Scientometrics
https://doi.org/10.1007/s11192-019-03222-9

Investigating the applications of artificial intelligence in cyber security

Naveed Naeem Abbas[1,2] · Tanveer Ahmed[3] · Syed Habib Ullah Shah[1,4] · Muhammad Omar[1] · Han Woo Park[5]

Received: 16 June 2019

Abstract
Artificial Intelligence (AI) provides instant insights to pierce through the noise of thousands of daily security alerts. The recent literature focuses on AI's application to cyber security but lacks visual analysis of AI applications. Structural changes have been observed in cyber security since the emergence of AI. This study promotes the development of theory about AI in cyber security, helps researchers establish research directions, and provides a reference that enterprises and governments can use to plan AI applications in the cyber security industry. Many countries, institutions and authors are densely connected through collaboration and citation networks. Artificial neural networks, an AI technique, gave birth to today's research on cloud cyber security. Many research hotspots such as those on face recognition and deep neural networks for speech recognition may create future hotspots on emerging technology, such as on artificial intelligence systems for security. This study visualizes the structural changes, hotspots and emerging trends in AI studies. Five evaluation factors are used to judge the hotspots and trends of this domain and a heat map is used to identify the areas of the world that are generating research on AI applications in cyber security. This study is the first to provide an overall perspective of hotspots and trends in the research on AI in the cyber security domain.

Keywords Artificial intelligence · Cyber security · Scientometric · Visualization · Emerging trend · Research hotspot

Introduction

Security takes many forms, such as security of information, security of documents and security of property. Security, in its many forms, is constantly being improved through the application of modern techniques. Our world is undergirded by networked technology, from internet banking to government infrastructure. Thus, protecting data is critical.

✉ Muhammad Omar
m.omar.nazeer@gmail.com

✉ Han Woo Park
hanpark@ynu.ac.kr

Extended author information available on the last page of the article

Published online: 09 September 2019

Cyber security reduces the risk of losing essential data, but cyber attacks have increased and have become more powerful. According to a 2014 Consumer News and Business Channel (CNBC) report, the global economy suffers a loss of US $400 billion every year due to cyber crimes. The human factor is the weakest link and is the main reason for cyber security failure. To address this weakness, automated systems, such as artificial intelligence (AI) applications are used in cyber security.

Researchers have explored AI and cyber security from various perspectives. Artificial intelligence is becoming popular across the globe. It is popular even in countries that lack research in this field (Omar et al. 2017; Pannu 2015). Artificial intelligence is argued to be part of the fourth industrial revolution. It is applied in many fields, such as disaster response (Imran et al. 2014; Ofli et al. 2016; Ramchurn et al. 2016), medicine (Jha and Topol 2016; Zhou and Jiang 2003; Malav et al. 2017), vehicles (Hengstler et al. 2016; Litman 2014; Wang et al. 2017), economics and management (Parkes and Wellman 2015; Aghion et al. 2017) and business models (Chen and Storey 2012; Loebbecke and Picot 2015). Göztepe (2012) used a fuzzy rule-based expert system to meet critical data needs against cyber terrorist attacks. Dilek et al. (2015) review the advances made in the application of AI techniques to combat cyber crimes to demonstrate how these techniques can be effective. Performing a cyber security audit of home control systems is necessary in order to understand how secure the system is and where its vulnerabilities might lie (Byres 2004). Cyber security has been growing rapidly since cyber attacks began increasing in the mid-2000s (Saridakis et al. 2015). It is necessary to conduct a visual analysis of the hotspots and emerging trends regarding AI applications in cyber security through scientometric techniques.

This study also identifies the historical changes in the discipline and the dynamic trajectory of AI applications in cyber security. It provides a reference for future theoretical research and practical developments of AI applications in cyber security. It should also help scholars identify future research fields concerning AI in cyber security. This study's research questions are as follows:

RQ 1. What structural changes have taken place in cyber security research since AI applications came into use?
RQ 2. What are the implications of the dense and loose connections between journals, authors, institutions and countries in terms of collaboration and citation networks?
RQ 3. How can we apply a scientometric visualization to detect emerging trends and generate research agendas in the AI-mediated cyber security domain?

Figure 1 shows 4658 Web of Science articles. Figure 1a shows the articles published in 2007–2018 on AI applications in cyber security. More than 900 articles were published in 2018, which indicates that research on AI applications in cyber security is a developing field. Figure 1b shows the 2007–2019 citation trends for articles on AI applications in cyber security.

Figure 2 shows the global area distribution of studies on AI applications in cyber security research. This research has spread across the globe, especially active in the United States, China, Germany, Japan, India, Australia and several European countries.

The remainder of the paper is organized as follows. First, the study's methodology is described, including its data source and analytical framework. Then, the study analyzes five indicators- the co-cited references network, burst references, co-occurrence keywords network, burst keywords, and dual-map overlays network using the information visualization software CiteSpace V (Chen 2006). The program is also used to highlight the structural

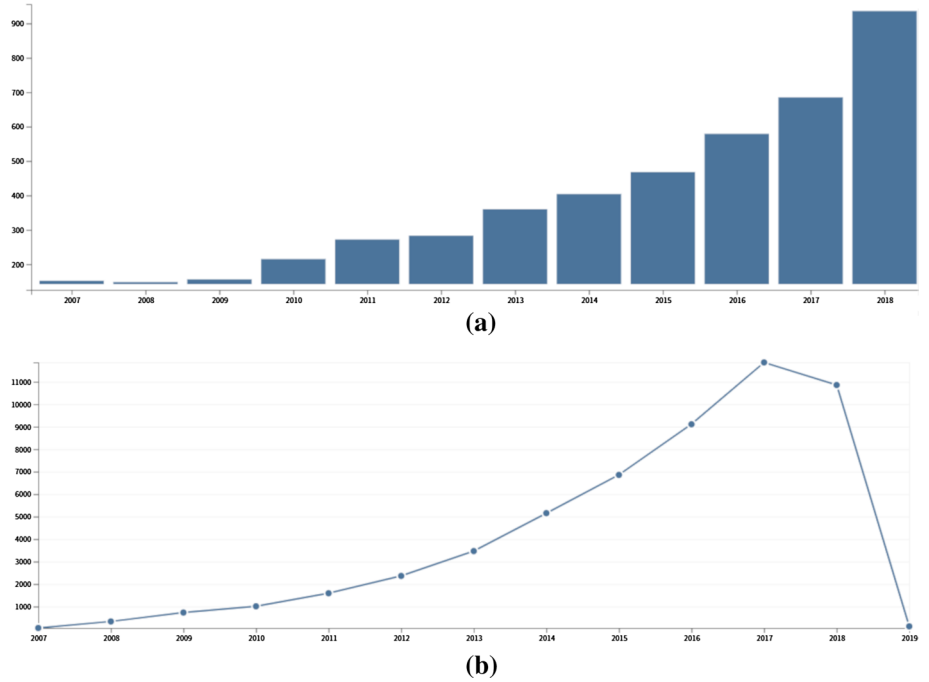


Fig. 1 Trend in research on AI applications in cyber security field: **a** published articles each year; **b** article citations each year

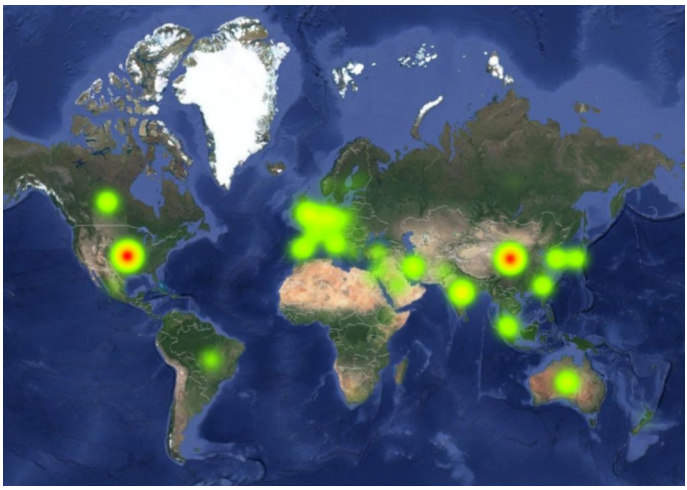


Fig. 2 The heatmap for studies on AI applications in cyber security research: the green spots indicate active research areas, and the red spots indicate highly active areas

changes in cyber security and identify the emerging trends in studies on AI applications in cyber security. Finally, a conclusion is drawn and the study's limitations are discussed.

Methodology

Data collection

The study retrieves articles from the SCIE database of the Web of Science (WoS). Using WoS allows one to easily explore and follow links to additional information. The database is searchable and offers complete bibliographic data, cited reference data, navigation and links to full texts. The WoS adds approximately 25,000 articles and 700,000 cited references each week.

We try to include as much of the literature as possible. We first test the completeness of the selected papers using different keyword combinations. We also manually verify the documents obtained from the WoS. We search the related research using the following query:

> TS="(Artificial Intelligence OR Machine Learning OR Deep learning OR Artificial Neural Network OR Random forest OR Decision tree OR Intelligent Automation OR Support Vector Machine OR SVM OR AI OR ML OR Intelligent Agents OR Artificial Immune System OR Fuzzy Sets OR linear regression OR logistic regression OR supervised learning OR LDA OR unsupervised clustering OR k-means OR word embedding OR topic models OR neural net OR genetic algorithm OR evolutionary algorithm) AND (Cyber Security OR Network Security OR Information Security OR Telecommunication Security OR Data Privacy OR cyber attribution OR Intrusion Detection System OR IDS OR Cryptography OR Intrusion Prevention Systems OR IPS OR Internet Security OR IP Security OR Preventing Packet Sniffing OR attack prevention mechanisms OR User to root attack OR Root to local Attack OR Cyber Attack OR IT security)"

This query is comprised of two parts: (1) AI-related terms and (2) cyber security-related terms. The query uses 46 keywords that cover most of the fields of AI and cyber security. The main purpose of this query is to find articles that combine work in both fields. Each bibliographic record contains the metadata of a published article, including its title, abstract, authors, keywords and references. Our scientometric review is based mainly on the SCIE dataset, which consists of 4854 unique records.

Scientometrics analysis

With the rapid growth in the scientific literature and the development of network technology, a large amount of scientific literature data can be processed through information visualization technology. Table 1 defines the basic terms relevant to this analysis.

The CiteSpace series software developed by Chaomei Chen, professor at Dexrel University, is a popular information visualization tool based on scientometric metrology. CiteSpace can eliminate information that is irrelevant to the research topic, can identify and display hotspots and new trends in a certain research area clearly and scientifically (Chen 2016). The latest version, CiteSpace V, is used for this study.

Table 1 Basic terms and definitions

No.	Term	Definition	Purpose
1	Co-cited references network	The co-cited references network comprises situations in which two documents are cited simultaneously in a single document	It reveals the research focuses and knowledge base of a domain. It helps to identify hotspots and emerging trends in a field
2	Burst references	The dynamic characteristics of a subject can be reflected by a substantial increase in citations of documents on this subject. This kind of surge in citations in a short period of time is called "burst references"	It shows the fields with which the scientific community is concerned, namely the research hotspots
3	Co-occurrence keywords network	If two keywords appear simultaneously in a document, both keywords are usually considered relevant for the content. A co-occurrence Keywords network is made up of such keywords	It reflects the emergence and evolution of important keywords in an area
4	Hotspots	A hotspot is something that attracts a substantial amount of attention within a short period of time	It helps to identify the articles, keywords, and references that were popular in a specific period of time
5	Dual-map overlays network	This function superimposes a map generated by CiteSpace onto another basic knowledge panorama map. The former map is called an "overlay" and the latter is called the "base layer." The base layer is a knowledge panoramic map of the discipline defined by the JCR (Journal Citation Reports)	It shows the citation relations and evolution sequence of various disciplines in a research field based on the citing and cited journals. Scholars can identify the historical changes in the dynamic trajectories of a discipline's search field more easily
6	Burst keywords	These are surging occurrences in a short period of time	These reflect the emergence of certain keywords within a short time. They can be used as an indicator of hotspots and emerging trends
7	Centrality	This refers to the quality or fact of being in the middle of somewhere or something	It measures the extent to which a node lies on paths between other nodes
8	Silhouette value	The silhouette value is a measure of how similar an object is to its own cluster relative to other clusters	The silhouette value ranges from −1 to 1, which reflects the quality of a cluster configuration
9	Mutual information (MI)	This refers to information obtained from two partitions	It quantifies the information shared by the two clusters and can thus be employed as a clustering similarity measure
10	Modularity	This is a measure of the structure of networks	It is designed to measure the strength of division of a network into modules

Using CiteSpace V allows us to generate a co-cited references network, co-occurrence keywords network and journal dual-map overlays network. It can identify structural changes and hotspots by measuring the size of clusters from the co-cited references network and determine the frontier topics by calculating the average annual publications in a cluster. We also use VOSviewer (Jan and Ludo 2010) to perform co-authorship analysis. VOSviewer is a software tool for constructing and visualizing bibliometric networks. VOSviewer also offers text-mining functionality that can be used to construct and visualize co-occurrence networks of important terms extracted from a body of scientific literature. We also investigate the intellectual landscape of studies on AI applications in cyber security research, which can be depicted via the co-cited references network and co-occurring keywords network (Chen et al. 2014; Park and Park 2018).

The research hotspots and emerging trends in studies of AI applications in cyber security are revealed through the analysis of these networks. In addition, a discipline trajectory analysis conducted via dual-map overlays function is used to identify discipline hotspots and emerging trends in the research on AI applications in cyber security.

Scientometric visualization to detect structural changes, emerging trends, and research agendas in AI-mediated cyber security domain

References network as indicator

Maps composed of co-citation links (between document pairs) can reveal the research focus and knowledge base of a domain (Kim et al. 2016; Small and Greenlee 1980; Jin and Li 2018). A co-cited references network for research on AI applications in cyber security is created by importing all 4854 document records to CiteSpace V.

Other parameters are set as follows. First, as most of the research on AI applications in cyber security has appeared over recent years, we targeted the literature published within the last 12 years and set "Time Slicing" to 2007–2018 and set 01 year per slice; set "Top N per slice" to 100, which means that the top 100 nodes of occurrence/citation frequency are selected from per slice; and set "Node Types" to cited references. In addition, as the body of relevant literature is not very large, the generated network does not need to be pruned. Thus, the corresponding parameter "Pruning" is not selected.

The results show that the co-cited references network generated by 160,574 cited documents (from 4854 citing documents) produced 659 nodes, 1705 connections and 161 clusters from 2007 to 2018 when we fix the nodes at $e = 3.0$. To display the important clusters, we remove the small clusters from the periphery and present the co-citation core map (see Fig. 3). Modularity $Q = 0.8028$ indicates that the clustering results of the network spectrum are very good. In Fig. 3, the nodes denote co-cited references and the size of the nodes is determined mainly by the number of cited times. The larger the node, the higher the number of cited times and the greater the research value. Nodes marked with red rings represent a burst reference, which reflects the research hotspots in different periods. The lines connecting nodes are co-citation links, whose different colors show when a connection was made for the first time. The knowledge map reveals the spatial and temporal evolution of the cluster knowledge structure and the hot topics in studies on AI applications in cyber security. Figure 3 shows that research on AI applications in cyber security has formed around a large number of topics and there are several links between them. It shows that this research has formed a system and has not been conducted in isolation. For

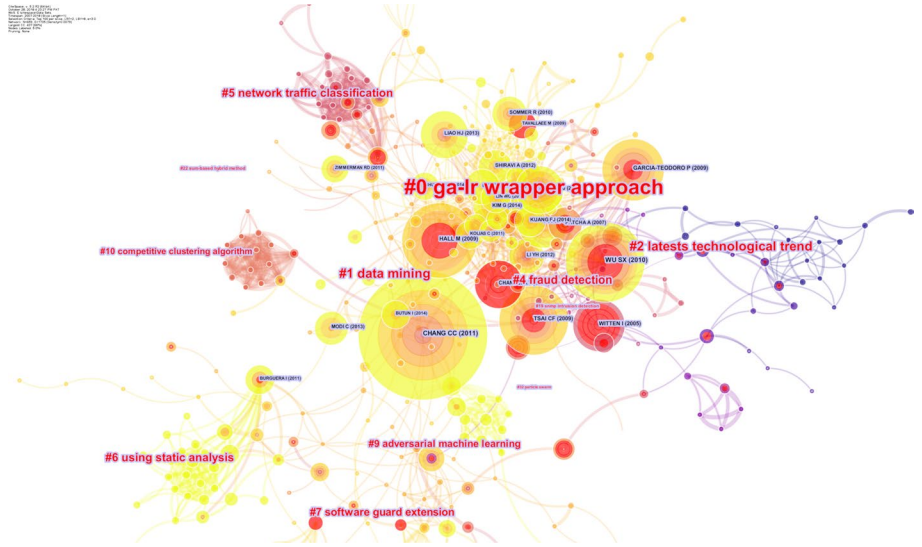


Fig. 3 The co-cited references network of AI applications in cyber security. The nodes denote co-cited references. The nodes marked with red rings represent burst references. The lines connecting nodes are co-citation links

example, links are observed between the cluster "#1 data mining" and "#4 fraud detection" which suggests that "#1 data mining" may lead to the emergence of more innovation. Some larger nodes, such as "#0 ga-lr wrapper approach," "#1 data mining" and "#5 network traffic classification," play an important role in studies on AI applications in cyber security research. Although some clusters, such as "#22 sum-based hybrid method" and "#9 adversarial machine learning" are smaller because they appeared later, they are likely to become hot topics.

Profiles of the 10 largest clusters of AI application studies in cyber security research are shown in Table 2, which lists the corresponding clustering labels. The cluster number in the table is the position in which the literature is located. The size of the cluster represents the number of references, which reflect its hotspot status. The mutual information (MI) value quantifies the information shared by the two clusters and can thus be employed as a clustering similarity measure. The year shows the average publication year of all the studies in a given cluster. The later the time, the closer it is to being a frontier; this can indicate emerging trends in the cluster (Liu et al. 2014).

As shown in Table 2, the larger clusters such as "ga-lr wrapper approach (2012)," "data mining (2011)," "latest technology trend (2002)" and "private k-mean (2012)" are the main hotspots in research on AI applications in cyber security. The emerging clusters, such as "private k-mean (2012)," "using static analysis (2012)" and "adversarial machine learning (2013)" are the current research frontiers in this field. In terms of structural changes, the early cyber security research focused on basic security problems (e.g. intrusion detection, p2p data, attacks, privacy, data security); widespread concern about security caused research on security improvement methods such as fraud detection and network traffic classification to become hotspots. In recent years, new research in cyber security has been promoted to a new level through the impacts of machine learning and android malware detection, as is represented by "adversarial machine learning (2013)" and "private k-mean

Table 2 Brief summary of top 10 clusters based on references network

Cluster	Size	Silhouette	Mean (year)	Top terms (LSI)	Top terms (likelihood ratio, p level = 1.0E−4)	Terms (MI)
0	96	0.755	2012	Detection, high speed big network	Ga-lr wrapper approach (1583.02)	Privacy-preserving heterogeneous health data sharing
1	40	0.767	2011	Detection, using machine	Data mining (751.14)	Recent achievement, new challenge
2	37	0.901	2002	Intrusion detection	Latest technology trend (1289.31)	Privacy-preserving heterogeneous health data sharing
3	32	0.87	2012	Extreme learning machine	Private k-mean (919.69)	Privacy-preserving heterogeneous health data sharing
4	30	0.847	2007	Intrusion detection, SQL injection	Fraud detection (950.93)	Privacy-preserving heterogeneous health data sharing
5	30	0.956	2008	Detection, p2p data, attacks	Network traffic Classification (2491.17)	Privacy-preserving heterogeneous health data sharing
6	29	0.963	2012	Android malware detection	Using static analysis (2257.08)	Privacy-preserving heterogeneous health data sharing
7	28	0.884	2011	Privacy, data	Software guard extension (1417.37)	Privacy-preserving heterogeneous health data sharing
8	28	0.989	2007	Power systems, massive data	Transient stability (1080.09)	Privacy-preserving heterogeneous health data sharing
9	24	0.973	2013	Machine learning, survey, data	Adversarial machine learning (1615.65)	Privacy-preserving heterogeneous health data sharing

(2012)". Table 2 shows that the thematic patterns in the scientific literature differ over time. The changing nature of the thematic patterns throughout the years proves that structural changes have been continuous in cyber security studies since AI emerged.

Burst references as an indicator

The dynamic characteristics of a subject are reflected in an increase in citations of studies on it. These are called "burst references" (see Table 1) and they reflect the fields with which the scientific community is most concerned (i.e., research hotspots) (Chen 2016; Chen et al. 2014).

Tracking the temporal trends in burst references allows us to identify the important research areas at specific points in time. The burst intensities and durations of these areas differ and their research content continues to evolve. Figure 4 shows that structural changes have appeared continuously since AI began to be applied in cyber security. The application of AI in cyber security has been a persistent research hotspot since 2007. The two outstanding years are 2009 and 2010, when a particularly large number of studies emerged, these constitute the outbreak period for studies of AI applications in cyber security research.

Figure 4 lists the top 10 references with the strongest burst values, which allows us to analyze the results more representatively and excavate the research hotspots and evolution trends in studies of AI applications in cyber security. Figure 4 shows that the literature on AI applications in cyber security truly emerged in 2007, when its concentration intensity was high. This is the year when AI applications in cyber security became the focus of academic research and achieved important academic results.

Among the top 10 burst references, the first article was written by Witten et al. (Machine and Tools, n.d.). This article concerns data-mining machine learning tools and techniques for AI applications in cyber security. It was published in 2005, and its burst ranges from 2008 to 2013, as the red line shows, with the earliest burst in 2008 and the highest burst value being 18.9548. This is clearly a landmark article about AI applications in cyber security.

Obviously, the content of this paper about data mining and machine learning techniques in AI with cyber security attracted widespread attention and made studies on AI applications in cyber security a research hotspot. An article by Ian H. Witten was ranked first and was highly cited from 2008 to 2013, especially in 2010, when the number of citations peaked at nine.

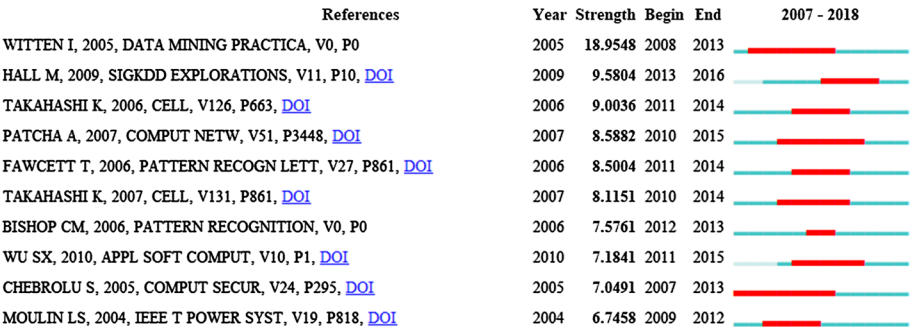


Fig. 4 Top 10 references with strongest burst values, red line represents burst time and dark blue line represents publication time. (Color figure online)

The second burst reference, "The WEKA Data Mining Software," was published by Hall et al. (2009). It burst from 2013 to 2016 and had the second highest burst value of 9.5804.

The WEKA project aims to provide a comprehensive collection of machine learning algorithms and data preprocessing tools to researchers and practitioners. It allows users to quickly try and compare different machine learning methods on new datasets, mostly related to AI applications in cyber security. This article is also a landmark paper about AI applications in cyber security. The article was popular from 2013 to 2016; aside from those years, its level of attention has been up and down.

Co-occurrence keywords network and burst keywords as indicators

If two keywords appear in a document simultaneously, both are usually considered relevant. A co-occurrence keywords network is composed of such keywords, which reflect the emergence and evolution of important keywords in a research area. The hotspots and emerging trends in a certain field can be revealed by studying a co-occurrence keywords network map (Li and Sun 2013; Su and Lee 2010). After "Node Types" was set as "Keyword" and "Top N per slice" was set as 100 in CiteSpace V, a time zone map of the co-occurrence network for studies of AI applications in cyber security was generated, as shown in Fig. 5.

The network contains 337 keywords and 1927 links between 2007 and 2018. The nodes in the map represent the keywords and the size represents the co-occurrence frequency of the keywords. The lines connecting the nodes are co-occurrence links; the different line

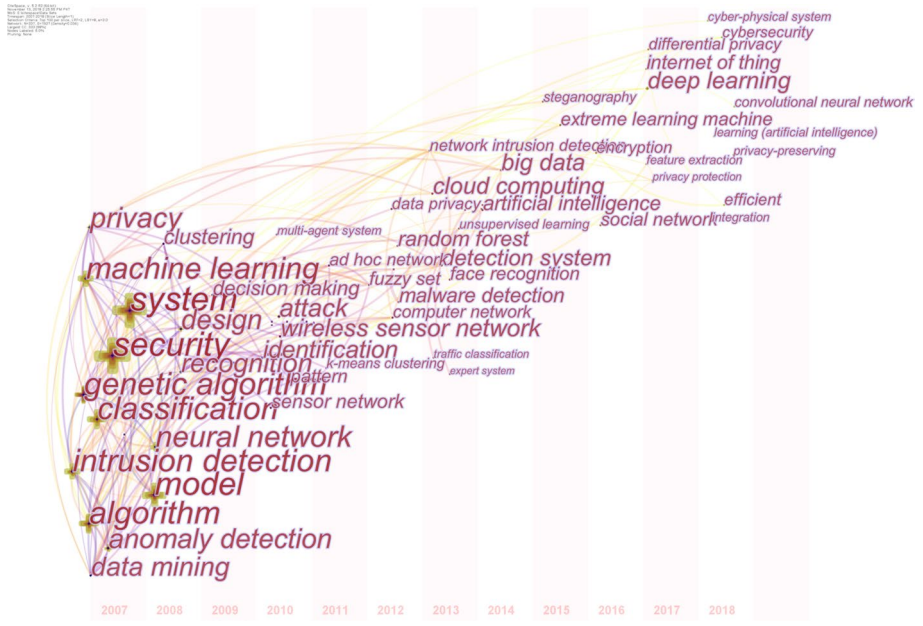


Fig. 5 Time zone map of co-occurrence network in studies of AI applications in cyber security. The nodes represent keywords, and the size of keywords represents co-occurrence frequency. The colors of the lines show when a connection was made for the first time and the thickness of the lines represents co-occurrence strength. (Color figure online)

colors show when a connection was made for the first time and the line thickness represents the co-occurrence strength.

As shown in Fig. 5, the research hotspots in studies of AI applications in cyber security from 2007 to 2010 include "system," "security," "algorithm," "model," "machine learning," "classification,""support vector machine," "data mining," "anomaly detection," "wireless sensor network," "cryptography," and "big data". The research hotspots from 2011 to 2014 include "food security," "artificial intelligence," "detection system," "random forest," "malware detection," "deep learning," "internet of things," "extreme machine learning," "social network," and "pattern". The research hotspots from 2015 to 2018 include "fuzzy set," "data privacy," "cyber security," "sensor," "stenography," "k-mean cluster," "cyber physical system," "learning artificial intelligence," "privacy preserving," "confidentiality" and "feature extraction"; these reflect the emerging trends in the field. In addition, the keywords "system" and "security" are the most frequent and they have the greatest total co-occurrence frequency. System security is thus the core issue in the research on AI applications in cyber security. The emergence of AI in cyber security has led to continuous changes in the research, as shown in Fig. 5.

Keywords represent there fined and summarized versions of the core content of article. Burst keywords reflect the emergence of certain keywords within a short time. Therefore, burst keywords can be used as an indicator of hotspots and emerging trends (Chen 2006; Pak Chung et al. 2011). Figure 6 lists the burst keywords based on starting time in order to show the structural changes/changing trends in the field clearly and comprehensively. The earliest burst keywords appeared in 2007; these include "cryptography," "genetic algorithm," "voltage stability" and "fuzzy logic". In the early stage, the most important concern was data security, especially in data communication. Therefore "cryptography," "genetic algorithm," "fuzzy logic," "data mining" and "intrusion detection" attracted much attention from the academic community. The burst keywords emerging in 2008 include "neural network," "identification," and "pattern." Clearly, the research hotspots in this period focused on data security and privacy, mainly because people sought to ensure the security of stored data via encryption and keys. Shortly afterwards, with the rapid development of AI applications, the new burst keywords "face recognition," "computer network," "prevalence," and "social network" emerged after 2014 and are ongoing; these have been the emerging trends in studies of AI applications in cyber security research.

In addition, "computer security," "artificial immune system," and "United States" have the longest burst times, of at least seven years. Figure 6 shows that network security has been the key topic in the field of AI applications in cyber security and the fact that the longest burst time is observed in the keyword "United States" indicates that most of the research in this field concerns the United States.

Co-occurrence keywords timeline networks

The co-occurrence keywords timeline networks of studies on AI applications in cyber security based on the SCIE dataset is generated by CiteSpace V (see Fig. 7). We examine co-occurrence keywords to identify the structural changes, hotspots and emerging trends in a direct way and avoid the complexity and possible inaccuracy of extracting information from references. In Fig. 7, the nodes represent important keywords, the curves represent the co-occurrence relationships between the keywords (showing the emergence of hotspots), the colors of the curves indicate the appearance times (consistent with the time represented by the top color bar), the horizontal lines represent the time process and the

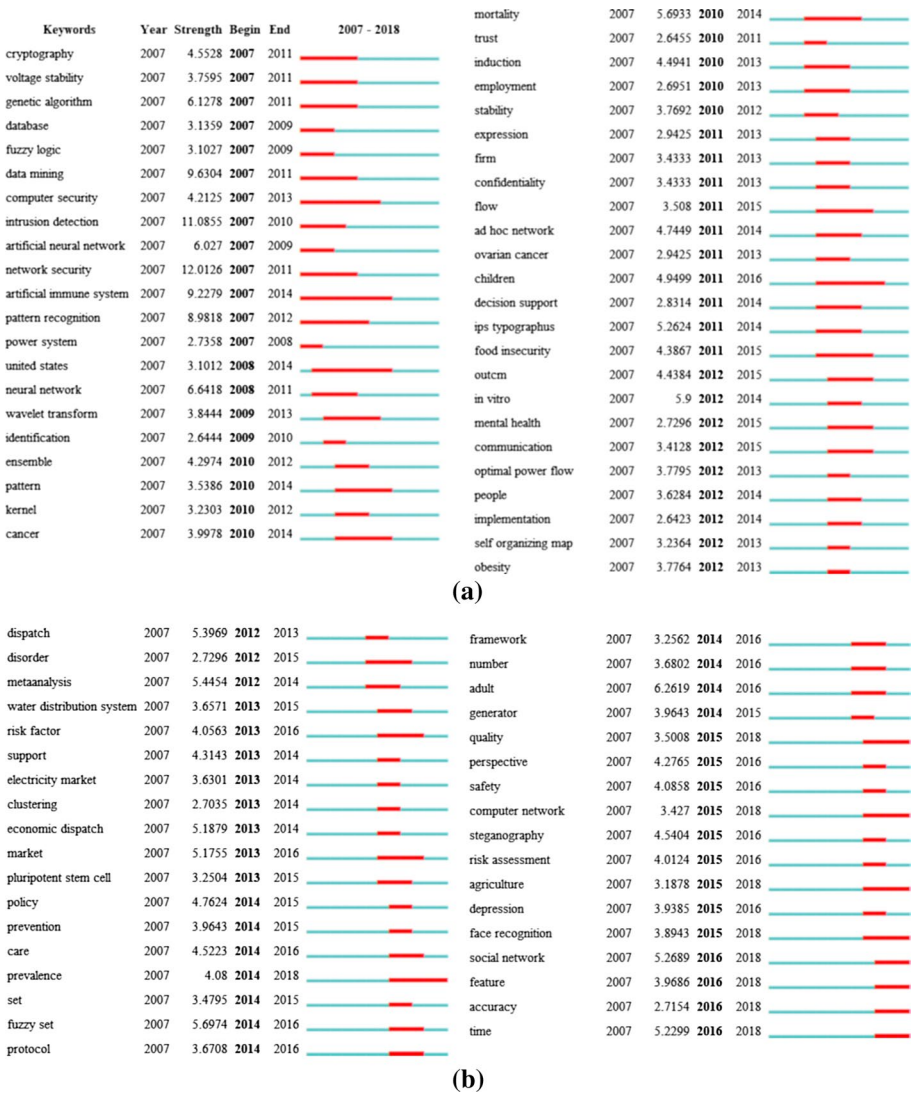


Fig. 6 Burst keywords based on burst time. Red line represents burst time and dark blue line represents publication time. (Color figure online)

words on the right-hand side are the names of the clusters. Figure 7 shows that "sensor network," "reference interval," "transient security assessment," "security constraint," "household food security," "text-based video content classification," "induced pluripotent stem," and "gravitational search" are the top seven research hotspots.

In terms of structural changes, "sensor network" was researched earliest, and "information security cryptography" was its starting point. In the "transient security assessment" hotspot, "classification algorithm model" promoted the emergence of "artificial neural networks". The divergent directions of the curve of "artificial neural networks" shows that this topic gave birth to today's research on cloud cyber security. Moreover, the time line shows

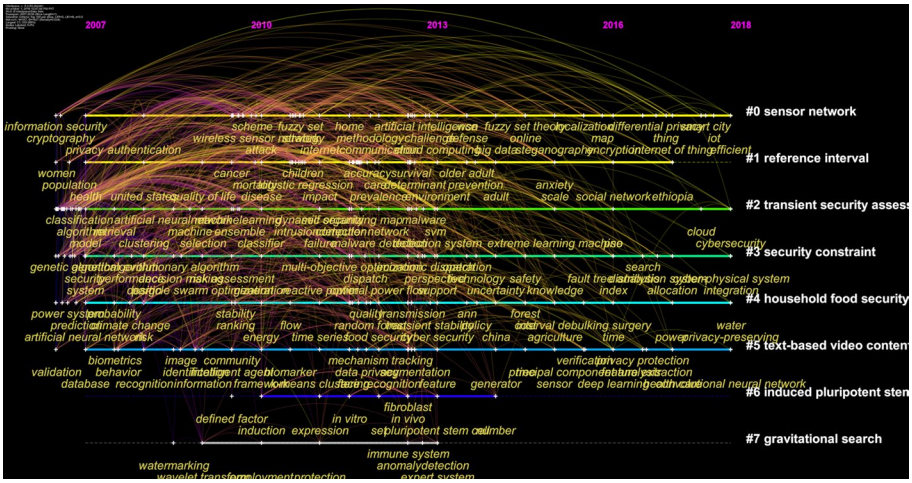


Fig. 7 Co-occurrence keywords timeline networks of AI applications in cyber security

that "sensor network," "transient security assessment," "security constraint," "household food security" and "text-based video content classification" were the emerging research hotspots in this era.

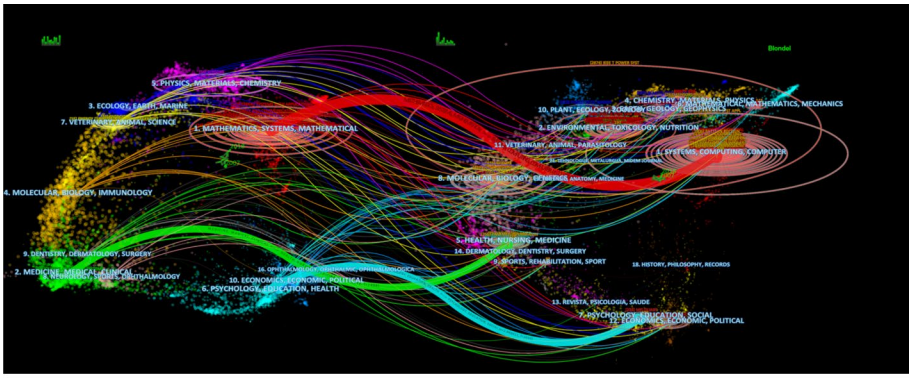
Dual-map overlays network as indicator

Knowledge map of dual-map overlays in AI applications in cyber security

The journal dual-map overlays in CiteSpace V superimpose a map generated by the program onto another basic knowledge panorama map. The former map is called the "overlay" and the latter map is called the "base layer". The base layer is a knowledge panoramic map of the discipline defined by the JCR. Journal dual-map overlays can help scholars identify the historical changes in a discipline's dynamic trajectories easily.

There are two base maps in Fig. 8a: a base map generated by citing journals (the left half) and a base map generated by cited journals (the right half). These were visualized via the same user interface for the discipline distribution presentation regarding AI applications in cyber security. The left side of the map presents the frontier research results, which shows what disciplines and journals are actively involved in the study of AI applications in cyber security.

The right side shows the knowledge sources the frontier studies rely on, through which we can judge what journals or disciplines provide research support for studies on AI applications in cyber security. Figure 8a shows where a citation entity originates and where it points to. By examining these citation relations, we can track the frontiers of research on AI applications in cyber security. The ellipses in Fig. 8a are the journal clusters and the size of those ellipses indicates the total number of journals in a discipline area. Journals play an important role in the development of this discipline. The number in front of each journal is the number of papers published in the journal on AI applications in cyber security. The weak arc links or powerful lane curves with different colors in the overlay map demonstrate the ins and outs of the journals and disciplines. The disciplines are represented by



(a)

(b)

Fig. 8 **a** A knowledge panorama of studies on AI applications in cyber security with dual-map overlays method. The left side represents citing journals and represents cited journals. **b** Zoomed view of (**a**) Discipline trajectory map of AI applications in cyber security: The green fold line indicates the shift trajectory of the discipline. (Color figure online)

their corresponding number and name. Figure 8a identifies the important discipline fields and powerful publication journals related to the study of AI applications in cyber security.

Hot disciplines and important journals

The complex links intertwined in differently colored arcs shown in Fig. 8a indicate not only that studies on AI applications in cyber security are divided into many discipline areas but also that the knowledge base is derived from various knowledge areas. This indicates that research on AI applications in cyber security is developing towards the academic ecology direction of cross-melting. The discipline "MATHEMATICS, SYSTEMS, MATHEMATICAL" forms a complete curve channel. This shows that it is a hot topic in this research field. In addition, the discipline "PHYSICS, MATERIALS, CHEMISTRY" has also taken an active part in studies on AI applications in cyber security, as has the [54] *Journal of Sensors* and "MOLECULAR, BIOLOGY, GENETICS". The map shows that "SYSTEMS, COMPUTING, COMPUTER" is an important knowledge base and source for studies on AI applications in cyber security, and provides an important theoretical basis for research on and development of AI applications for cyber security. In this area, [1814] *Expert System with Application*, [834] *Computer Security* and [589] *Electric Power System* are among

the most important journals. *Expert System with Applications* has published 1814 articles in the "SYSTEMS, COMPUTING, COMPUTER" field, and these have been frequently cited by related frontier research on AI applications in cyber security. This provides a knowledge-sharing position for cross-research on AI applications in cyber security with more disciplines. The discipline "SYSTEMS, COMPUTING, COMPUTER" shown with a red curve, provides the main support for the frontier development of studies on AI applications in cyber security in "MATHEMATICS, SYSTEMS, MATHEMATICAL".

Meanwhile, the frontier research in "MATHEMATICS, SYSTEMS, MATHEMATICAL" is also influenced by other disciplines to varying degrees, such as "MOLECULAR, BIOLOGY, GENETICS" and "CHEMISTRY, MATERIALS, PHYSICS". Overall, the research on AI applications in cyber security has developed rapidly in many disciplines and is showing interdisciplinary, which indicates ongoing structural changes in cyber security research. It not only forms a distinct interdisciplinary citation curve but also has small citation branches. Studies on AI applications in cyber security can be expected to follow a trend characterized by diversity, with the continuous development of cross-disciplinary integration.

Emerging trends based on discipline trajectories

Figure 8b shows a discipline trajectory map of the citing journals in the research on AI applications in cyber security. It reveals the dynamic discipline trajectory of studies on AI applications in cyber security research from 2007 to 2018. We can grasp the development trend of the research as a whole by analyzing the green fold line in the figure. We can track the structural changes and hotspots at different time points as well as the key turning points. The green fold line describes the discipline trajectory, which is supported by 4854 documents about AI applications in cyber security.

The data in Fig. 8b show that the active study of AI applications in cyber security begins with the discipline field of "MATHEMATICS, SYSTEMS, MATHEMATICAL", where academic activity is long standing. The trajectory began between "MATHEMATICS, SYSTEMS, MATHEMATICAL" and "MOLECULAR, BIOLOGY, IMMUNOLOGY" in 2007, then changed to the direction of "MATHEMATICS, SYSTEMS, MATHEMATICAL". Thus, "MATHEMATICS, SYSTEMS, MATHEMATICAL" has been the core topic in studies of AI applications in cyber security research. It is not only the earliest active discipline in the field but has also been a hot discipline in recent years.

Implications of networks connected in terms of collaboration and citation networks

Country implications

As mentioned, cyber attacks are increasing day by day. Around 70% of Internet of Things (IoT) devices are vulnerable to hacking. Recently, Pakistani banks were hit by biggest cyber attacks in the country's history. Hackers stole Rs. 2.6 million via debit cards issued by the Islami Bank of Pakistan and sold the data of 8000 account holders. Hackers have stolen more than 1 billion dollars from bank accounts around the world. Figure 9 presents a network consisting of 68 nodes and 493 links involving collaborating countries between 2007 and 2018. As can be seen, the major contributions come from the United States and China. The United States is the largest contributor, publishing 1148 papers. One possible reason is that 22.5% of all hacking attacks come from within the United States. Almost

Fig. 9 Country network of papers on AI applications in cyber security

27 million Americans had their identities stolen in the last 5 years. Therefore, the United States dominates research on AI applications in cyber security. On the other hand, 18.5% of all hacking attacks originate from inside China, which, with a frequency of 1086 articles, ranks second. A total of 16,000 Indian websites are hacked every year, so India has paid attention to cyber security research, it ranks third, with 387 papers. England ranks fourth, with 276 articles.

Interestingly, several countries have relatively low article frequencies but high centrality values. France leads other countries (see purple node rings in Fig. 9). France is an important node in the network, with the highest betweenness centrality: France has considerable influence within the network by virtue of their control over information passing between other countries.

Journal implications

Figure 10 displays the co-citation network of papers on AI applications in cyber security published between 2007 and 2018. The network contains the most frequently cited 386 journals, along with 1909 co-citation links among them. The journals are sorted in terms of article frequency. It can be seen that "LECT NOTES COMPUT SC" (*Lecture Notes in Computer Science*) is first, with a frequency of 1347, followed by "EXPERT SYST APPL" (*Expert Systems with Applications*) and "INFORM SCIENCES'' (*Information Sciences*) with 754 and 510 co-citations respectively. The publisher of *Lecture Notes in Computer Science* is American publishing company Springer. It is distributed in the United States, Canada, India, Australia and several European countries. This result indicates that the United States is densely connected with the world in terms of its journals.

Institution implications

As shown in Table 3, most of the important research institutions are located in China. China's important research institutions include the Chinese Academy of Sciences, Beijing University of Posts and Telecommunication and Tsinghua University. The Chinese Academy

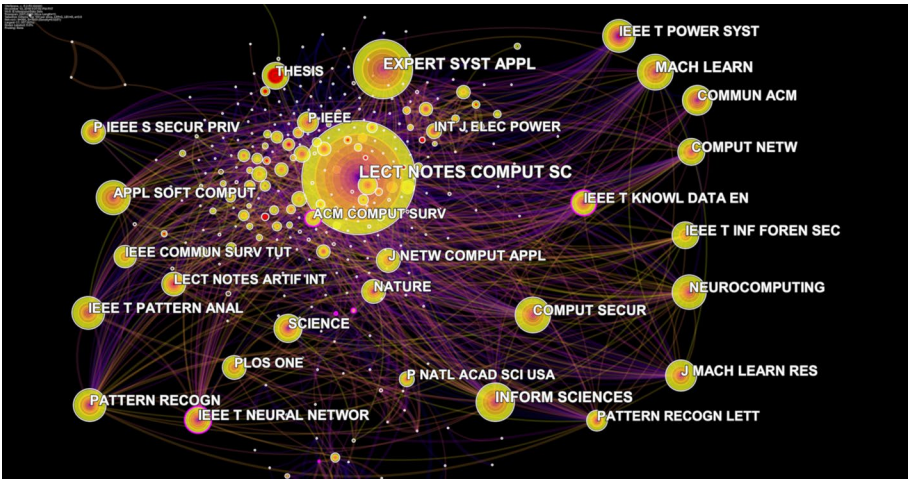


Fig. 10 Journal co-citation network of research on AI applications in cyber security

Table 3 World's top 10 institutions in publications on AI applications in cyber security

Serial	Institute	No. of Publications	City	Country	Continent
1	Chinese Academy of Sciences	102	Beijing	China	Asia
2	Islamic Azad University	61	Tehran	Iran	Asia
3	Beijing University of Posts and Telecommunications	40	Beijing	China	Asia
4	King Saud University	38	Riyadh	Saudi Arabia	Asia
5	University of Malaya	34	Kuala Lumpur	Malaysia	Asia
6	Indian Institutes of Technology	31	New Delhi	India	Asia
7	Nanyang Technological University	31	Singapore	Singapore	Asia
8	Deakin University	29	Geelong	Australia	Australia
9	University of California, San Diego	28	California	United States	America
10	Tsinghua University	28	Beijing	China	Asia

of Sciences is in first place, with a frequency of 102 articles. In second place is Islamic Azad University of Iran, with a frequency of 61 articles. Other institutions participating in research on AI in cyber security include King Saud University (Saudi Arabia) and the University of Malaya (Malaysia). Asian institutions have played an important role in research on AI applications in cyber security: Eight of the world's top 10 institutions are in Asia.

Author implications

The co-authorship network for this field (see Fig. 11) is obtained using the VOSviewer. The minimum number of published articles is three. Out of 13,803 authors, 917 meet this

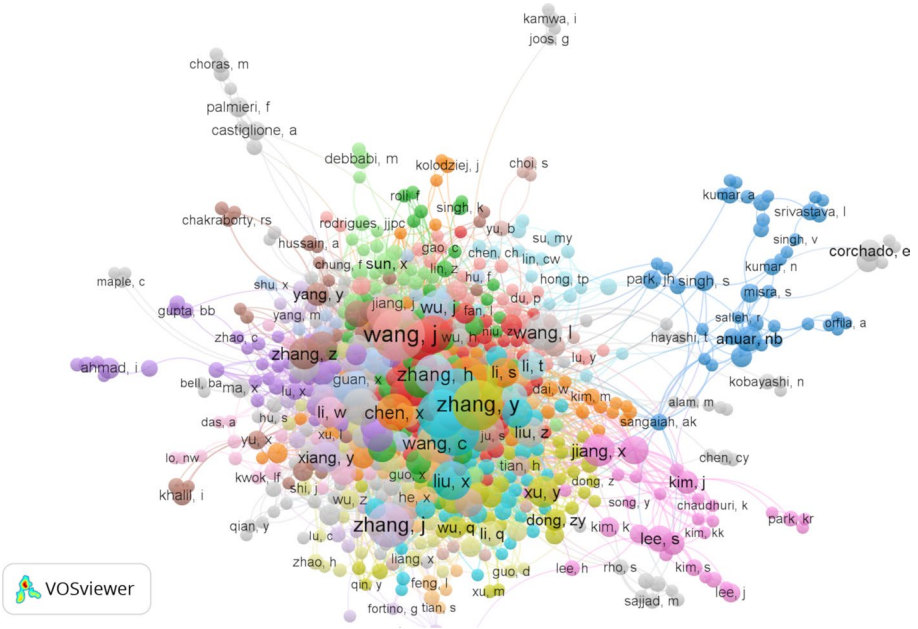


Fig. 11 Co-authorship network

criterion. In the next step, 242 authors who lack co-authorship are excluded, leaving 675 authors for this analysis.

A cluster analysis of the co-authorship network indicates that this network includes 29 clusters in different colors. The most important cluster, "Wang J" is shown in pink. Wang J has 52 articles, 606 citations and link strength of 127. The second most important cluster "Zhang Y" is shown in light green. Zhang Y has 49 articles, 373, citations and link strength of 127. Authors with higher degrees of centrality are more central in the network structure and tend to have a greater capacity to influence others. As we see in Fig. 11, Wang J and Zhang Y are the most active authors, with 127 links, and have the highest degree of collaboration. Wang Y, Li Y, Liu Y, and Chen Y have link strengths of 115, 99, 89 and 87 respectively. The co-authorship analysis indicates that most of the authors of papers on AI in cyber security are densely connected with each other in terms of collaboration and citations.

Conclusions and discussion

The knowledge map of AI applications in cyber security is visualized. Through the co-cited references network analysis, co-occurrence keywords network analysis, burst references analysis, burst keywords analysis and dual-map overlays analysis, the structural changes, hotspots and emerging trends of AI applications in cyber security have been identified in a multi criteria and comprehensiveness way. Besides, we generated the area distribution of AI applications in cyber security research all over the world.

Country, journal, institution, and author implications of networks

The application of AI in cyber security is spreading across the globe, especially in the United States, China and Europe. A growing number of scholars are paying attention to this phenomenon because cyber attacks are increasing rapidly. The Online Trust Alliance (OTA) named 2017 "the worst year ever in data breaches and cyber-incidents around the world." The OTA claims that the number of cyber attacks doubled in 2017, with ransomware leading the way. Therefore, it is necessary to improve cyber security with the help of AI applications. As Fig. 9 shows, the United States is densely connected in terms of collaboration and citations with other countries in the research on AI applications in cyber security; it is also the largest research contributor, having published 1148 articles. China is also densely connected in terms of collaboration and citations, as shown in Table 3, most of the important research institutions are located in China. In continental terms, Asia dominates research on AI applications in cyber security. As Fig. 10 shows, *Lecture Notes in Computer Science* is a top journal and has published 1347 articles related to AI in cyber security. Its publisher is American company Springer and it is distributed in the United States, Canada, India, Australia, and several European countries.

Data from the WoS show that the number of published and cited papers on AI applications in cyber security has grown rapidly in recent years. The United States is densely connected in terms of both journals and collaboration. Dutch journal *Expert System Applications* is ranked second, with 754 articles, and it is distributed in around 24 countries. Several countries, like France and the Netherlands, have fewer articles but are densely connected with other countries. Regarding authorship, Fig. 11 shows that most of the authors (e.g., Wang J, Zhang Y, Wang Y, Li Y, Liu Y and Chen Y) are densely connected with each other in terms of collaboration and citations.

Structural changes in cyber security after AI emerged

The indicators show that structural changes have occurred since AI came into use with cyber security:

1. According to the co-cited reference network indicator (see Table 2), the early research in cyber security focused on basic security problems (intrusion detection, p2p data, attacks, privacy, data security), mainly because people were concerned about security. In recent years, amid the impacts of machine learning and android malware detection, research in cyber security has risen to a new level represented by "Adversarial machine learning (2013)" and "private k-mean (2012)". The thematic patterns in the scientific literature differ over time, which indicates that structural changes in the field have appeared continuously since AI first emerged.
2. The time zone map of the co-occurrence keywords network (see Fig. 5) indicates that from 2007 to 2010, most of the literature of AI in cyber security was reflected in the following keywords: "system," "security," "algorithm," "model," "machine learning," "classification" and "support vector machine". Later, "food security," "artificial intelligence," "detection system," "random forest," "malware detection," "deep learning," "internet of things" and "extreme machine learning" were the focal keywords from 2011 to 2014. Later, "fuzzy set," "data privacy," "cyber security," "sensor," "stenography," "k-mean cluster," "cyber physical system," "learning artificial intelligence," "privacy

preserving," "confidentiality" and "feature extraction" were the emerging keywords from 2015 to 2018. Changes in the research on the use of AI in cyber security have been continuous since 2007.

3. The timeline map of the co-occurrence keywords network (see Fig. 7) shows the structural changes in the field. We see that "sensor network" was researched earliest and "information security cryptography" was the starting point. Moreover, the "transient security assessment" hotspot "classification algorithm model" promoted the emergence of "artificial neural networks". The divergent directions of the curve of "artificial neural networks" show that it gave birth to today's research on cloud cyber security.

Intellectual landscape, emerging trends, hotspots and research agenda in AI-mediated cyber security domain

The intellectual landscape of research on AI applications in cyber security depicted by the co-cited references network and co-occurring keywords network is shown in Figs. 3 and 5. The comprehensive map in Fig. 12 summarizes the findings of the different indicators for the clusters, burst references, keywords and landmark references. It shows hotspots and emerging trends in studies on AI in cyber security. The x-axis represents time (year) and the y-axis represents the relative importance of the hotspots, divided into 10 levels. In the cluster analysis, the hotness level is measured according to the size of the clustering, regarding the landmark references, this is judged according to the citation counts, burst references and burst keywords are measured according to their burst strength. Based on the above, we can draw the following comprehensive conclusions. Hotspots appeared first in 2007 (the staring year of our query) and grew rapidly from 2011. As shown in Fig. 12, the hotspots and emerging trends in studies on AI applications in cyber security produced by different indicators are not exactly the same. The hotspots are concentrated in the security field (including "anomaly detection," "intrusion detection," "face recognition," "pattern recognition," "fraud detection" and "network security").

The emerging hotspots include "intelligence in IDS," "random forests-based network IDS," "stenography," and "fuzzy set". Moreover, "deep neural network for speech recognition," "social network," "face recognition," and "artificial intelligence for cyber security"

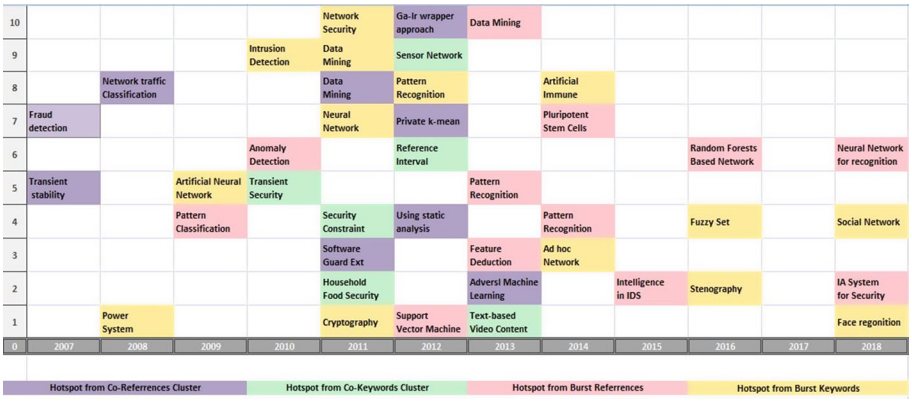


Fig. 12 Overall perspective of hotspots and trends in studies of AI applications in cyber security. No hotspot is observed in 2017

show the structural changes that have been taking place in the security field and reflect the next research frontiers. The co-cited reference network shown in Fig. 3 indicates that "private k-mean," "using static analysis," and "adversarial machine learning" have been research frontiers. Structural changes appear continuously, showing that this field is still emerging and developing.

Limitations and future outlook

Although the WoS core collection was chosen as the study's data source, we may have missed some important research publications on AI applications in cyber security. To ensure high data quality, this study selected only articles from the SCIE database, which may also have led us to omit some important research results (e.g., books, Ph.D. theses, SSCI database).

Furthermore, "Top 100 per slice" was set as the standard for data extraction using CiteSpace V, which will also have had some effect on the analyses. In the future, we will perform a detailed analysis of studies on AI applications in cyber security using soft clustering analysis, multidimensional analysis, factor analysis and other visualization and mapping techniques (Gautam 2019). We also plan to use a Latent Dirichlet Allocation (LDA) model for text clustering in the future. Evidence-based policy programs could also be planned using scientometric research (Li et al. 2018), search engine-based metrics (Omar et al. 2017), and new altmetric indicators (Holmberg and Park 2018; Park et al. 2018).

Acknowledgements I wish to acknowledge someone who means a lot to me, my father (Mr. Irshad Hussain), for showing faith in me and giving me the liberty to make my own choices. I salute you for the selfless love, care, pain and sacrifice you offered to me in order to shape my life.

References

Aghion, P., Jones, B. F., & Jones, C. I. (2017). Artificial intelligence and economic growth. *NBER Working Paper Series*. https://doi.org/10.3386/w23928.

Byres, E. (2004). The myths and facts behind cyber security risks for industrial control systems. *Proceedings of the VDE Kongress*. https://rampages.us/keckjw/wp-content/uploads/sites/2169/2014/11/Myths-and-Facts-for-Control-System-Cyber-security.pdf

Chen, C. (2006). CiteSpace II: Detecting and visualizing emerging trends and transient patterns in scientific literature. *Journal of the American Society for Information Science and Technology*. https://doi.org/10.1002/asi.20317.

Chen, C. (2016). *How to use CiteSpace*. British Columbia, Canada: Lean Publishing. Retrieved from https://leanpub.com/howtousecitespace.

Chen, C., Dubin, R., & Kim, M. C. (2014). Orphan drugs and rare diseases: A scientometric review (2000–2014). *Expert Opinion on Orphan Drugs, 2*(7), 709–724. https://doi.org/10.1517/21678707.2014.920251.

Chen, C., & Leydesdorff, L. (2013). Patterns of connections and movements in dual-map overlays: A new method of publication portfolio analysis. *Journal of the American Society for Information Science and Technology*. Retrieved from https://www.researchgate.net/publication/236039476_Patterns_of_Connections_and_Movements_in_Dual-Map_Overlays_A_New_Method_of_Publication_Portfolio_Analysis.

Chen, H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS Quarterly, 36*(4), 1165–1188. https://doi.org/10.1145/2463676.2463712.

Dilek, S., Cakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *International Journal of Artificial Intelligence & Applications, 6*(1), 21–39. https://doi.org/10.5121/ijaia.2015.6102.

Gautam, P. (2019). A bibliometric approach for department-level disciplinary analysis and science mapping of research output using multiple classification schemes. *Journal of Contemporary Eastern Asia, 18*(1), 7–29. https://doi.org/10.17477/jcea.2019.18.1.007.

Göztepe, K. (2012). Designing fuzzy rule based expert system for cyber security. *International Journal of Information Security Science, 1*(1), 13–19.

Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., & Witten, I. H. (2009). The WEKA data mining software: An update. *ACM SIGKDD Explorations Newsletter*, *11*. Retrieved from https://dl.acm.org/citation.cfm?id=1656278.

Hengstler, M., Enkel, E., & Duelli, S. (2016). Technological forecasting & social change applied artificial intelligence and trust—The case of autonomous vehicles and medical assistance devices. *Technological Forecasting and Social Change, 105,* 105–120. https://doi.org/10.1016/j.techfore.2015.12.014.

Holmberg, K., & Park, H. W. (2018). An altmetric investigation of the online visibility of South Korea-based scientific journals. *Scientometrics, 117*(1), 603–613.

Imran, M., Castillo, C., Lucas, J., Meier, P., & Vieweg, S. (2014). Aidr. In *Proceedings of the 23rd international conference on world wide web—WWW'14 companion*, (April) (pp. 159–162). https://doi.org/10.1145/2567948.2577034.

Jan, N., & Ludo, V. E. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*. https://doi.org/10.1007/s11192-009-0146-3.

Jha, S., & Topol, E. J. (2016). Adapting to artificial intelligence: Radiologists and pathologists as information specialists. *JAMA Journal of the American Medical Association, 316*(22), 2353–2354. https://doi.org/10.1001/jama.2016.17438.

Jin, Y., & Li, X. (2018). Visualizing the hotspots and emerging trends of multimedia big data through scientometrics. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-018-6172-5.

Kim, H. J., Jeong, Y. K., & Song, M. (2016). Content- and proximity-based author co-citation analysis using citation sentences. *Journal of Informetrics, 10*(4), 954–966. https://doi.org/10.1016/j.joi.2016.07.007.

Li, S., & Sun, Y. (2013). The application of weighted co-occurring keywords time gram in academic research temporal sequence discovery. *Proceedings of the American Society for Information Science and Technology*, *50*(1), 1–10. https://doi.org/10.1002/meet.14505001037.

Li, J., Xu, W. W., Wang, F., Chen, S., & Sun, J. (2018). Examining China's internet policies through a bibliometric approach. *Journal of Contemporary Eastern Asia, 17*(2), 237–253. https://doi.org/10.17477/jcea.2018.17.2.237.

Litman, T. (2014). Autonomous vehicle implementation predictions implications for transport planning. *Transportation Research Board Annual Meeting, 42*(January), 36–42. https://doi.org/10.1613/jair.301.

Liu, S., Chen, C., Ding, K., Wang, B., Xu, K., & Lin, Y. (2014). Literature retrieval based on citation context. *Scientometrics, 101*(2), 1293–1307. https://doi.org/10.1007/s11192-014-1233-7.

Loebbecke, C., & Picot, A. (2015). Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. *Journal of Strategic Information Systems, 24*(3), 149–157. https://doi.org/10.1016/j.jsis.2015.08.002.

Machine, P., & Tools, L. (n.d.). *Datamining. Practical machine learning tools and technicals with java implementations.*

Malav, A., Kadam, K., & Kamat, P. (2017). Prediction of heart disease using K-means and artificial neural network as hybrid approach to improve accuracy. *International Journal of Engineering and Technology, 9*(4), 3081–3085. https://doi.org/10.21817/ijet/2017/v9i4/170904101.

Ofli, F., Meier, P., Imran, M., Castillo, C., Tuia, D., Rey, N., et al. (2016). Combining human computing and machine learning to make sense of big (aerial) data for disaster response. *Big Data, 4*(1), 47–59. https://doi.org/10.1089/big.2014.0064.

Omar, M., Mehmood, A., Choi, G. S., & Park, H. W. (2017). Global mapping of artificial intelligence in Google and Google Scholar. *Scientometrics, 113*(3), 1269–1305. https://doi.org/10.1007/s11192-017-2534-4.

Pak Chung, W., Chen, C., Gorg, C., Shneiderman, B., Stasko, J., & Thomas, J. (2011). Graph analytics-lessons learned and challenges ahead. *IEEE Computer Graphics and Applications, 31*(5), 18–29. https://doi.org/10.1109/MCG.2011.72.

Pannu, A. (2015). Artificial intelligence and its application in different areas. *Certified International Journal of Engineering and Innovative Technology, 4*(10), 79–84. https://doi.org/10.1155/2009/251652.

Park, H. J., & Park, H. W. (2018). Two-side face of knowledge building using scientometric analysis. *Quality & Quantity, 52*(6), 2815–2836.

Park, H. C., Youn, J. M., & Park, H. W. (2018). Global mapping of scientific information exchange using altmetric data. *Quality & Quantity, 53*(2), 935–955.

Parkes, D. C., & Wellman, M. P. (2015). Economic reasoning and artificial intelligence. *Science, 349*(6245), 267–272. https://doi.org/10.1126/science.aaa8403.

Ramchurn, S. D., Huynh, T. D., Wu, F., Ikuno, Y., Flann, J., Moreau, L., et al. (2016). A disaster response system based on human-agent collectives. *Journal of Artificial Intelligence Research, 57,* 661–708. https://doi.org/10.1613/jair.5098.

Saridakis, G., Benson, V., Ezingeard, J., & Tennakoon, H. (2015). Technological forecasting & social change individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*. https://doi.org/10.1016/j.techfore.2015.08.012.

Small, H., & Greenlee, E. (1980). Citation context analysis of a co-citation cluster: Recombinant-DNA. *Scientometrics, 2*(4), 277–301. https://doi.org/10.1007/BF02016349.

Su, H. N., & Lee, P. C. (2010). Mapping knowledge structure by keyword co-occurrence: A first look at journal papers in Technology Foresight. *Scientometrics, 85*(1), 65–79. https://doi.org/10.1007/s11192-010-0259-8.

Wang, F. Y., Zheng, N. N., Cao, D., Martinez, C. M., Li, L., & Liu, T. (2017). Parallel driving in CPSS: A unified approach for transport automation and vehicle intelligence. *IEEE/CAA Journal of Automatica Sinica, 4*(4), 577–587. https://doi.org/10.1109/JAS.2017.7510598.

Zhou, Z. H., & Jiang, Y. (2003). Medical diagnosis with C4.5 Rule preceded by artificial neural network ensemble. *IEEE Transactions on Information Technology in Biomedicine, 7*(1), 37–42. https://doi.org/10.1109/TITB.2003.808498.

Affiliations

Naveed Naeem Abbas[1,2] · Tanveer Ahmed[3] · Syed Habib Ullah Shah[1,4] · Muhammad Omar[1] · Han Woo Park[5]

Naveed Naeem Abbas
naveednaeemabbas@gmail.com

Tanveer Ahmed
tanveerahmed@comsats.edu.pk

Syed Habib Ullah Shah
syedhabib7779@gmail.com

[1] Department of Computer Science and IT, The Islamia University of Bahawalpur, Bahawalpur, Pakistan

[2] H/No. 39-A, Jamal-E-Sarwar Colony, Chowk Churratah, Dera Ghazi Khan, Pakistan

[3] Department of Computer Science, COMSATS University, Islamabad, Pakistan

[4] H/No. 2147, Block 18, College Chowk, Dera Ghazi Khan, Pakistan

[5] Department of Media and Communication, Interdisciplinary Program of Digital Convergence Business, YeungNam University, 214-1, Dae-dong, Gyeongsan-si, Gyeongsangbuk-do 712-749, South Korea