such link strengths of a keyword with all other co-occurring keywords over all published papers. The co-occurrence based TLS of keywords is always a whole number (not a fraction) because the sum of fractional link strengths of a keyword in any published article will always be one. Hence, the total co-occurrence link strength of a keyword over all published articles will be equal to the number of such published articles (P). However, this phenomenon is not evident in Table 13, wherein the TLS is always a whole number but is always lesser than the actual number of publications (P). This observation indicates that there are some published articles wherein no other cybersecurity keyword has been mentioned by the authors. It may also mean that in some published articles only such cybersecurity keywords co-occurred that had less than 10 occurrences themselves, thus getting omitted from the current analysis and not getting counted as co-occurred keywords. For instance, in case of the topmost TLS keyword ‘machine learning’, publications are 2990 whereas TLS is 2844. Hence, there are 146 articles that mentioned this keyword and, either did not include any other cybersecurity WoS keyword or mentioned such keywords that had less than a total of 10 occurrences themselves (individually). In case of the keyword ‘internet’, only four papers did not include any other cybersecurity keyword/included keywords that were not shortlisted as per the selected threshold. It may be noted in Table 13 that the fifth (‘intrusion detection’) and the eleventh (‘intrusion detection system’) keywords are similar. Fourth (‘malware detection’) and eighth (‘malware’) keywords are also similar to each other, as was the case in author keywords 5. The top five keywords indicate the focus of most research articles — anomaly and intrusion detection suing machine/deep learning based classification. It may be observed from this list that generally, higher number of occurrences correspond with higher TLS of the keywords. However, ‘malware detection’ has higher TLS (581) than ‘security’ (TLS 545) despite having lesser co-occurrence links (345) than ‘security’ (links 456). This observation indicates that ‘malware detection’ co-occurred with lesser keywords as compared to ‘security’, but co-occurred together in greater number of articles as compared to the co-occurring keywords network of ‘security’. Similar trends may be observed in case of ‘intrusion detection system’, ‘cyber security’ and ‘internet’.

Fig. 16 shows the co-occurrence network of all keywords in the field of cybersecurity and forensics. It shows a pictorial representation of how strongly the ‘machine learning’ keyword is connected to ‘malware’, ‘malware detection’ and ‘classification’ in its blue colored network. Similarly, strong linkages are evident among the keywords ‘anomaly detection’, ‘deep learning’, ‘algorithm’, ‘model’ and ‘neural networks’ among others in a red colored network. The green colored network shows relatively lesser prominent keywords (evident by the smaller keyword nodes) such as ‘intrusion detection’, ‘security’, ‘internet’ and ‘internet of things’ among many others.

6. Citation analysis

This section showcases the citations based networks among authors, countries, organizations, published documents and sources in the field of cybersecurity and forensics in the past decade.

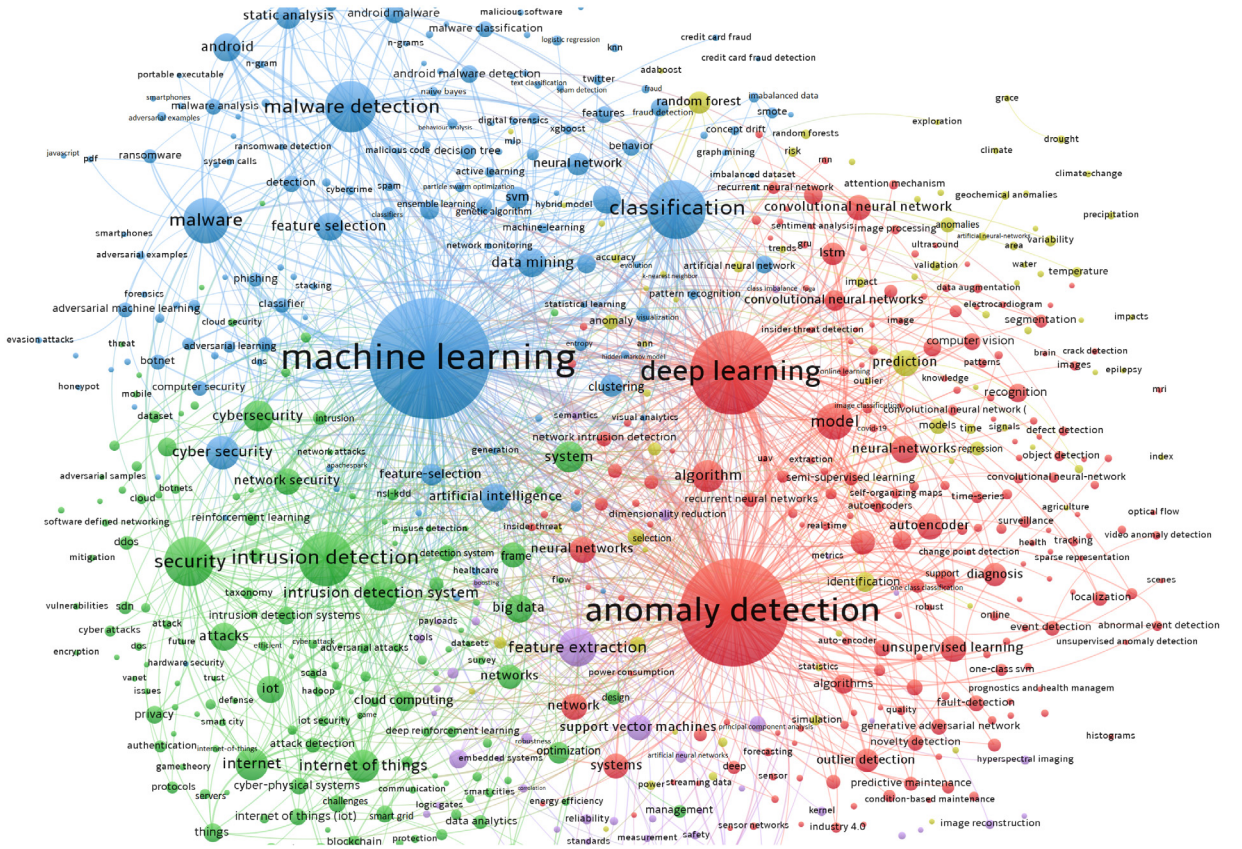

Fig. 16. Co-occurrence network of all keywords in the field of cyber-security and forensics (WoS) . (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

6.1. Citation analysis based on authors

This subsection presents citation analysis of cybersecurity research publishing authors during the past decade. VoS search yielded a total of 20 827 such authors. The citations of these authors were analyzed using a threshold of minimum 5 publications and 10 citations per author. Documents co-authored by more than 25 authors were not considered. Only 900 authors were found to satisfy these criteria. Of these, only 897 were found to compose the largest set of connected authors. The top ten cited authors (from the connected set) with highest TLS values are listed in Table 7. This table shows the top thirteen authors with the highest number of citations in cybersecurity and forensics research. This table also shows the number of citation links of each author, i.e. the number of unique researchers who cited a particular author's cybersecurity and forensic articles published in WoS. For instance, Chen J (Canada) published 43 cybersecurity and forensic articles in WoS during the last decade. These publications received 1301 citations from the published documents of 245 unique researchers (each having minimum 5 publications and 10 citations). In this way, each of these researchers established a citation based link with Chen J. The number of citations contained in such a link is its link strength. TLS of the cited author is the sum of strengths of all such citations based links. Table 7 is dominated by researchers affiliated to the USA, with as many as five authors making it to the top thirteen list. China is the next most represented country in this list, with three authors. Canada, Singapore, Australia and Saudi Arabia are represented by one author each. Interestingly, Li Y. placed seventh as per the citation counts (863) has the maximum TLS (1099) among all other researchers featuring in the list. Another interesting observation is that the author (Chen J.) with the most citations (1301) has the least TLS (432) among all authors in the list!

Fig. 17 shows the citations based networks among the international cybersecurity and forensics research community. Different citation networks are depicted in distinct colors viz. For instance, the author Li Y (TLS 1099) is connected to Liu L (TLS 498), Liu Y (TLS 813), Liu J (TLS 509) and Zhang Y (TLS 719) in a blue colored network. Alazab (TLS 764), Chen J (TLS 432) and Elovici (TLS 906) are located in the green red and yellow colored networks, respectively.

6.2. Citation analysis based on countries

This subsection presents citation analysis of cybersecurity research publishing countries during the past decade. VoS search yielded a total of 124 such nations. The citations of these nations were analyzed using a threshold of minimum 1 published document

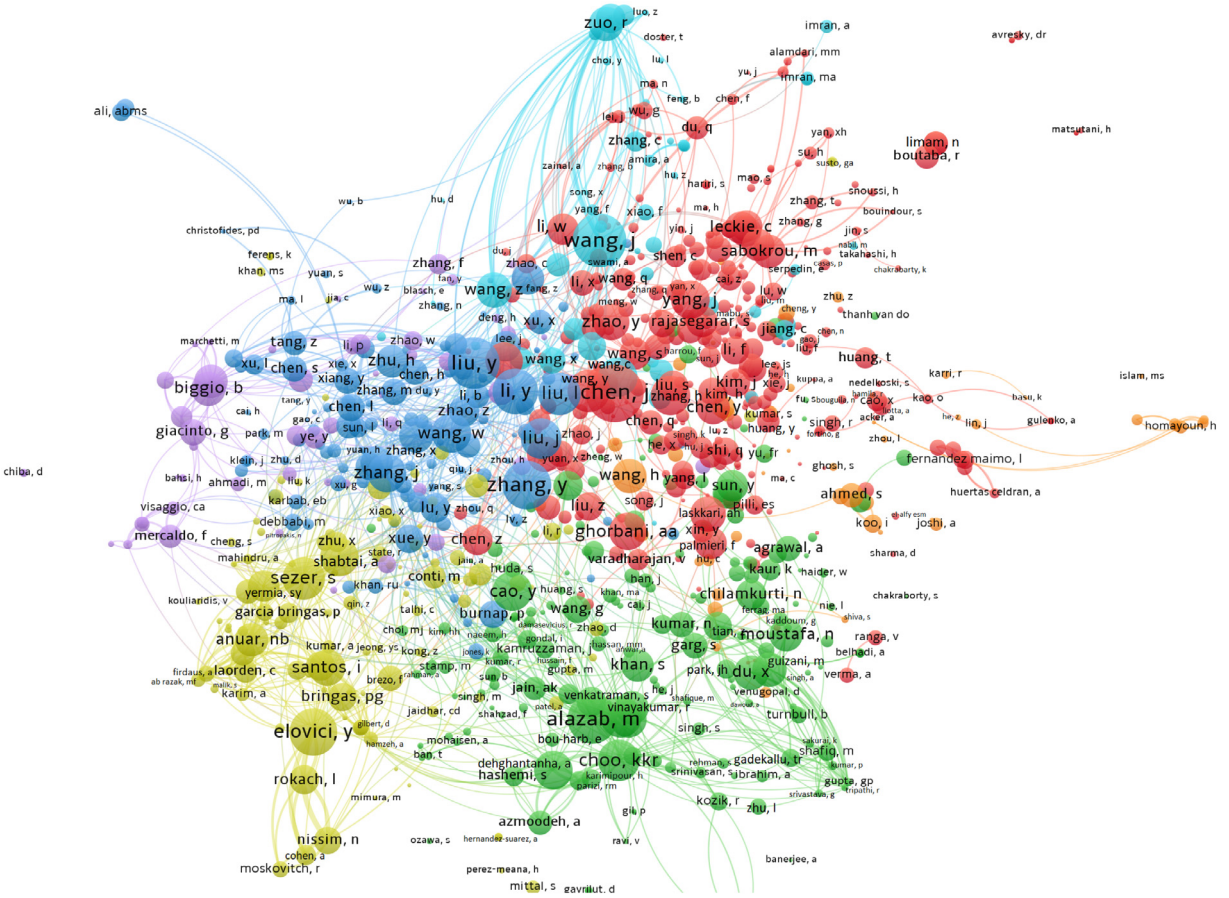

Fig. 17. Citation network based on authors from the international cybersecurity and forensics research community (WoS). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Table 7
The top 13 researchers with the highest citation TLS values.

Rank	Author	Country	P	Citations	Links	TLS
1	Chen, J	Canada	43	1301	245	432
2	Wang, J	USA	87	1140	364	902
3	Liu, Y	Singapore	75	1059	362	813
4	Alazab, M	Australia	28	991	267	764
5	Zhang, Y	China	97	955	346	719
6	Elovici, Y	Israel	27	926	305	906
7	Li, Y	China	87	863	406	1099
8	Liu, L	USA	38	753	291	498
9	Sezer, S	USA	18	749	293	903
10	Wang, Y	China	83	744	285	589
11	Choo, Kkr	USA	25	740	233	633
12	Vinayakumar, R	Saudi Arabia	23	716	216	623
13	Liu, J	USA	61	687	294	509

and 10 citations per nation. Documents co-authored by more than 25 nations were not considered. Only 79 countries were found to satisfy these criteria. From this set of 79, the top ten cited nations with highest TLS values are listed in Table 8. This table shows the top thirteen countries with the maximum citations based TLS values in the field of cybersecurity and forensics. This list shows the number of WoS papers published by the country, the number of citations received by such documents, the number of other unique countries from which these citations have originated (links) and the total strengths of all such citation based links (TLS of the cited country). This list is topped by China with 76 international citing linkages having a total link strength of 9709. The Chinese affiliated authors have published 1757 WoS papers in cybersecurity, obtaining 15 991 citations for them. These papers were cited by authors of 76 nations (citation links) shortlisted as per the threshold criteria mentioned above (minimum 1 published document and 10 citations per nation). USA has a similar number of international citing linkages (78) and TLS (9014) despite having much

Table 8
The top 13 countries with the maximum citation TLS values.

Rank	Country	P	Citations	Links	TLS
1	China	1757	15 991	76	9709
2	USA	2157	25 773	78	9014
3	India	968	6233	77	5571
4	Australia	456	7467	76	4705
5	England	482	6504	71	3926
6	Canada	407	5609	71	3116
7	South Korea	428	3352	70	2964
8	Saudi Arabia	271	2301	73	2882
9	Italy	400	4622	73	2510
10	Pakistan	202	2212	68	2336
11	Iran	180	2345	68	1876
12	Spain	268	2560	71	1827
13	Malaysia	180	1801	70	1705

higher citations (25 773) as compared to that of China (15 991). Similarly, India has higher TLS (5571) as compared to that of Australia (citations 7467, TLS 4705) despite having lesser citations (6233). It is notable that Australia has 7467 citations from just 456 papers as compared to India's 6233 citations from 968 publications. England also has a good number of citations (6504) from just 482 papers with good number of international citing linkages (71). However, its TLS is relatively lower (3926) as compared to that of India and Australia with similar citations and co-citation linkages. This observation implies that the number of English authored papers cited per individual international linkages is relatively lower than that of Indian and Australian papers. Iran and Malaysia have impressive number of international citing linkages (68 and 70 respectively) with comparatively lower number of papers (180 each) and citations (2345 and 1801 respectively).

Fig. 18 shows the citation network of the cybersecurity and forensic publishing nations. This figure shows two major networks depicted in green and red colored nodes and linkages. Red colored network is composed of countries with higher citation metrics including USA, China, India, Canada, South Korea and others. On the other hand, green colored network is made up of relatively lower citation metric nations such as Italy, Spain, France, Japan, Germany and others.

6.3. Citation analysis based on documents

This subsection presents citation analysis of cybersecurity research publications during the past decade. VoS search yielded a total of 9152 such publications. The citations of these documents were analyzed using a threshold of 10 citations per document. Only 1836 sources were found to satisfy this criterion. Of these, 1244 were found to compose the largest set of connected documents. From this set of 1244 connected sources, the top ten cited documents are listed in Table 9. This table also lists the number of citations based links of these articles i.e., the number of cybersecurity and forensic articles published in WoS and citing these articles. For instance, the paper titled 'Deep Walk: Online Learning of Social Representations' [51] obtained 1198 citations in total, of which only ten belonged to the cybersecurity and forensic articles published in the WoS and having minimum ten citations each. On the other hand, the article titled 'Andromaly: a behavioral malware detection framework for android devices' [56] attracted a total of 380 citations, 65 of them from cybersecurity and forensic WoS literature having minimum ten citations each. Fig. 19 shows the citation based networks of cybersecurity and forensic documents published in WoS, depicted in different colored nodes and linkages as per respective co-citations. For instance, the documents by Schlegl et al. [54], Pimentel et al. [52] and Khan [57] form the prominent nodes of the green colored citation network, whereas documents by Sharafaldin et al. [53] and Shone et al. [58] form the red colored network. Documents of Pei et al. [59], Rieck et al. [60] and Shabtai et al [56] form the prominent nodes of the purple, yellow and blue colored citation networks.

6.4. Citation analysis based on organizations

This subsection presents citation analysis of cybersecurity research publishing organizations during the past decade. VoS search yielded a total of 6338 such organizations. The citations of these organizations were analyzed using a threshold of minimum 5 published documents and 10 citations per organization. Documents co-authored by more than 20 organizations were not considered. Only 798 sources were found to satisfy these criteria. Of these, 794 were found to compose the largest set of connected sources. From this set of 794 connected sources, the top ten cited sources with highest TLS values are listed in Table 10. This table lists thirteen organization worldwide with the maximum citations based TLS in the field of cybersecurity and forensics. The list shows the number of publications (P), citations, number of unique citing organizations (links) and the total strengths of all such links (TLS) for an institution. This list is composed of four Chinese institutions, three Australian and one each from Saudi Arabia, USA, UK, Israel, Iran and Malaysia. The Chinese Academy Science tops the list with 159 papers, 1531 citations, 369 inter-institutional citation linkages and TLS 1090. This organization received 1531 citations from various organizations, of which only 369 were shortlisted in the current study as per the above mentioned criteria (minimum 5 published documents and 10 citations per organization). The TLS of 1090 is due to these 369 shortlisted organizations citing the works of the Chinese Academy Science. The Deakin University, Australia achieved the second highest position with a TLS of 952 from just 62 publications, owing to comparatively higher citations

Table 9
The top 10 WoS articles with maximum citation links.

Rank	Title of article	Authors	Year	Journal	Citations	Links
1	DeepWalk: Online learning of social representations [51]	Bryan Perozzi, Rami Al-Rfou, Steven Skiena	2014	Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining.	1198	10
2	A review of novelty detection [52]	Pimentel MA, Clifton DA, Clifton L, Tarassenko L	2014	Signal processing	671	37
3	Towards generating a new intrusion detection dataset and intrusion traffic characterization [53]	Sharafaldin, I., Lashkari, A.H. and Ghorbani, A.A	2018	ICISSP: proceedings of the 4th international conference on information,	518	40
4	Unsupervised anomaly detection with generative adversarial networks to guide marker discovery [54]	Schlegl, T., Seeböck, P., Waldstein, S.M., Schmidt-Erfurth, U. and Langs, G.,	2017	International conference on information processing in medical imaging	509	39
5	High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning [55]	Erfani, S.M., Rajasegarar, S., Karunasekera, S. and Leckie, C.,	2016	Pattern Recognition	400	40
6	"Andromaly": a behavioral malware detection framework for android devices [56]	Shabtai, A., Kanonov, U., Elovici, Y., Glezer, C. and Weiss, Y.,	2012	Journal of Intelligent Information Systems	380	65
7	A review on the application of deep learning in system health management [57]	Khan, S. and Yairi, T.	2018	Mechanical Systems and Signal Processing	361	3
8	A deep learning approach to network intrusion detection [58]	Shone, N., Ngoc, T.N., Phai, V.D. and Shi, Q.	2018	IEEE transactions on emerging topics in computational intelligence	344	39
9	Deepxplore: Automated whitebox testing of deep learning systems [59]	Pei, K., Cao, Y., Yang, J. and Jana, S.,	2017	Proceedings of the 26th Symposium on Operating Systems Principles	300	3
10	Automatic analysis of malware behavior using machine learning [60]	Rieck, K., Trinius, P., Willems, C. and Holz, T.	2011	Journal of Computer Security	282	26

Table 10
The top 13 organizations with the highest citation TLS values.

Rank	Organization	Country	P	Citations	Links	TLS
1	Chinese Academy Science	China	159	1531	369	1090
2	Deakin University	Australia	62	924	355	952
3	King Saud University	Saudi Arabia	64	1080	342	903
4	Tsinghua University	China	67	1436	347	868
5	The University of Texas at San Antonio	USA	48	852	272	798
6	Queen's University Belfast	United Kingdom	22	722	255	741
7	Ben-Gurion University of the Negev	Israel	53	1094	283	647
8	Beijing University of Posts and Telecommunications	China	84	1089	308	632
9	University of Chinese Academy of Sciences	China	101	738	260	614
10	Shiraz University	Iran	31	464	209	578
11	University of Malaya	Malaysia	26	989	255	574
12	Charles Darwin University	Australia	26	824	237	553
13	University of New South Wales	Australia	46	1011	249	551

(924) and inter-institutional citation linkages (355) per publication. The King Saud University published more papers (64) and attracted more citations (1080) than Deakin University, still it attained the third highest spot with TLS 903. This was due to its slightly lesser number of citation linkages (342) as compared to the Deakin University (355 links). Similarly, the Tsinghua University (China) also published more papers (67) and received lot more citations (1436), yet managed to attain fourth highest TLS (868). In this case, Tsinghua University had slightly better linkages (347) than King Saud University (342), but the individual strengths of the former's linkages proved to be lesser than the latter's. The most notable organization in this list is the Queens's University Belfast (United Kingdom), which is ranked sixth in the top citations based TLS rankings worldwide. The authors affiliated to this university published just 22 WoS papers which were cited by papers from 255 other organizations publishing in this field! The TLS of such citing organizations with Queen's University is 741, indicating that the cybersecurity and forensic publications of this university were cited by the articles of many other organizations per paper. Interestingly, the University of Malaya (ranked eleven) also published similar number of papers (26) and the same number of inter-organizational citation linkages (255) as the Queen's

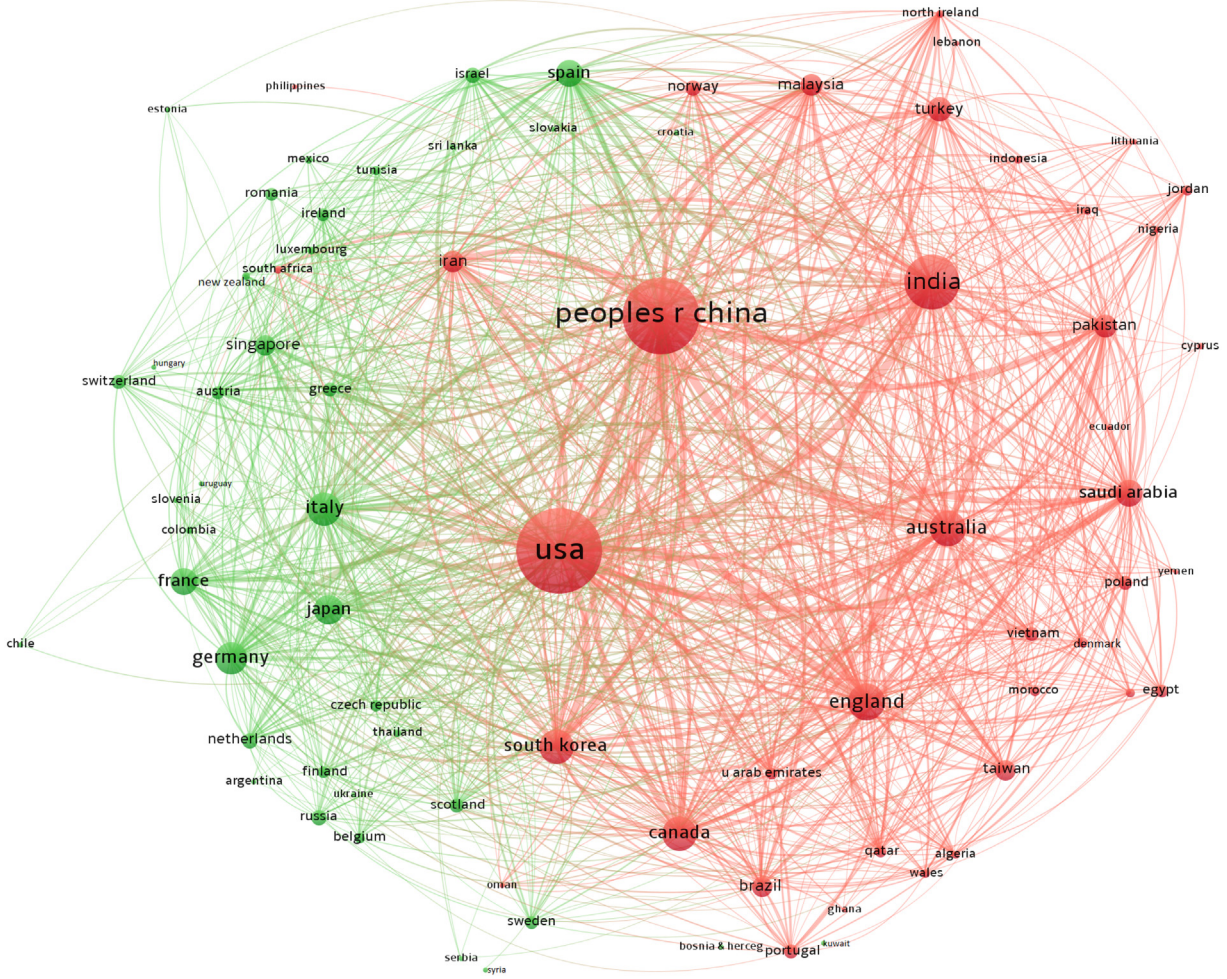

Fig. 18. Citation network of the cybersecurity and forensic publishing nations (WoS). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

University. However, the TLS of former is 574 as compared to 741 of the latter in spite of having higher citations (989) than the latter (722). The University of Malaya is a classic example of an institution having lesser cited articles per organizational linkage as compared to another (Queen's) with the same number of inter-organizational citation linkages.

Fig. 20 shows various worldwide institutional citation based linkages in the field of cybersecurity and forensics. Different citation networks are depicted in distinct colors. It may be observed that some of the topmost citation-TLS universities are connected together in the green colored network: Chinese Academy Science, Deakin University, Tsinghua University, Ben-Gurion University of the Negev, University of Malaya and the Queen's University Belfast. Other top citation TLS universities such as the Beijing University of Posts and Telecommunications (citation TLS rank 8), King Saud University (citation TLS rank 3) and the Charles Darwin University, Australia (citation TLS rank 12) form important nodes of the yellow colored network. Similarly, the University of New South Wales (citation TLS rank 13) and the University of Texas at San Antonio (citation TLS rank 5) form important nodes of the blue and purple colored networks respectively.

6.5. Citation analysis based on sources

This subsection presents citation analysis of cybersecurity research publishing sources during the past decade. VoS search yielded a total of 3730 such sources. The citations of these sources were analyzed using a threshold of minimum 5 published documents and 10 citations per source. Only 229 sources were found to satisfy these criteria. Of these, 227 were found to compose the largest set of connected sources. From this set of 227 connected sources, the top ten cited sources with highest TLS values are listed in Table 11. This table shows the top thirteen WoS publishing sources with the highest citations based TLS values. Similar to the TLS lists described in the previous subsections, this list also shows the number of publications (P), citations, citation based links (unique number of WoS sources citing articles of a particular journal) and the total strengths of all such links (TLS). This list is

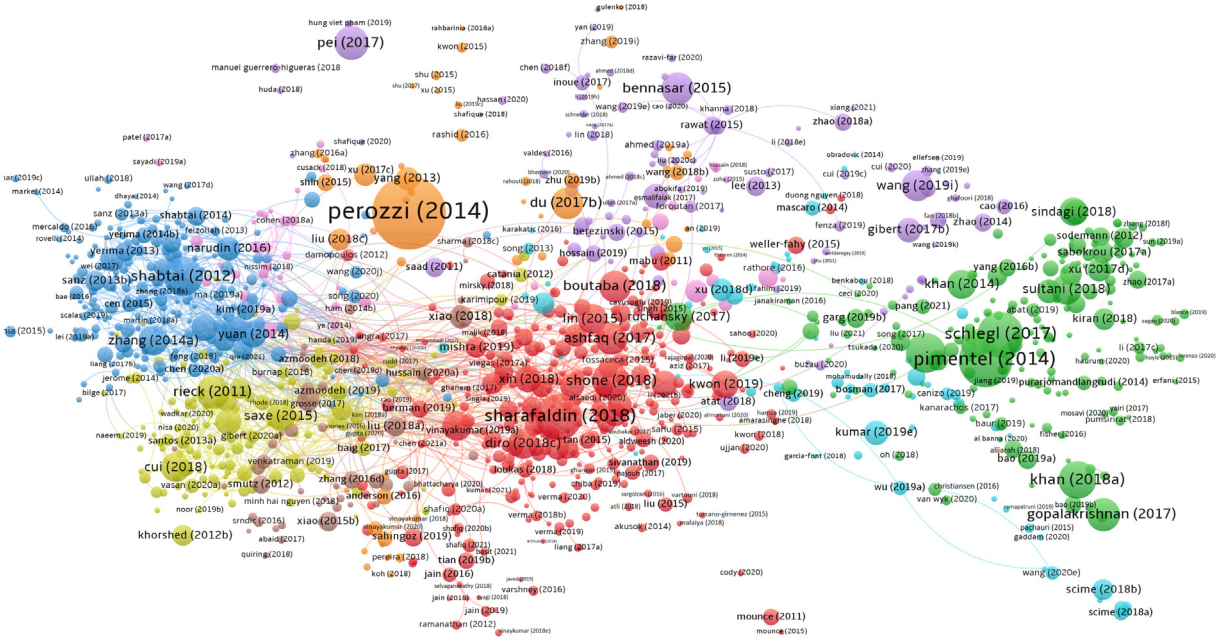

Fig. 19. Citation network among cyber-security and forensic documents published in WoS. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Fig. 20. Citation network based on organizations in the field of cyber-security and forensics (WoS). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

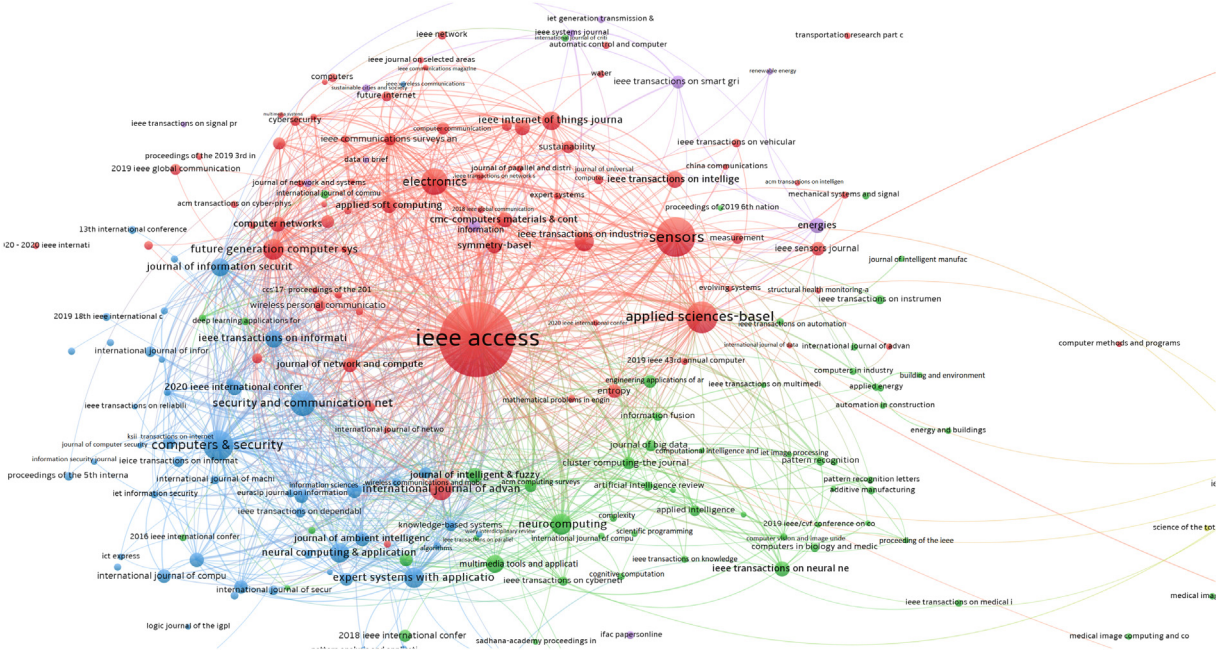

Fig. 21. Citation network based on sources in the field of cyber-security and forensics (WoS). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Table 11
The top 13 sources with the maximum TLS values.

Rank	Source	P	Citations	Links	TLS
1	IEEE Access	490	5095	177	2133
2	Computers & Security	96	1386	106	559
3	Electronics	78	375	95	425
4	Sensors	157	1018	113	420
5	Applied Sciences-basel	106	561	115	396
6	Future Generation Computer Systems -The International Journal of eScience	49	1146	95	376
7	Neurocomputing	51	1127	102	287
8	IEEE Communications Surveys and Tutorials	19	1193	82	284
9	Journal of Information Security and Applications	39	486	88	269
10	Security and Communication Networks	71	474	71	264
11	Information Sciences	26	1043	89	255
12	IEEE Transactions on Industrial Informatics	44	1191	83	245
13	Journal of Network and Computer Applications	26	512	75	236

topped by IEEE Access, which has published 490 articles related to cybersecurity and forensics. These articles have received 5095 citations from other WoS journals also publishing cybersecurity and forensic research. Of these citing sources, only a few satisfy the shortlisting criteria set in the current study (minimum 5 published documents and 10 citations per source). Thus, the sum of total citations received by IEEE Access from such 177 linked and shortlisted journals is 2133 (TLS). Computer and Security has the second best TLS of only 559, indicating the vastly significant citation TLS of IEEE Access in comparison to all other WoS sources. Hence, IEEE Access is depicted as the biggest node in source citation network map (Fig. 21), with other journals in its red colored network such as Electronics (TLS 425), Sensors (TLS 420), Applied Sciences-basel (TLS 396) and IEEE Transactions on Industrial Informatics (TLS 245). The blue colored source citation network is dominated by Computers and Security (TLS 559), Journal of Information Security and Applications (TLS 269) and Security and Communication Networks (TLS 264). Neurocomputing (TLS 287) is the most significant node in the green colored network of cybersecurity and forensic publishing WoS sources.

Table 12
The top 13 researchers with the highest co-citation TLS values.

Rank	Author	Country	Citations	Links	TLS
1	Chandola, V	USA	883	1910	867.8323
2	Lecun, Y	USA	811	2031	799.7607
3	Breiman, I	USA	780	1963	755.404
4	Kingma, DP	Netherlands	694	1780	681.5361
5	Hochreiter, S	Germany	579	1899	573.6133
6	Krizhevsky, A	Canada	562	1765	557.1928
7	Moustafa, N	Australia	573	1644	534.8279
8	Hinton, GE	Canada	532	1855	518.256
9	Goodfellow, I	USA	521	1943	517.5279
10	Wang, W	China	551	1853	515.3845
11	Zhang, Y	China	503	1932	488.7062
12	Scholkopf, B	Germany	476	1660	467.9065
13	Goodfellow, IJ	USA	465	1781	462.2123

7. Co-citation analysis

This section showcases the co-citations based networks among authors, documents and sources in the field of cybersecurity and forensics in the past decade.

7.1. Co-citation analysis based on cited authors

This subsection presents an analysis of cybersecurity research publishing authors co-cited during the past decade. VoS search yielded a total of 107 632 cited authors (first authors of published articles). The co-citations among these authors were analyzed using fractional counting method with a threshold of minimum 20 citations to be considered in the current study. Only 2269 authors were found to be cited 20 times or more. Of these, the top ten cited sources with highest TLS values are listed in Table 12. This table shows the list of authors with the highest co-cited TLS in the field of cybersecurity and forensics depicting author names, countries of affiliation, citations (number of individual citing documents), number of co-cited authors and the sum of total strength of each co-cited link (TLS). It is dominated by five researchers from the USA, followed by two authors each from China, Germany and Canada. Australia and Netherlands have been represented by one author each. Herein, if 'n' authors were co-cited by an article, then the strength of link among each pair of authors was computed as 1/n (in the citing article). If an author was co-cited twice (that is, two different articles of an author were cited by the same citing article), then the link strength with that co-author would be 2/n in that citing article. In this way, the total strength of all links over all citing documents for each article was computed and listed as TLS. This methodology implies that more the number of co-cited authors in an article, the lesser will be the individual co-cited link strengths in that article. Conversely, lesser the number of co-cited authors in an article, greater will be the co-cited link strengths as result of that article. For instance, Lecun Y has lesser TLS (799.7607) as compared to Chandola V (TLS 867.8323) because the former has higher co-cited links (2031) per citing document (total citations 811) as compared to the latter (1910 co-cited links over 883 citing documents). Similar occurrence may be observed in case of Hinton GE (TLS 518.256, links 1855, citations 532) and Moustafa N. (TLS 534.8279, links 1644, citations 573).

Fig. 22 depicts the co-citation network maps of the cybersecurity and forensic investigating authors. The figure shows top co-cited TLS authors like Chandola V (USA), Zhang Y (China), Scholkopf B (Germany) and Breiman I (USA) forming the yellow colored network. Lecun Y (USA), Hinton GE (Canada), Hochreiter S (Germany) and Krizhevsky A (Canada) form the prominent nodes of the red colored network. Wang W (China) and Moustafa *N* (Australia) denote the most important nodes of the blue and green colored networks respectively.

7.2. Co-citation analysis based on cited references

This subsection presents co-citation analysis of cybersecurity research papers cited by WoS documents during the past decade. VoS search yielded 199 584 cited cybersecurity research documents. These documents were analyzed using the fractional counting method with a threshold of minimum 20 citations to be considered in the current study. Only 1141 documents were found to be cited 20 times or more. Of these, the top ten cited documents with highest TLS values are listed in Table 13. This table shows the list of documents with top co-cited TLS values based on citations from cybersecurity and forensic related WoS publications in the last decade. This list depicts document titles, authors, year of publication, name of publishing journal, citations (number of individual citing documents), number of co-cited documents (links) and the sum of total strength of each co-cited link (TLS). Herein, if 'n' documents were co-cited by an article, then the strength of link among each pair of co-cited documents was computed as 1/n (due to the citing article). For instance, if ten documents were co-cited by an article, then the link strengths among each of them would be 1/10. TLS indicates the sum of such link strengths of a cited document with all other co-cited documents over all citing papers. The co-citations based TLS of cited documents is always a whole number (not a fraction) because the sum of fractional link strengths of a cited document in any citing article will always be one. Hence, the total co-citation link strength of a cited document over all citing articles will be equal to the number of such citing articles, i.e., the number of citations of that cited document. However, this

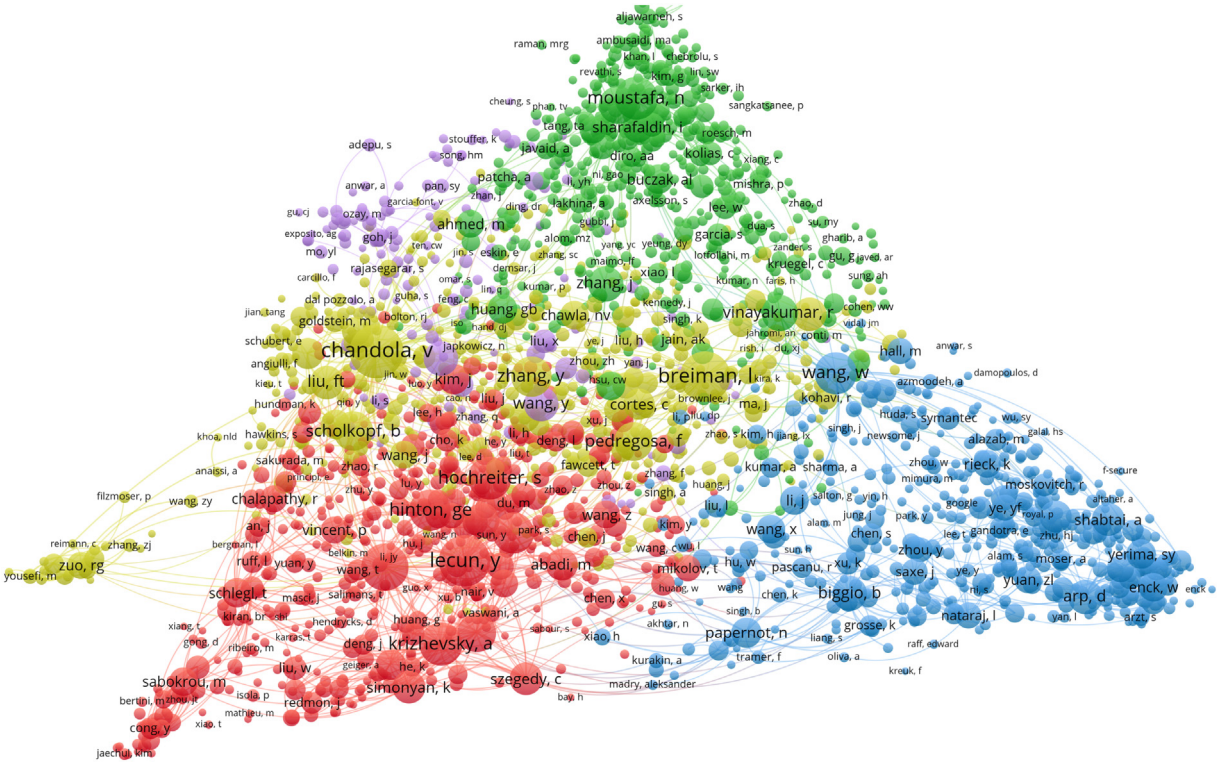

Fig. 22. Co-citation network map of the cyber-security and forensic investigating authors (WoS). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

phenomenon is not evident in Table 13, wherein the TLS is always a whole number but is always lesser than the actual number of citations. This observation indicates that there are some citing articles wherein no other cybersecurity paper has been co-cited. It may also mean that some citing articles co-cited only such cybersecurity papers that had less than 20 citations themselves, thus getting omitted from the current analysis and not getting counted as co-cited articles. For instance, in case of the topmost TLS document by Chandola et al. [61], citations are 796 whereas TLS is 750. Hence, there are 46 articles that cited this document [61] and, either did not cite any other cybersecurity WoS paper or cited such papers that had less than a total of 20 citations themselves (individually). Similar observation may be made in case of the document by Tavallaee et al. [62], with tenth highest TLS of 261 and 262 citations. Herein, only one citing document did not refer any other cybersecurity paper or cited such cybersecurity documents with less than 20 citations each.

Fig. 23 depicts the co-citation network maps of the cybersecurity and forensic investigating documents. The figure shows top co-cited TLS documents such as Chandola et al. [61], Hochreiter et al. [63], Krizhevsky et al. [64] and Goodfellow et al. [65] connected in red colored co-cited network. Breiman [66] forms a prominent node of the yellow colored network, whereas other co-cited documents are shown connected in green, purple and blue colored networks.

7.3. Co-citation analysis based on cited sources

This subsection presents an analysis of cybersecurity research publishing WoS journals co-cited during the past decade. VoS search yielded 71 119 such cited journals. These journals were analyzed using fractional counting method with a threshold of minimum 20 citations to be considered in the current study. Only 1940 sources were found to be cited 20 times or more. Of these, the top ten cited sources with highest TLS values are listed in Table 14. This table shows the list of WoS journals with top co-citations based TLS values indicating source names, WoS citations, the number of individual co-cited journals (links) and the sum total of their respective strengths (TLS). In this case, if articles of 'n' journals were co-cited by a citing document, then the strength of link among each pair of journals was computed as 1/n (due to the citing article). If 'm' articles of the same journal were co-cited by the citing article (with cited articles from other journals as well), then the link strength of each cited source with the multi-cited journal would be m/n in that citing article. In this way, the total strength of all co-cited links over all citing documents for each publishing source was computed as TLS of that source. This methodology implies that more the number of articles from the same journals co-cited in a citing document, the higher will be their individual co-cited link strengths due to that article. However, since the number of co-cited articles belonging to different sources (n) is generally higher than the number of co-cited articles belonging to the same journal (m), hence the TLS values of sources is generally lower than their total citations (citations is a function of 'm', whereas TLS

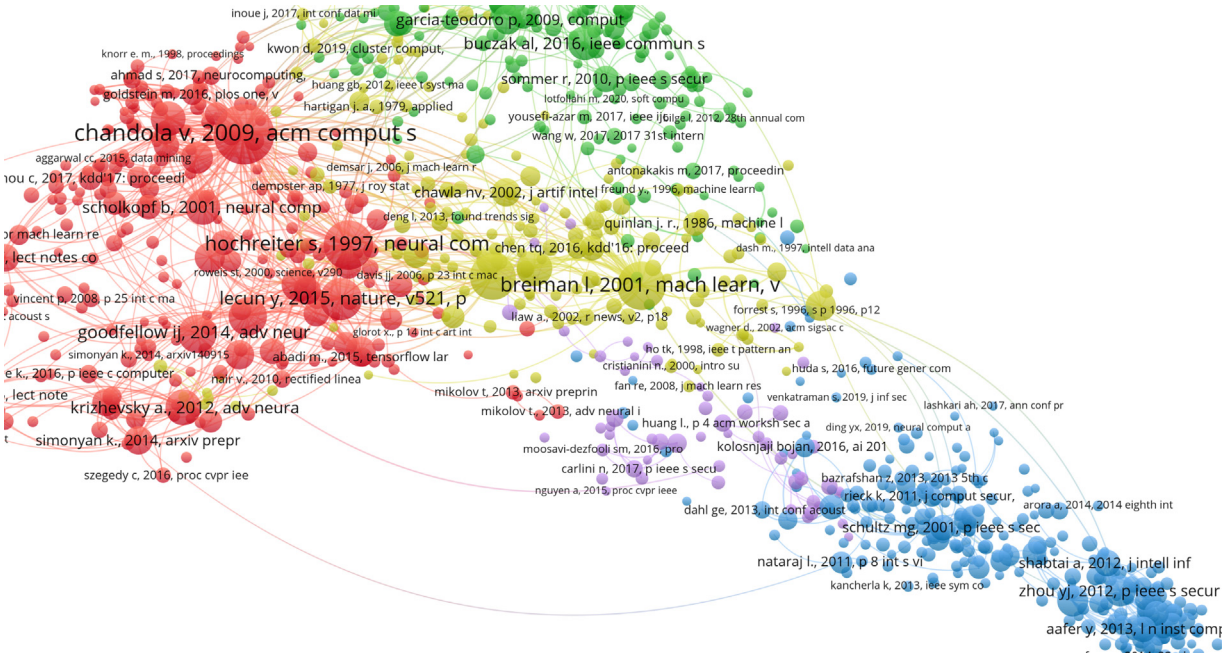

Fig. 23. Co-citation network based on cited references in the cyber-security and forensic field (WoS).

Table 13
The top 10 WoS articles with maximum co-citation TLS.

Rank	Paper title	Authors	Year	Journal name	Citation	Link	TLS
1	Anomaly detection: A survey [61]	Chandola, Varun, Arindam Banerjee, and Vipin Kumar	2009	ACM computing surveys	796	910	750.00
2	Long short-term memory [63]	Hochreiter, Sepp, and Jürgen Schmidhuber	1997	Neural computation	526	966	504.00
3	Random forests [66]	Breiman, Leo	2001	Machine Learning	521	950	498.00
4	Scikit-learn: Machine learning in Python [67]	Pedregosa, Fabian, Gaël Varoquaux, Alexandre Gramfort, Vincent Michel, Bertrand Thirion, Olivier Grisel, Mathieu Blondel et al.	2011	The Journal of machine Learning research	455	919	415.00
5	Deep learning [68]	LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton	2015	Nature	382	917	371.00
6	Generative adversarial nets [65]	Goodfellow, Ian, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio	2014	Advances in neural information processing systems	331	833	322.00
7	Adam: A Method for Stochastic Optimization [69]	Diederik Kingma, Jimmy Ba	2015	Proceedings of the 3rd international conference for learning representations	322	813	317.00
8	Support-vector networks [70]	Cortes, Corinna, and Vladimir Vapnik.	1995	Machine learning	280	842	270.00
9	Imagenet classification with deep convolutional neural networks [64]	Krizhevsky, Alex, Ilya Sutskever, and Geoffrey E. Hinton.	2012	Advances in neural information processing systems	277	750	267.00
10	A detailed analysis of the KDD CUP 99 data set [62]	Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani.	2009	n 2009 IEEE symposium on computational intelligence for security and defense applications	262	681	261.00

is a function of m/n/). Table 14 shows that the number of co-cited links may be lesser (TLS ranks 1–9), equal to (TLS rank 10) or greater (TLS ranks 12,13) than the number of total source citations. Lesser links than citations implies co-citations coming from

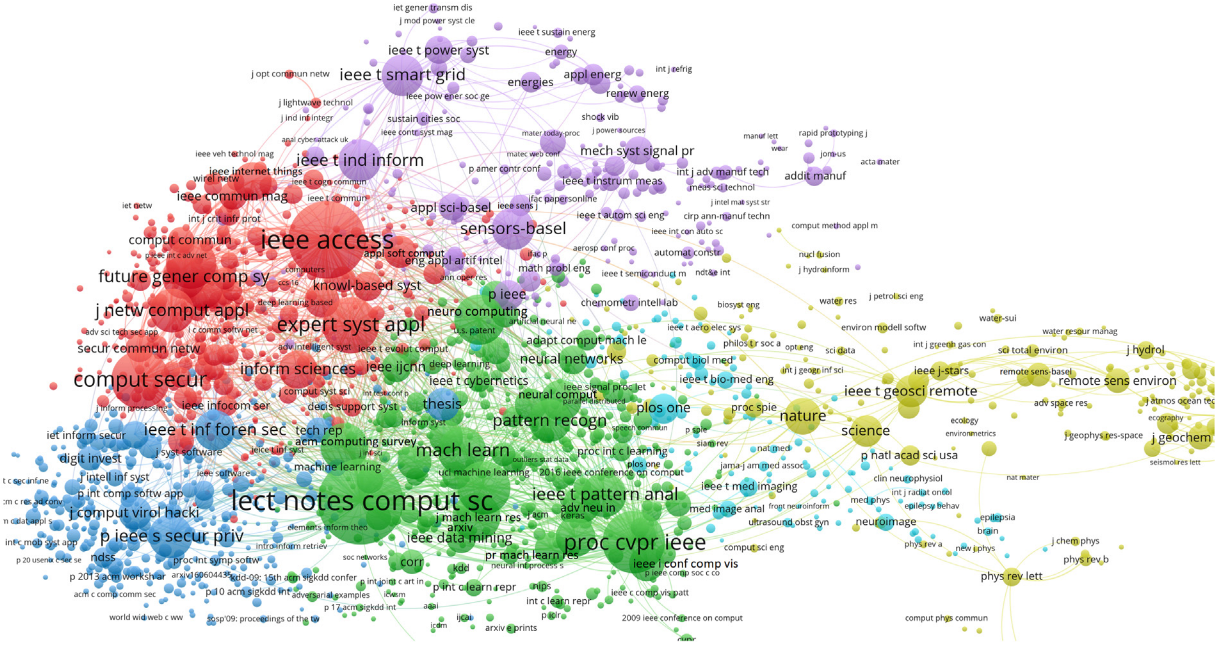

Fig. 24. Co-citation network based on cited sources in the cyber-security and forensic field (WoS). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Table 14
The top 13 Sources with the highest co-citation TLS values.

Rank	Sources	Citations	Link	TLS
1	Lecture notes in computer science	6109	1927	5680.4689
2	IEEE Access	5057	1904	4648.9634
3	Proceedings conference on computer vision and pattern recognition IEEE	3296	1777	2860.4096
4	Computers & Security	2846	1710	2710.8824
5	Expert systems with applications	2665	1883	2503.4892
6	Journal of machine learning research	2375	1919	2316.677
7	Neurocomputing	2129	1875	2054.5846
8	IEEE communications surveys and tutorials	2143	1685	2048.8988
9	Machine learning	1949	1906	1901.3627
10	ACM computing surveys	1875	1875	1850.0171
11	arXiv preprint arXiv	1941	1861	1820.5568
12	IEEE transactions on pattern analysis and machine intelligence	1695	1842	1632.0281
13	Journal of network and computer applications	1601	1704	1554.646

comparatively lower number of select sources. Greater links than citations indicates articles from larger number of varied sources being co-cited. Links equal to citations for a journal shows that the number of co-cited sources is exactly equal to the total number of citations received by the articles of that particular journal.

Fig. 24 depicts the co-citations based networks among different WoS publishing sources in distinct colors. The red colored network is predominated by top co-citation TLS journals such as IEEE Access, Expert Systems With Applications, Computers and Security and the Journal of Network and Computer Applications. Sources such as the Lecture Notes in Computer Science, Proceedings Conference on Computer Vision and Pattern Recognition IEEE, Machine Learning, IEEE Transactions on Pattern Analysis and Machine Intelligence and Neurocomputing form their own co-cited network depicted in green color. Other sources such as Sensors-basel and Nature form prominent nodes in the purple and yellow colored distinct networks, respectively.

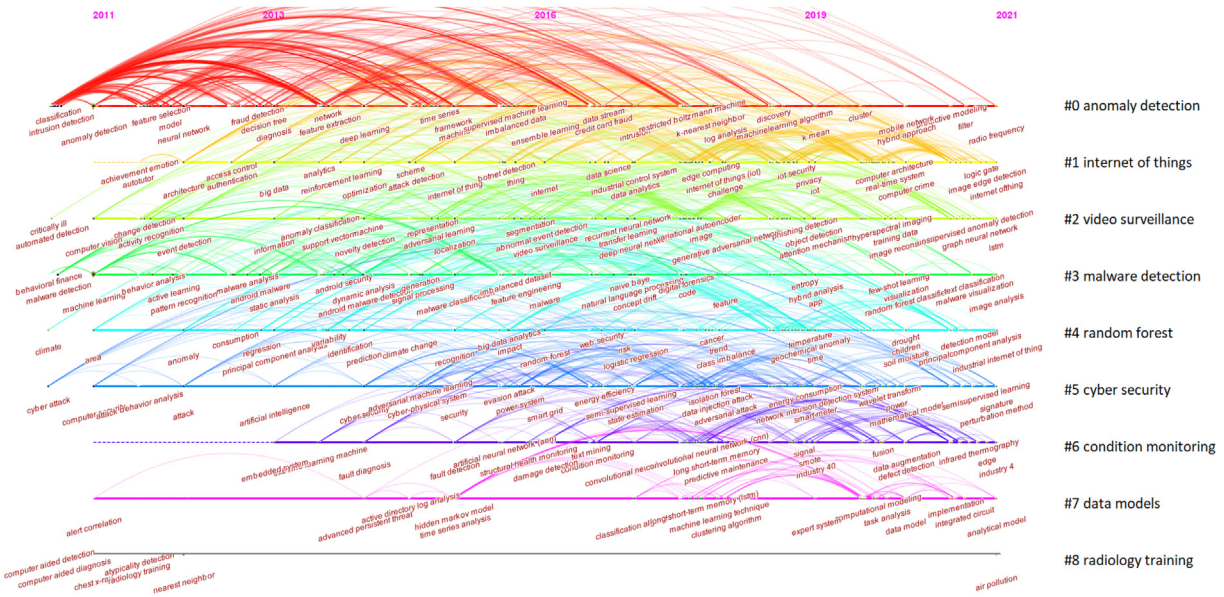

Fig. 25. Timeline view of keywords (WoS).

8. Timeline analysis and burst detection

This section presents the results of timeline review and burst detection analyses obtained from CiteSpace tool. The timeline review analysis indicates the evolution of research trends in the field of cybersecurity and forensics over the selected period (2011–2021). On the other hand, burst detection analyses reveal the documents/keywords that witnessed a sudden spike in citations in a certain time period. These analyses also indicate the strengths of such bursts and are helpful to understand the relative temporal importance given to certain documents/keywords by the research community.

8.1. Timeline review analysis

The timeline analysis results for cybersecurity and forensic research during 2011–2021 (as obtained from the CiteSpace) are shown in Fig. 25. This figure shows trend timelines of nine topic clusters, marked in distinct colors. It is evident from the figure that the topic of anomaly detection attracted maximum research attention during first half of the previous decade i.e. 2011–2016. Its importance has gradually reduced since 2016. On the other hand, topic clusters such as internet of things, video surveillance, malware detection and random forest have sustained researchers' interest over major part of the past ten years. Cybersecurity, condition monitoring and data models have started gaining prominence in the last 3–4 years. Radiology training has not received adequate attention and is an open research area for cybersecurity and forensic investigators.

8.2. Keyword burst detection

This subsection details upon the burst detection analysis carried out for cybersecurity and forensic keywords during the last decade. Table 15 shows the top 15 keywords arranged in the descending order of their respective burst strengths. The keywords 'malware detection', 'data mining' and 'support vector machine' obtained the highest burst strengths of 28.80, 24.19 and 24.16 during 2012–18, 2011–17 and 2011–16 respectively. These three keywords witnessed citation bursts for the maximum number of years. Other keywords such as 'intrusion detection' and 'algorithm' also witnessed bursts right from the beginning of the decade in 2011 up to 2015 with respective strengths of 10.97 and 6.19. Most of the remaining keyword bursts occurred in the middle part of the decade viz. 'static analysis' (2013–18), 'decision tree' (2013–18), 'extreme learning machine' (2014–18), 'intrusion detection system' (2013–16), 'mobile malware' (2013–16) and 'mobile security' (2014–17). A few keywords such as 'machine learning', 'feature selection' and 'traffic classification' experienced very short bursts of just one year i.e. 2016–17, 2014–15 and 2015–16 respectively. The latest keyword burst occurred in 2018–19 in 'deep neural network' with a strength of 8.04. This analysis clearly indicates a shift towards deep networks among the cybersecurity and forensic research community.

8.3. References burst detection

This subsection presents the burst detection analysis carried out for cybersecurity and forensic documents cited during the last decade. Table 16 shows the top 15 research articles arranged in the descending order of their respective burst strengths. The article

Table 15
The top 15 keywords with the strongest citation burst.

Rank	Keywords	Year	Strength	Begin	End	2011–2021
1	Malware detection	2011	28.80	2012	2018	
2	Data mining	2011	24.19	2011	2017	
3	Support vector machine	2011	24.16	2011	2016	
4	Machine learning	2011	17.33	2016	2017	
5	Static analysis	2011	14.90	2013	2018	
6	Decision tree	2011	11.46	2013	2018	
7	Intrusion detection	2011	10.97	2011	2015	
8	Feature selection	2011	9.10	2014	2015	
9	Extreme learning machine	2001	8.39	2014	2018	
10	Deep neural network	2011	8.04	2018	2019	
11	Intrusion detection System	2011	6.25	2013	2016	
12	Algorithm	2011	6.19	2011	2015	
13	Mobile malware	2011	5.85	2013	2016	
14	Mobile security	2011	5.20	2014	2017	
15	Traffic classification	2011	5.09	2015	2016	

Table 16
The top 15 References with the strongest citation burst.

Rank	References	Year	Strength	Begin	End	2011–2021
1	Goodfellow IJ, 2014, Adv Neur In, V27, P2672 [65]	2014	45.43	2018	2019	
2	Zhou YJ, 2012, P IEEE S Secur Priv, V0, P95 [72]	2012	43.19	2013	2017	
3	Srivastava N, 2014, J Mach Learn Res, V15, P1929 [76]	2014	33.81	2017	2019	
4	Kingma DP, 2015, Proc Int C Learning, V0, P0 [77]	2015	33.65	2019	2021	
5	Lecun Y, 2015, Nature, V521, P436 [68]	2015	33.51	2017	2019	
6	Shabtai A, 2012, J Intell Inf Syst, V38, P161 [56]	2012	31.48	2013	2017	
7	Aafer Y, 2013, L N Inst Comp Sci So, V127, P86 [73]	2013	31.38	2014	2018	
8	Chandola V, 2009, ACM Comput Surv, V41, P0 [61]	2009	31.05	2011	2014	
9	Chang CC, 2011, ACM T Intel Syst Tec, V2, P0 [74]	2011	29.60	2012	2016	
10	Arp D, 2014, 21st Annual NDSS Symposium, V0, P0 [78]	2014	26.11	2016	2019	
11	Santos I, 2013, Inform Sciences, V231, P64 [71]	2013	26.00	2013	2018	
12	Bhuyan MH, 2014, IEEE Commun Surv Tut, V16, P303 [75]	2014	23.11	2015	2019	
13	Wu DJ, 2012, Asia Jt Conf Inf Sec, V0, P62 [79]	2012	22.45	2014	2017	
14	Simonyan K, 2014, Arxiv Preprint Arxiv, V0, P0 [80]	2014	22.38	2017	2019	
15	Grace M, 2012, P Int C Mob Syst App, V0, P281 [81]	2012	20.68	2014	2017	

published by Goodfellow et al. [65] obtained the highest burst strength of 45.43 during the shortest time period of one year, i.e. 2018–19. It is interesting to note that this publication witnessed the above mentioned burst four years after its publication. On the other hand, the article published by Santos et al. [71] in 2013 immediately experienced a citation burst (strength 26.00) than continued for the longest period of five years as compared to all other documents, i.e. 2013–18. Articles by Zhou et al. [72], Shabtai et al. [56], Aafer et al. [73], Chang et al. [74] and Bhuyan [75] witnessed citation bursts one year after their respective years of publications. Interestingly, all these articles retained their respective citation bursts for a period of four years each. The latest citation burst is observed for the document published by Srivastava [76] which was published in 2014 but witnessed burst during 2017–19 with the third highest strength of 33.81.

9. Conclusions and future directions

The current study presents an extensive bibliometric analysis of various aspects of cybersecurity and forensic research published over the past decade. This paper firstly presented analysis of yearly publications, types of publications, sources, organizations, researchers, countries and areas. Secondly, the above mentioned detailed analysis was carried out from co-authorship, co-occurrence, citation and co-citation perspectives. Fractional counting method was followed for co-authorship, co-citation and co-occurrence analyses. Finally, timeline and burst detection results were discussed to identify the temporally most trending keywords and documents. The primary findings of the current study are listed as follows -

1. More than 2000 cybersecurity and forensics related publications occur every year in WoS
2. Majority of these publications is composed of research papers (51.19%)
3. The journal IEEE Access published the most cybersecurity and forensic articles (490) in WoS
4. Chinese Academy of Science published maximum articles (203)
5. Wang, Yong (China) published the maximum papers (40) in cybersecurity and forensics as the first author

6. Researchers from USA published maximum articles till 2020, followed by maximum publications by Chinese authors in 2021
7. Computer science is the most popular research area with maximum cybersecurity publications (6245)
8. Most of the WoS cybersecurity and forensic publications (4258) belong to the Conference Proceedings Citation Index.
9. Most of the WoS cybersecurity and forensic publications belong to the subject category of 'engineering electrical electronic'
10. Zhang Y (China) has the highest co-authorship based TLS of 82 with 158 co-author linkages
11. Chinese Academy Science has the highest co-authorship based TLS of 142 having co-author linkages with 100 other organizations
12. USA has the highest co-authorship based TLS of 768 having co-author linkages with 68 other nations
13. Machine learning has the highest co-occurrence based TLS of 2707 having linkages with 458 other author defined cybersecurity and forensic keywords
14. Machine learning also has the highest co-occurrence based TLS of 2844 having linkages with 654 other author defined WoS indexed keywords
15. Chen J (Canada) has the highest citation based TLS of 432 having citation linkages with 245 cybersecurity and forensic researchers
16. China has the highest citation based TLS of 9709 having citation linkages with 76 countries
17. Chinese Academy Science has the highest citation based TLS of 1090 having citation linkages with 369 institutions
18. IEEE Access has the highest citation based TLS of 2133 having citation linkages with 177 journals
19. Chandola V (USA) has the highest co-citation TLS of 867.8323 and co-citation linkages with 1910 researchers. His article [61] obtained the highest co-citation TLS of 750 and co-citation linkages with 910 documents
20. Lecture Notes in Computer Science journal obtained the highest co-citation TLS of 5680.4689 and co-citation linkages with 1927 researchers.
21. The keyword 'malware detection' obtained the highest burst strength of 28.80 during 2012–18
22. The article published by Goodfellow et al. [65] obtained the highest burst strength of 45.43 during 2018–19

Based on the extensive bibliometric analysis of cybersecurity and forensic research over the past decade, future investigations may be directed towards exploring newer deep learning and transfer learning architectures towards improved anomaly/threat detection, classification and faster elimination with greater accuracy. System condition monitoring, cybersecurity and forensic data modeling and radiology training require more investigations. There is a lot of scope to conduct cybersecurity and forensic research in hardware architectures, automation control systems and multi/interdisciplinary software applications. Applied physics, chemistry, instrumentation, imaging science, photography technology and advanced materials are some of the lesser explored cybersecurity and forensic application areas. Researchers may also conduct extensive bibliometric analyses of specific areas of cybersecurity and forensic research such as malware detection and deep neural networks in cybersecurity to reveal underlying trends influencing the current cybersecurity/forensic efforts and shaping the future of information/data security as a whole. All of the above mentioned insights and recommendations provide directions for more multi-faceted and widespread applications in this field, positively impacting multiple disciplines and sectors globally towards a more digitally secure future.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] Ahmed U, Raza I, Hussain SA, Ali A, Iqbal M, Wang X. Modelling cyber security for software-defined networks those grow strong when exposed to threats. J Reliab Intell Environ 2015;1(2):123–46.
[2] Ramim M, Levy Y. Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. J Cases Inf Technol (JCIT) 2006;8(4):24–34.
[3] Chabrow E. China blamed for Penn State breach: Hackers remained undetected for more than two years. Data Breach Today 2015;1.
[4] Nakhodchi S, Dehghantanha A. A bibliometric analysis on the application of deep learning in cybersecurity. In: Security of cyber-physical systems. Cham, Switzerland: Springer; 2020, p. 203–21.
[5] Miskiewicz R. Internet of things in marketing: Bibliometric analysis. 2020.
[6] Rouzbahani HM, Karimipour H, Dehghantanha A, Parizi RM. Blockchain applications in power systems: A bibliometric analysis. In: Blockchain cybersecurity, trust and privacy. Cham, Switzerland: Springer; 2020, p. 129–45.
[7] Mohammadi S, Mirvaziri H, Ghazizadeh-Ahsaee M, Karimipour H. Cyber intrusion detection by combined feature selection algorithm. J Inf Secur Appl 2019;44:80–8.
[8] Grooby S, Dargahi T, Dehghantanha A. A bibliometric analysis of authentication and access control in IoT devices. In: Handbook of big data and IoT security. Cham, Switzerland: Springer; 2019, p. 25–51.
[9] Azmoodeh A, Dehghantanha A, Choo K-KR. Big data and internet of things security and forensics: Challenges and opportunities. In: Handbook of big data and IoT security. Cham, Switzerland: Springer; 2019, p. 1–4.
[10] Sekhar R, Sharma D, Shah P. State of the art in metal matrix composites research: A bibliometric analysis. Appl Syst Innov 2021;4(4):86.

[11] Sharma D, Gupta PK, Andreu-Perez J. A review on cyber physical systems and smart computing: Bibliometric analysis. In: Metaheuristic algorithms in industry 4.0. CRC Press; 2021, p. 1–31.
[12] van Raan AF. For your citations only? Hot topics in bibliometric analysis. Meas: Interdiscip Res Perspect 2005;3(1):50–62.
[13] Ye Q, Song H, Li T. Cross-institutional collaboration networks in tourism and hospitality research. Tour Manag Perspect 2012;2:55–64.
[14] Zupic I, Čater T. Bibliometric methods in management and organization. Organ Res Methods 2015;18(3):429–72.
[15] Jiang Y, Ritchie BW, Benckendorff P. Bibliometric visualisation: An application in tourism crisis and disaster management research. Curr Issues Tour 2019;22(16):1925–57.
[16] Borgman CL, Furner J. Scholarly communication and bibliometrics. Annu Rev Inf Sci Technol 2002;36(1):1–53.
[17] Jamal T, Smith B, Watson E. Ranking, rating and scoring of tourism journals: Interdisciplinary challenges and innovations. Tour Manag 2008;29(1):66–78.
[18] Benckendorff P. Themes and trends in Australian and New Zealand tourism research: A social network analysis of citations in two leading journals (1994–2007). J Hosp Tour Manag 2009;16(1):1–15.
[19] Benckendorff P, Zehrer A. A network analysis of tourism research. Ann Tour Res 2013;43:121–49.
[20] Hu C, Racherla P. Visual representation of knowledge networks: A social network analysis of hospitality research domain. Int J Hosp Manag 2008;27(2):302–12.
[21] White HD, McCain KW. Visualizing a discipline: An author co-citation analysis of information science, 1972–1995. J Am Soc Inf Sci 1998;49(4):327–55.
[22] Baggio R, Scott N, Arcodia C. Collaboration in the events literature: a co-authorship network study. In: Proceedings of the EUTO. 2008, p. 1–16.
[23] McKercher B. A citation analysis of tourism scholars. Tour Manag 2008;29(6):1226–32.
[24] Ying T, Xiao H. Knowledge linkage: A social network analysis of tourism dissertation subjects. J Hosp Tour Res 2012;36(4):450–77.
[25] Cheng C-K, Li XR, Petrick JF, O'Leary JT. An examination of tourism journal development. Tour Manag 2011;32(1):53–61.
[26] McKercher B, Law R, Lam T. Rating tourism and hospitality journals. Tour Manag 2006;27(6):1235–52.
[27] Scott N, Baggio R, Cooper C. Network analysis and tourism. England: Channel View Publications; 2008.
[28] Eck NJv, Waltman L. VOS: A new method for visualizing similarities between objects. In: Advances in data analysis. Heidelberg,Germany: Springer; 2007, p. 299–306.
[29] Chen C. Searching for intellectual turning points: Progressive knowledge domain visualization. Proc Natl Acad Sci 2004;101(suppl 1):5303–10.
[30] Cobo MJ, López-Herrera AG, Herrera-Viedma E, Herrera F. Science mapping software tools: Review, analysis, and cooperative study among tools. J Am Soc Inf Sci Technol 2011;62(7):1382–402.
[31] Jalali MS, Razak S, Gordon W, Perakslis E, Madnick S. Health care and cybersecurity: bibliometric analysis of the literature. J Med Internet Res 2019;21(2):e12644.
[32] Rahim N. Bibliometric analysis of cyber threat and cyber attack literature: Exploring the higher education context. In: Sarfraz M, editor. Cybersecurity threats with new perspectives. Rijeka: IntechOpen; 2021, Ch. 10.
[33] Makawana P, Jhaveri R. A bibliometric analysis of recent research on machine learning for cyber security. 2018, p. 213–26.
[34] Elango B, Matilda S, Jeyasankari J. Redefining search terms for cybersecurity: a bibliometric perspective. In: Proceedings of the international conference on recent advances in computational techniques (IC-RACT). 2020.
[35] Azambuja AJGd, Almeida VR. A bibliometric study of cybersecurity in industry 4.0 publications. Res Soc Dev 2021;(3):1–26.
[36] Mahmud M, Haq IU, et al. Information security in business: a bibliometric analysis of the 100 top cited articles. Libr Philos Pract 2021;1–49.
[37] Shukla G, Gochhait S. Cyber security trend analysis using Web of Science: a bibliometric analysis. Eur J Mol Clin Med 2020;7(6):2567–76.
[38] Nakhodchi S, Dehghantanha A. A bibliometric analysis on the application of deep learning in cybersecurity. In: Karimipour H, Srikantha P, Farag H, Wei-Kocsis J, editors. Security of cyber-physical systems: Vulnerability and impact. Cham: Springer International Publishing; 2020, p. 203–21.
[39] Gill J, Okere I, Haddadpajouh H, Dehghantanha A. Mobile forensics: A bibliometric analysis. Adv Inf Secur 2018;297–310.
[40] Kusuma M, Hariyadi D, Fazlurrahman, Nugroho MA. The bibliometric analysis the digital forensics researcher in Indonesia based on garba rujukan digital: 2008–2020. In: 2021 IEEE Mysore sub section international conference (MysuruCon). 2021, p. 13–7.
[41] Baldwin J, Alhawi OM, Shaughnessy S, Akinbi A, Dehghantanha A. Emerging from the cloud: A bibliometric analysis of cloud forensics studies. In: Cyber threat intelligence. Cham, Switzerland: Springer; 2018, p. 311–31.
[42] Gokhale A, Mulay P, Pramod D, Kulkarni R. A bibliometric analysis of digital image forensics. Sci Technol Libr 2020;39(1):96–113.
[43] Gou X, Liu H, Qiang Y, Lang Z, Wang H, Ye D, Wang Z, Wang H. In-depth analysis on safety and security research based on system dynamics: A bibliometric mapping approach-based study. Saf Sci 2022;147:105617, URL https://www.sciencedirect.com/science/article/pii/S0925753521004574.
[44] Thakur H, Purandare P. Comparative study on bibliometric data of cyber attacks on financial institutions. AIP Conf Proc 2022;2519(1):030044. http://dx.doi.org/10.1063/5.0112569.
[45] Yarovenko HM, Rogkova M. Dynamic and bibliometric analysis of terms identifying the combating financial and cyber fraud system. 2022.
[46] Bolbot V, Kulkarni K, Brunou P, Banda OV, Musharraf M. Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. Int J Crit Infrastruct Prot 2022;39:100571. http://dx.doi.org/10.1016/j.ijcip.2022.100571.
[47] Cojocaru I, Cojocaru I, et al. A bibliomeric analysis of cybersecurity research papers in Eastern Europe: Case study from the Republic of Moldova. In: Central and Eastern European eDem and eGov days, Vol. 335. 2019, p. 151–62.
[48] Goyal R. Blockchain technology in forensic science. a bibliometric review. In: 2021 3rd international conference on advances in computing, communication control and networking (ICAC3N). 2021, p. 1570–3. http://dx.doi.org/10.1109/ICAC3N53548.2021.9725660.
[49] Ismayilova N. Bibliometric analysis of information security research. Comput Commun 2015;616(1.352):1–352.
[50] Perianes-Rodriguez A, Waltman L, van Eck NJ. Constructing bibliometric networks: A comparison between full and fractional counting. J Informetr 2016;10(4):1178–95.
[51] Perozzi B, Al-Rfou R, Skiena S. Deepwalk: Online learning of social representations. In: Proceedings of the 20th ACM SIGKDD international conference on knowledge discovery and data mining. 2014, p. 701–10.
[52] Pimentel MA, Clifton DA, Clifton L, Tarassenko L. A review of novelty detection. Signal Process 2014;99:215–49.
[53] Sharafaldin I, Lashkari AH, Ghorbani AA. Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp 2018;1:108–16.
[54] Schlegl T, Seeböck P, Waldstein SM, Schmidt-Erfurth U, Langs G. Unsupervised anomaly detection with generative adversarial networks to guide marker discovery. In: International conference on information processing in medical imaging. Springer; 2017, p. 146–57.
[55] Erfani SM, Rajasegarar S, Karunasekera S, Leckie C. High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning. Pattern Recognit 2016;58:121–34.
[56] Shabtai A, Kanonov U, Elovici Y, Glezer C, Weiss Y. "Andromaly": a behavioral malware detection framework for android devices. J Intell Inf Syst 2012;38(1):161–90.
[57] Khan S, Yairi T. A review on the application of deep learning in system health management. Mech Syst Signal Process 2018;107:241–65.
[58] Shone N, Ngoc TN, Phai VD, Shi Q. A deep learning approach to network intrusion detection. IEEE Trans Emerg Top Comput Intell 2018;2(1):41–50.
[59] Pei K, Cao Y, Yang J, Jana S. Deepxplore: Automated whitebox testing of deep learning systems. In: Proceedings of the 26th symposium on operating systems principles. 2017, p. 1–18.
[60] Rieck K, Trinius P, Willems C, Holz T. Automatic analysis of malware behavior using machine learning. J Comput Secur 2011;19(4):639–68.
[61] Chandola V, Banerjee A, Kumar V. Anomaly detection: A survey. ACM Comput Surv 2009;41(3):1–58.

[62] Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the KDD CUP 99 data set. In: 2009 IEEE symposium on computational intelligence for security and defense applications. Ieee; 2009, p. 1–6.
[63] Hochreiter S, Schmidhuber J. Long short-term memory. Neural Comput 1997;9(8):1735–80.
[64] Krizhevsky A, Sutskever I, Hinton GE. Imagenet classification with deep convolutional neural networks. Adv Neural Inf Process Syst 2012;25.
[65] Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, Courville A, Bengio Y. Generative adversarial nets. Adv Neural Inf Process Syst 2014;27.
[66] Breiman L. Random forests. Mach Learn 2001;45(1):5–32.
[67] Pedregosa F, Varoquaux G, Gramfort A, Michel V, Thirion B, Grisel O, Blondel M, Prettenhofer P, Weiss R, Dubourg V, et al. Scikit-learn: Machine learning in Python. J Mach Learn Res 2011;12:2825–30.
[68] LeCun Y, Bengio Y, Hinton G. Deep learning. Nature 2015;521(7553):436–44.
[69] Kingma D, Ba J. 3Rd international conference on learning representations, ICLR 2015-conference track proceedings. In: International conference on learning representations, ICLR) Adam: A method for stochastic optimization Go to reference in article. 2015.
[70] Cortes C, Vapnik V. Support-vector networks. Mach Learn 1995;20(3):273–97.
[71] Santos I, Brezo F, Ugarte-Pedrero X, Bringas PG. Opcode sequences as representation of executables for data-mining-based unknown malware detection. Inform Sci 2013;231:64–82.
[72] Zhou Y, Jiang X. Dissecting android malware: Characterization and evolution. In: 2012 IEEE symposium on security and privacy. IEEE; 2012, p. 95–109.
[73] Aafer Y, Du W, Yin H. Droidapiminer: Mining api-level features for robust malware detection in android. In: International conference on security and privacy in communication systems. Springer; 2013, p. 86–103.
[74] Chang C-C, Lin C-J. LIBSVM: a library for support vector machines. ACM Trans Intell Syst Technol 2011;2(3):1–27.
[75] Bhuyan MH, Bhattacharyya DK, Kalita JK. Network anomaly detection: methods, systems and tools. Ieee Commun Surv Tutor 2013;16(1):303–36.
[76] Srivastava N, Hinton G, Krizhevsky A, Sutskever I, Salakhutdinov R. Dropout: a simple way to prevent neural networks from overfitting. J Mach Learn Res 2014;15(1):1929–58.
[77] Kingma D, Ba J. Adam: A method for stochastic optimization. In: Proceedings of the 3rd international conference for learning representations (iclr'15). San Diego; 2015.
[78] Arp D, Spreitzenbarth M, Hubner M, Gascon H, Rieck K, Siemens C. Drebin: Effective and explainable detection of android malware in your pocket. In: Ndss, Vol. 14. 2014, p. 23–6.
[79] Wu D-J, Mao C-H, Wei T-E, Lee H-M, Wu K-P. Droidmat: Android malware detection through manifest and api calls tracing. In: 2012 seventh Asia joint conference on information security. IEEE; 2012, p. 62–9.
[80] Chatfield K, Simonyan K, Vedaldi A, Zisserman A. Return of the devil in the details: Delving deep into convolutional nets. 2014, arXiv preprint arXiv:1405.3531.
[81] Grace M, Zhou Y, Zhang Q, Zou S, Jiang X. Riskranker: scalable and accurate zero-day android malware detection. In: Proceedings of the 10th international conference on mobile systems, applications, and services. 2012, p. 281–94.