International Journal of Innovative Research and Scientific Studies, 8(7) 2025, pages: 418-441

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Bio-inspired computational intelligence (BioCOIN) for cyber security during COVID-19 pandemic: A bibliometric review

Israel Edem Agbehadji[1], Abdultaofeek Abayomi[2], Oluwasegun Julius Aroba[3*], Emmanuel Freeman[4], Richard Nana Nketsiah[5]

[1]*Centre for Global Change, Sol Plaatje University, Kimberly 8301, South Africa / Honorary Research Associate, Faculty of Accounting and Informatics, Durban University of Technology, Durban 4001, South Africa.*

[2]*Research Associate, Faculty of Engineering, Built Environment and Information Technology, Water Sisulu University, Buffalo City Campus, East London 5200, South Africa | Innovation and Advanced Science Research Group (IASRG), Summit University, PMB 4412, Offa 250101, Kwara State, Nigeria.*

[3]*Centre for Ecological Intelligence Department, Faculty of Engineering and the Build Environment (FEBE), University of Johannesburg, Johannesburg 2006, South Africa.*

[3]*Operations and Quality Department, Faculty of Management Science, Durban University of Technology, South Africa 4001.*

[1,4,5]*Faculty of Computing and Information Systems, Ghana Communication Technology University, PMB 100. Accra North, Ghana.*

Corresponding author: Oluwasegun Julius Aroba (*Email: jaroba@uj.ac.za*)

Abstract

The COVID-19 pandemic profoundly disrupted the global economy, accelerating e-commerce and online activities while increasing the vulnerability of Information Technology (IT) systems. This paper aims to review the role of bio-inspired algorithms in enhancing cyber-security during the pandemic, addressing an evident research gap in this domain. A systematic review was conducted using data obtained from an online repository with broad coverage, focusing on the period 2020–2022. This timeframe captures the onset, peak, and aftermath of the pandemic. The study analyzed computational systems and applications that incorporated bio-inspired algorithms for security purposes. The review reveals that bio-inspired algorithms were already in use for cyber-security prior to the pandemic, with notable applications in Internet of Things Cyber-Physical Systems (IoT-CPS)-based Trojan detection circuits and network-layer optimization of security settings. However, the pandemic accelerated the need for resilient cyber-security frameworks and highlighted the potential of bio-inspired methods to adapt to rapidly evolving digital threats. Bio-inspired algorithms represent a valuable approach to strengthening cyber-security in times of crisis. Their adaptability and robustness make them suitable for addressing dynamic threats in increasingly interconnected ecosystems. The findings emphasize the need for continuous integration of bio-inspired approaches into cyber-security policies and infrastructures. Doing so can support more resilient digital ecosystems, enhance organizational processes, and promote better work practices in both crisis and post-crisis environments.

Keywords: Bio-inspired algorithm, COVID-19 pandemic, Cyber security systems.

DOI: 10.53894/ijirss.v8i7.10458
Funding: This research support from Operations and Quality Department, Faculty of Management Science, Durban University of Technology.
History: Received: 8 August 2025 / **Revised:** 11 September 2025 / **Accepted:** 15 September 2025 / **Published:** 2 October 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

Information is key to the success of an organization and when an unauthorised person accesses it then its security could be compromised. In view of this, the global COVID-19 pandemic created an opportunity for personal data to be compromised because of the over reliance on the internet for commerce, and many other online electronic activities. These activities created a surge in internet use which further increased cyber-related crimes. Moreover, the health sector is among the sectors that recorded high cybercrimes during the global COVID-19 pandemic [1].

The over-reliance on the internet, especially during COVID-19 exposed personal data even more than ever before, thus, leading to coining of words like "cyber pandemic" which refers to a pandemic that increased cyber activities to a greater extent. Thus, the impact on many organizations and their employees was severe. For instance, since employees were allowed to work from their homes and even perform critical job functions with their own devices such as personal laptops and other mobile, it exposed organizational data to breaches. Again, it was common for people to receive unsolicited emails and because majority of the people, especially first time technology users, were uninformed about how cyber-attacks are perpetuated, it created a high number of cyber-security related challenges. For instance, during the early months of COVID-19 disease outbreak, about 30,000 cyber-attacks, 907,000 spam messages, 737 malware incidents and 48,000 malicious uniform resource locators were recorded [2]. Fortunately, Google blocked approximately 18 million COVID-19-related spam daily. Also, average ransomware payment increased to 60% and phishing attacks increased by 220%. Both developed nations and developing nations were greatly impacted by cyber-related attacks. The COVID-19 pandemic greatly affected African economies because of the shutdown of major economic sectors while greatly accelerating digitalization and increased adoption of technology [3]. Though peoples' attitude and perception of how governments could manage the pandemic are divergent, there was an effective containment of the spread of the virus through lockdown and social distance [4].

During the pandemic, many organizations developed online platforms while others leveraged on existing ones like Zoom, Microsoft Teams and many more to facilitate interactions, communications and work. Unfortunately, most information technology-based companies were overwhelmed with the demand and pressure to develop online platforms quickly, despite their technical and human capacity challenges. Thus, robust privacy-preserving methods were not well integrated in most digital platforms [5]. For instance, contact tracing mobile applications were developed to trace most infected persons, thus leading to the exposure of sensitive health-related data [6]. The pandemic changed people's working habits and organizational responses to technology. However, it is unclear how bio-inspired algorithms played a role in the development of these online platforms to ensure the security of online applications developed during the pandemic.

Bio-inspired algorithms are computational models that leveraged the behaviour and characteristics of animals in their natural environments to real-world problems including cyber-security threats. While the impact of bio-inspired methods on the security of applications or systems during the COVID-19 pandemic is limited, it is imperative to investigate this and inform policymakers and cyber security practitioners. Thus, the current investigation was carried out from the perspective of the authors to identify the themes relating to bio-inspired cyber security. It also focused on issues regarding work from home, internet connectivity, COVID-19 impact and many more. In these regards, the research reviews some bio-inspired cyber security-based systems and applications employed during the COVID-19 pandemic. Sequel to this, the research poses the following questions:

i. What are the research trends of bio-inspired cyber security applications?
ii. What is the extent of knowledge structures on bio-inspired cyber security applications and architecture?
iii. What is the extent of utilisation of bio-inspired algorithms in cyber security applications during the COVID-19 pandemic?

This review contributes to the discussion on cyber-security applications through the lens of researchers using the scientific mapping, network analysis and performance of authors who actively contributed through publications to identify thematic areas that need the most attention for policy formulation. Additionally, the study contributes by discovering the bio-inspired algorithms that facilitated the security of applications within the identified thematic areas. Therefore, this paper is organized as follows: section 2 (related work), section 3 (method and material), section 4 (results), section 5 (discussion of findings) and sections 6 (limitation, policy and practical implication), and section 7 (conclusion and future direction).

2. Related Work

2.1. Work From Home and Cyber Security Risks

Work from home (WFH) was a measure to avoid spread of the pandemic among workers in an organization. For instance, in the work environment, workers are expected to adhere to re-spacing arrangements to reduce physical body contact with each another and surfaces. In many instances, organisations that were unable to adhere to the new workspace arrangements adopted the WFH as a practice. Thus, leading to the use of many online applications from homes [7]. During the pandemic, cybercriminals exploited individuals' use of online applications, and business practices to target vulnerable individuals leading to the spread of malware and stealing vital organizations' data.

Cybercrimes can be classified as cyber-dependent and cyber-enabled attacks. The latter was the most frequent attack during the global COVID-19 pandemic with phishing attempts being the most popular method. Email was one of the most secured means for communication in terms of transfer files, sensitive information, and messages, when most people worked from their home [8]. In phishing, malicious links are embedded in emails and when the target clicks on the link, it harvests key logging credentials of the employees to access vital business-related assets and information while acting as a legitimate employee. Sharing passwords and other security details with third parties, as well as using personal devices while working remotely were some of the security challenges. Hence, WFH was the norm during the pandemic thus highlighting the need to continue researching cyber security risks. Indeed, WFH impacted the well-being of workers as a result of stress-related factors brought on by the COVID-19 pandemic [9]. Again, the human element remained the main concern in cyber-related issues.

2.2. Internet and Network Infrastructure

During the pandemic the dependency on internet increased astronomically because employees, students, teachers and many more worked from home [10]. Internet infrastructure varies significantly across nations and while some countries have robust and advanced networks, others have limited internet infrastructure and connectivity. This divergence in internet infrastructure directly impacts the effectiveness of cybersecurity or cyber-security measures, with disparities in the ability to implement and maintain advanced technologies. Networks infrastructure used in homes generally do not apply security and lack awareness of possible cybersecurity threats Vira Yudha and Wisnu Wardhani [11]. Ratnayake, et al. [12] suggested the use of ARGUS technology for seamless connectivity across multiple devices to create a smart home system While some employees leveraged public and unsecured Wi-Fi, which exposed a network to further cyber-attacks.

In developing nations where digital divide is an existing critical challenge, it is beneficial to use the publicly available Wi-Fi as they were not password protected. Unfortunately, workers who resided at locations where communication network or internet infrastructure was inadequate, could end up using unprotected open Wi-Fi. Thus, the few who can afford to use modern advanced technology to create free Wi-Fi hotspots can make them available, which is a red flag to perpetrate cyber-attacks.

2.3. Bio-Inspired Cyber Security Systems

Cyber security is the use of technologies, processes and controls to protect systems, networks, programs, devices and data from any form of attack. Meanwhile, bio-inspired method is a search strategy that is based on the behaviour and characteristics of living organisms in their natural environment [13]. On the other hand, bio-inspired computation, a branch of Artificial Intelligence (AI), is a collection of intelligent algorithms and methods that adopt bio-inspired behaviours and characteristics to solve a wide range of complex and real-world problems including detection and categorization of malware, phishing and spam attacks.

Many bio-inspired search methods have been proposed to address complex challenges in real-world such as task allocation and many optimisation problems [14, 15]. Currently, the rise in security incidents and attacks indicate the weakness of current systems to detect, prevent or defend against security breaches in organizations. Preventing unauthorised access to sensitive information is critical in pandemic and access control models that use bio-inspired computational methods could provide automation and fine-tuning of security architecture parameters to identify a different set of activities that can compromise the security of any application. A bio-inspired approach applied to design control models for auto-resilience integration that react to insider attacks can be seen in the current cyber security architecture. Furthermore, the study reported in Hernández-Herrera, et al. [16] identified limitations of existing cyber security architecture as: lack of interaction or cooperation among network devices; lack of device self-adaptation or awareness in most network architectures; there is an error-prone and time-consuming configuration of network parameters, which are ineffective in real-time attack resolution; lack of diagnostic capability when there is network misconfiguration; and conflict resolution in times of multi-vendor management of security infrastructure. Thus, bio-inspired auto-resilient security architecture was suggested to address these aforementioned limitations [16]. The advantage of the bio-inspired approach is the ability to avoid unpromising mutual interaction because it is able to make random choices and still know past interactions in order to maintain the dynamics of correct feedback control in biological regulatory networks. However, intrusion detection is a challenging cybersecurity issue and for instance, leveraging the capabilities of every single swarm intelligence model is imperative [17].

2.4. COVID-19 Impact

The impact of COVID-19 on organizations, businesses, health care, transportation, agriculture and many more sectors cannot be underestimated [15]. For instance, the impact on businesses owned by African women entrepreneurs created more social inequality in accessing financial services thus leading them out of business [18]. This notwithstanding, WFH

created a greater cybersecurity risk [19] and the impact was devastating to the global economies [20]. On the other hand, the COVID-19 pandemic created a boom in internet technology since most nations (developed and developing), restricted citizens to their homes and they practised WFH [21]. This influenced the success of cyber-attacks such as phishing and scams [22]. During the pandemic, more health-related patient isolation cases are reassigned to qualified diagnosticians and front-line health workers thus stretching hospitals beyond their capacities. In addition, the use of home computing hardware for remote diagnosis applications resulted in extensive use of network bandwidth. Thus, raising the concern of cyber risk of remote digital diagnosis platforms. The pandemic created a chaotic environment and cybercriminals exploited the chaos to inflict more cybercrimes on suffering people and embattled organizations, in terms of cybercriminals monetizing system changes for instance, to carry out their new modus operandi [23].

2.5. Environmental Policies and Cyber-Security

The concern on the relationship between cyber-security, policy, and environmental issues were intensified due to the multi-dimensional impact of the pandemic. Key among the concern is technology incorporation to create a sustainable and environmental management initiatives. In order to ensure that environmental policies and sustainable practices are implemented effectively, cyber-security is essential to safeguard environmental systems, data and network infrastructure. As sustainability activities and digital transformation grow, more effort is required toward developing a strong cyber-security measure to protect environmental eco-systems that support the work from home practices [24].

3. Method and Material

3.1. Literature Search

Bibliometric analysis was used as the method to evaluate research articles between 2020 to 2022. The method is popularly used when a large dataset needs to be analysed to find insight into the data. Bibliometric analysis is a quantitative evaluation and qualitative interpretation technique; thus, it is more suitable for this study given the large impact of COVID-19 on countries and its associated huge datasets. Secondly, the method is ideal because reviewing large datasets manually is tedious which might lead to errors in analysis. Bibliometric methods introduce quantitative rigour into the subjective evaluation of literature and provide evidence of theoretically derived categories in a review article that help to provide answers to the research questions outlined in this current study. Research articles were extracted from the Scopus database on topics relating to but not limited to cyber security, bio-inspired algorithms, and COVID-19. A total of 974 documents were extracted from Scopus for bibliometric analysis.

The methodological scheme for bibliometric analysis is established by the following steps:

Step 1 - Determine the search terms: The search for the document was achieved using the following criteria: (ALL (“bio-inspired" OR "bioinspired" OR cyber AND security AND application) OR ALL ("bio-inspired" OR "bioinspired" OR cyber AND security AND systems) AND TITLE-ABS-KEY ("COVID-19 pandemic")).

Step 2 - Dataset: This defines the database used. Scopus was selected for this study because it is a comprehensive database that covers a broad range of disciplines and has been extensively used in the bibliometric analysis. It is the largest abstract and citation database of peer-reviewed literature including scientific journals, books and conference proceedings hence it has high quality standards, disciplinary coverage and tools for data extraction and visualisation.

Step 3 - Extract data: This defines data extraction process that is achieved using keywords on the topic.

Step 4 - Article selection: This defines article selection criteria which include year of publication; document type including articles, conference paper, and review articles that are written in English language.

Step 5 - Software selection: The R programming software and its Biblioshiny package was used for Bibliometric. This software was adopted because it provides extensive techniques to help in understanding the focus of this study.

Step 6 - Analysis: This defines the analysis including research trends and impact, and knowledge structures.

3.2. Bibliometric Methodology

Bibliometric is a set of methods that quantitatively measure and evaluate research output in terms of its intellectual structure. Bibliometric analysis help uncover emerging trends in research articles, journal performance, and author performance to help understand the intellectual structure of a specific domain in the extant literature. The bibliometric method can be categorized into three including science mapping, performance analysis and network analysis.

Science mapping is aimed at extracting knowledge from the conceptual or social structure of the particular research field based on the data that is extracted. Some of these techniques are citation analysis, co-citation analysis, bibliographic coupling, co-word analysis, and co-authorship analysis. The Word analysis technique was used extensively to understand the research topics in scientific production. The types of analysis include the most frequent words, word cloud, treemap, word dynamics and trend topics. Furthermore, the analysis was conducted based on keywords Plus, the author's keyword, title or abstract.

Performance analysis as employed is a descriptive analysis that examines the impact of researchers or contributions of research constituents such as authors, institutions, countries, and journals.

In addition, Network analysis uses network metrics, clustering, and visualization to highlight the relative importance of research constituents such as co-occurrence network, authors, institutions, countries etc. which may not necessarily be reflected through publications or citations.

3.2.1. Network Metrics

These metrics provide greater clarity on the degree of centrality, betweenness centrality, eigenvector centrality, closeness centrality, PageRank, etc. [25]. The degree of centrality refers to the number of relational ties a research constituent has in a network; Betweenness centrality focuses on how a node carries information between unconnected groups of nodes, whereby a node is the research constituent such as keyword, research topic; Eigenvector centrality looks at the connectivity of nodes. The more connected the nodes are to each other show the stronger relationship and the higher the eigenvector value; while the closeness centrality focuses on how a node is closer to other nodes on the network; and pageRank analysis refers to a publication's impact.

3.2.2. Clustering

Clustering creates themes or social clusters based on the nature of the analysis. The thematic cluster on co-citation analysis shows the major themes of the intellectual structure and its development over time.

3.2.3. Visualization

This provides a clear picture of the network and its thematic structures. Example of visualization software includes VOSviewer, and Bibliometrix package in R studio. Other software includes Bibexcel, Pajek, Gephi, SciMat, Sci2, and UCINET.

Despite the aforementioned categories, this study's analysis is aligned to understand the research trends and impact, and knowledge structures as highlighted: techniques to understand the research trends and impact include main information about datasets such as annual scientific production, average citation per year, three-fields plot; source analysis; authors analysis including authors production over time, authors impact; country analysis including corresponding author's country, most cited countries, country-specific production; and words analysis such as most frequent words, word cloud, treemap, word dynamics, and trend topics. On the other hand, techniques to understand knowledge structures include clustering such as document coupling, author coupling, and source coupling; conceptual structures which include co-occurrence network, thematic map, thematic evolution, factorial analysis - factorial map of most contributing papers, factorial map of most cited paper; and intellectual structure such as co-citation network and historiography.

4. Results

This study analysed the growth in the number of publications on cyber security especially during the COVID-19. The R studio was used for the bibliometric analysis because it presents modules that enable detail analysis of the research outputs. Preliminary analysis of the search results was conducted to understand the scope of documents and field of study and the results is presented in Figures 1 and 2.

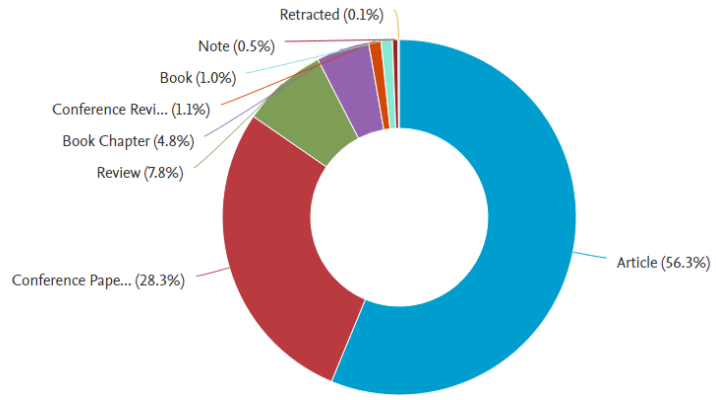

Figure 1.
Published document by type.

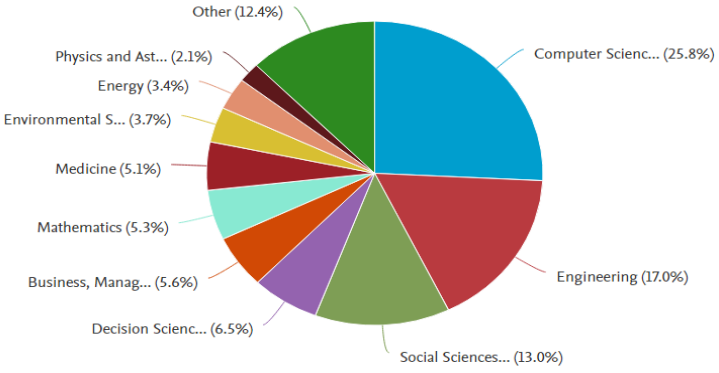

Figure 2.
Published documents by subject area.

4.1. Analysis of Research Trends and Impact

The analyses of research trends and impact are presented in this section using Tables and Figures with accompanying descriptive analysis. The analysis covers a statistical overview of the dataset, annual scientific production, average citation per year, three-field plot, source, author, country, and word analyses. Filters were applied to further narrow the search within the research topic. These include words like machine learning, artificial intelligence, and many more. The analysis starts with a general statistical overview of the dataset in Table 1. This statistical overview was generated from biblioshiny.

Table 1.
Statistical overview or main information on the dataset.

Description	Results
MAIN INFORMATION ABOUT DATA	
Timespan	2020:2022
Sources (Journals, Books, etc)	618
Documents	974
Annual Growth Rate %	71.63
Document Average Age	0.742
Average citations per doc	7.021
References	64927
DOCUMENT CONTENTS	
Keywords Plus (ID)	4357
Author's Keywords (DE)	2923
AUTHORS	
Authors	3411
Authors of single-authored docs	82
AUTHORS COLLABORATION	
Single-authored docs	93
Co-Authors per Doc	3.88
International co-authorships %	29.77
DOCUMENT TYPES	
Article	548
Book	10
book chapter	47
conference paper	276
conference review	11
Note	5
Retracted	1
Review	76

Table 1 shows the statistical overview covering main information about the dataset, document content and types, and authors. 618 documents were collected from different sources with an average citation per document of 7.021. There are 3411 authors from different document types where 548 articles are identified.

Table 2 shows that the annual scientific production of articles covering all subject area (see Figure 2) are 129, 465, 380 for 2020, 2021 and 2022 respectively while the average citation per year is also indicated. This indicates that the mean total citation per article in 2020 was 25.34 for 129 articles compared with 2021 (6.91) and 2022 (0.93) for 465 and 380 articles respectively.

Table 2.
Annual scientific production and Average Citation Per Year.

Year	Articles	Mean Total Citation per Article	Mean Total Citation per Year	Citable Years
2020	129	25.34	12.67	2
2021	465	6.91	6.91	1
2022	380	0.93	0	0

Figure 3 illustrates the Three-field plot on authors (AU), countries (AU_CO) and keywords (ID). USA tops the list of authors who contributed extensively towards research into themes considered in this study. COVID-19 pandemic was topical among the keywords plus. Also, internet of things, network security, cyber security, health care was recorded among the keywords.

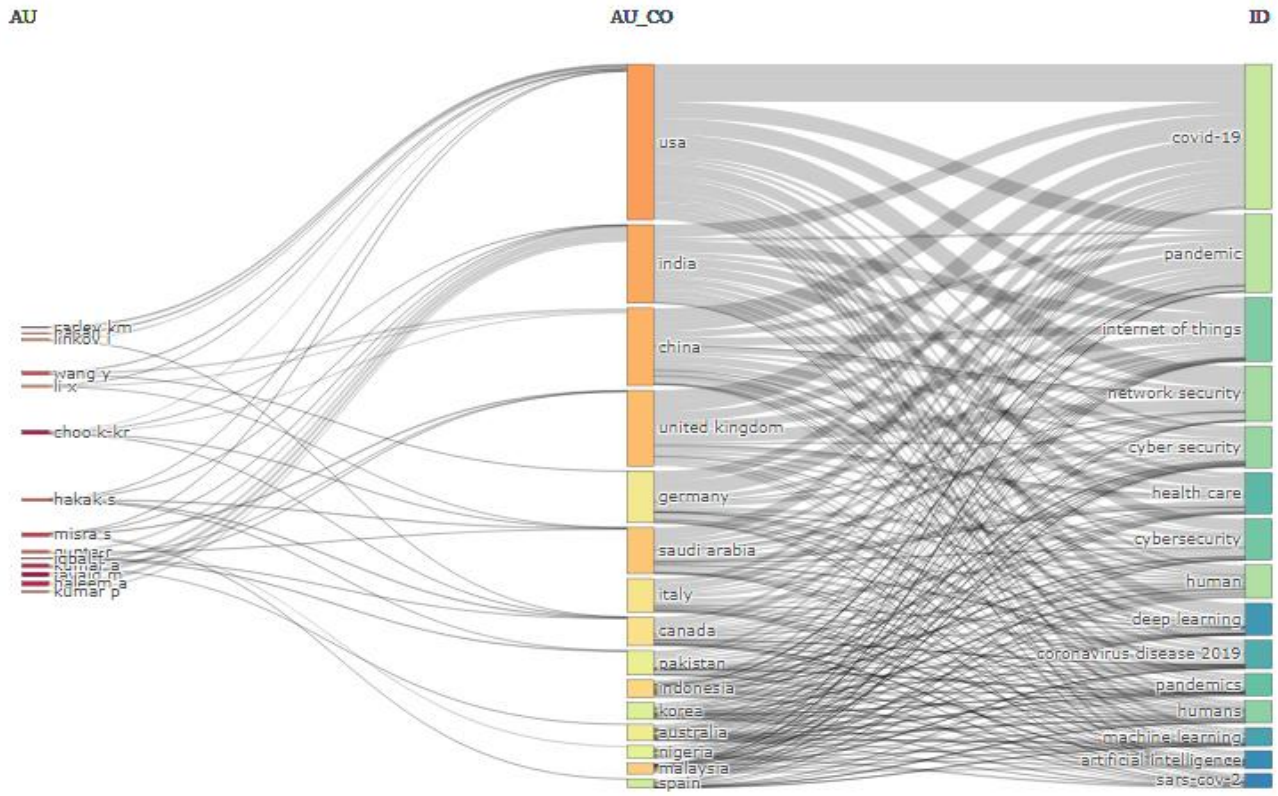

Figure 3.
Three-field plot of authors, authors' countries and keywords.

Figure 4 illustrates the source analysis which indicates that Sustainability recorded the highest (28) among the other sources for the top 10 source documents, followed by Lecture Notes in Networks and Systems (24), IEEE Access (23) and many others.

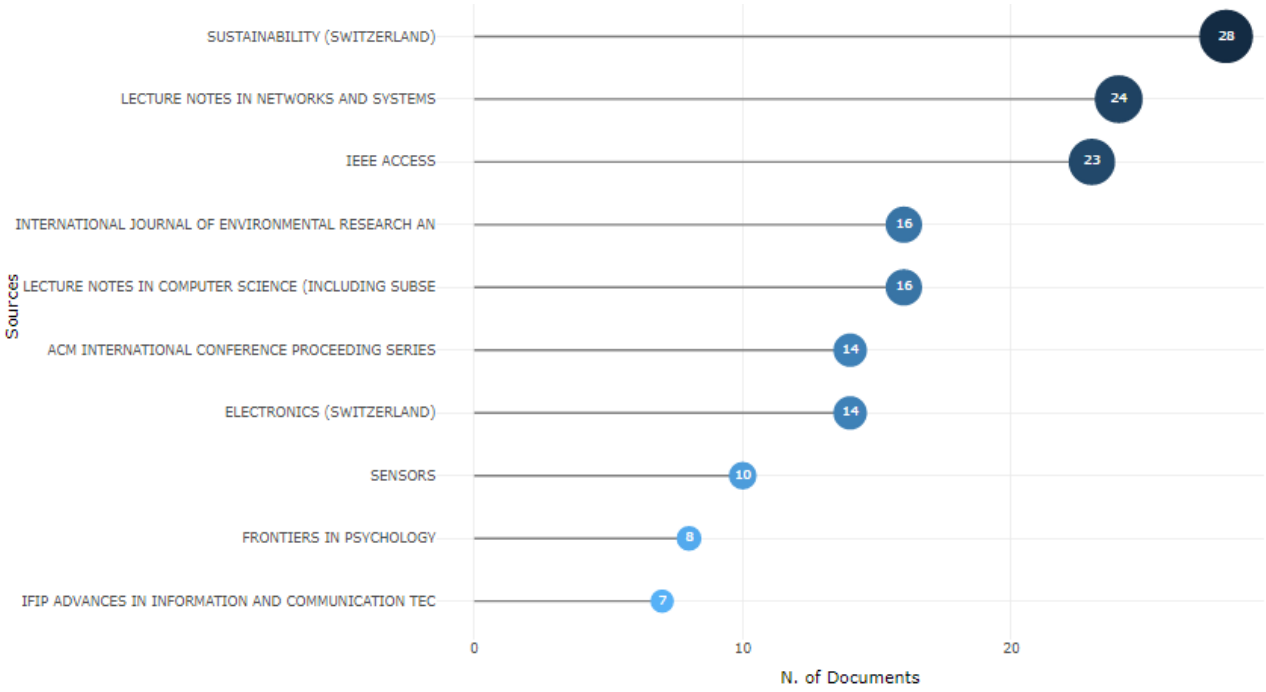

Figure 4.
Analysis of the source of documents.

Figure 5 illustrates source dynamics where Sustainability has the highest cumulative occurrence in 2021.

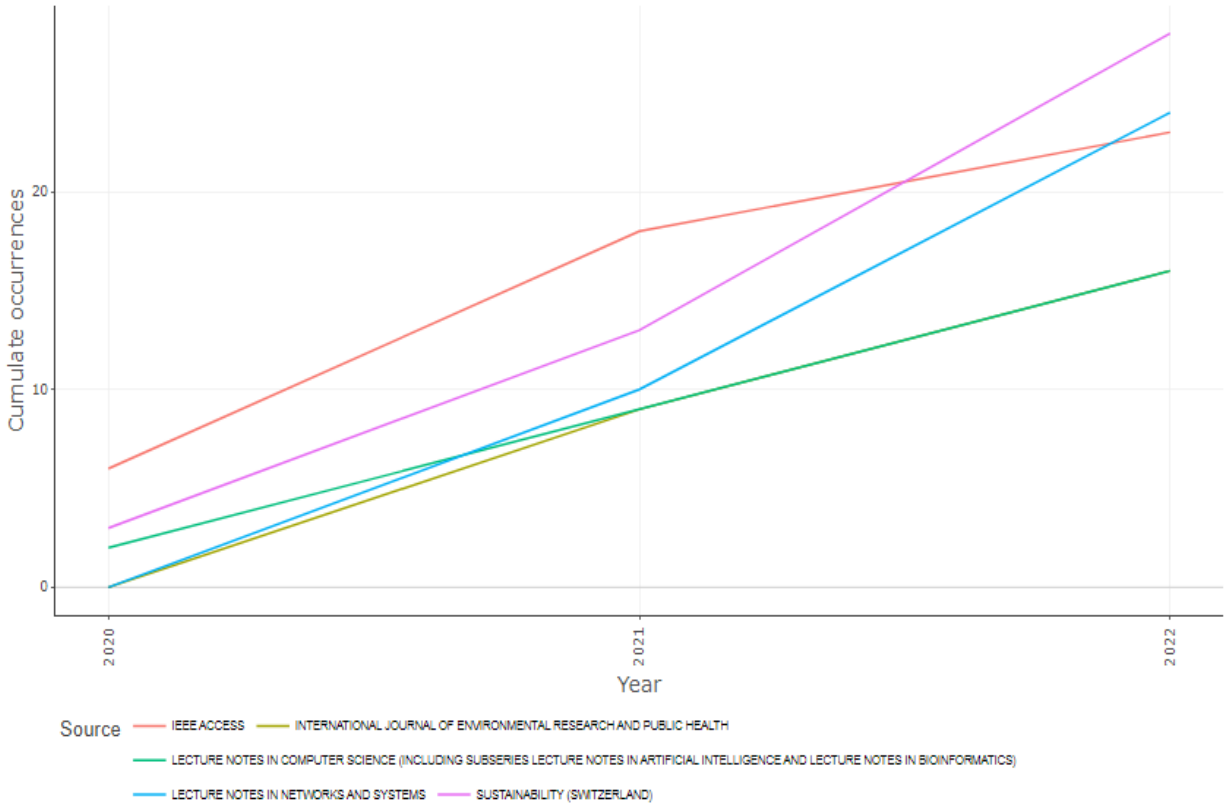

Figure 5.
Source dynamics of documents.

Figure 6 illustrates the most relevant authors and their impacts where Javaid and Haleem [26] recorded an impact of 7 followed by Choo [27] (6), Haleem, et al. [28], etc. This suggests that Javaid is the most relevant author among all the authors considered in this current study.

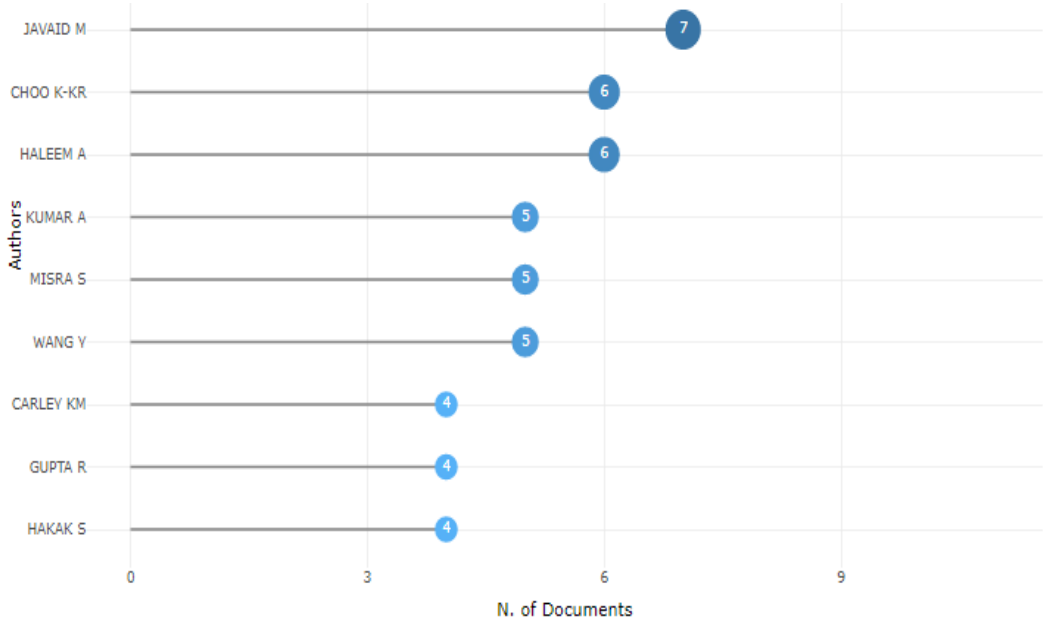

Figure 6.
Most relevant authors regarding documents and publications.
Source: Javaid and Haleem [26]; Choo [27]; Haleem, et al. [28]; Kumar, et al. [29]; Misra, et al. [30]; Wang, et al. [31]; Carley [32]; Gupta and Kohli [33] and Hakak, et al. [34].

Tables 3 and 4 shows country's scientific production and countries' production over time. On one hand, the USA leads in aspect of country's scientific production with frequency of 551 followed by INDIA (423), CHINA (260) and others for the first 10 countries. On the other hand, INDIA leads the countries' production over time during 2021 and 2022 with 222

and 423 articles respectively. It is observed that, scientific production of research scientist in Africa is conspicuously lacking which suggest a research gap.

Table 3.
Countries' scientific production.

Region	Frequency
USA	551
INDIA	423
CHINA	260
UK	257
SAUDI ARABIA	138
MALAYSIA	113
INDONESIA	112
CANADA	101
ITALY	98
GERMANY	97

Table 4.
Countries' production over time.

Country	Year	Articles
CHINA	2020	22
CHINA	2021	136
CHINA	2022	260
INDIA	2020	56
INDIA	2021	222
INDIA	2022	423
SAUDI ARABIA	2020	14
SAUDI ARABIA	2021	88
SAUDI ARABIA	2022	138
UNITED KINGDOM	2020	43

Figure 7 shows that most cited countries with INDIA constituting the highly cited country with approximately 1094 number of citations, followed by USA (905), UNITED KINGDOM (741) and others. This shows a gap required to be filled, in terms of Africa's production of research publication over time.

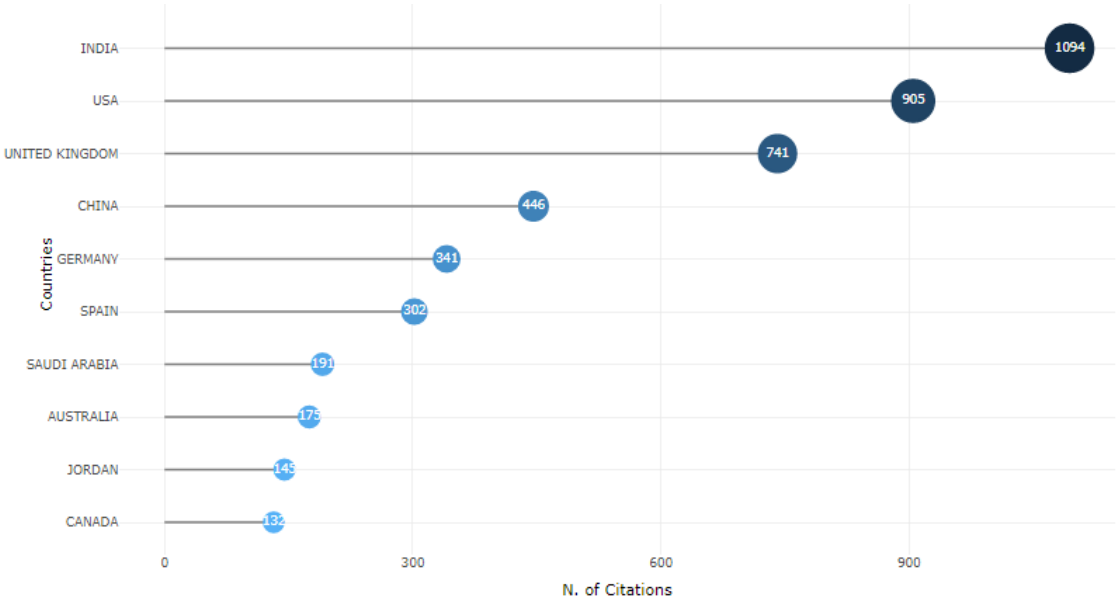

Figure 7.
Most cited publication countries.

Figure 8 shows the most frequent words recorded where the number of occurrences of COVID-19 is 207 keywords plus and cyber security constitutes 81 while pandemic has 116 keywords plus.

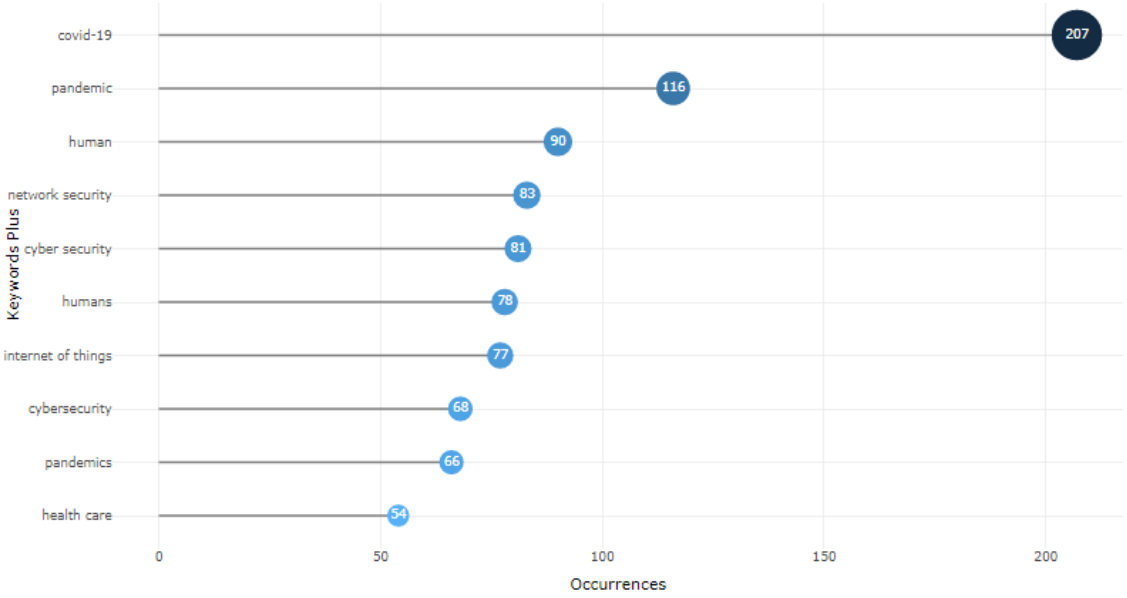

Figure 8.
Most frequent words.

Alternatively, Figure 9 shows the tree map (indicating hierarchical data in nested figures) of the top 50 words generated based on Keywords Plus, percentages, and number of occurrences of the most frequent words. The tree map indicates that COVID-19 constitutes 10% of the most frequent words, pandemic (5%), whereas machine learning, deep learning, and artificial intelligence models constitute 2% of the most frequent words. Cybersecurity or Cyber security constitutes between 3% to 4%. It is revealing that network security and the Internet of Things (IoT) also constitutes 4% of keywords plus occurrence.

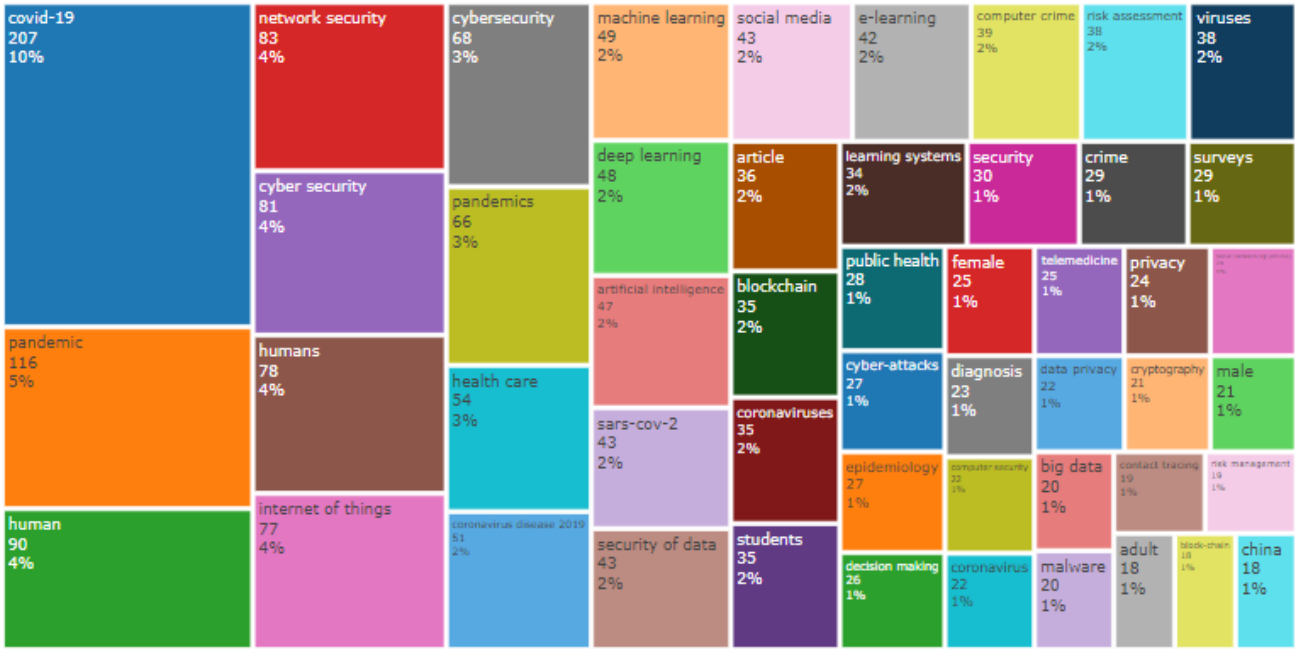

Figure 9.
Tree map of the top 50 words.

Figure 10 and Appendix A1 show the COVID-19, cyber security and machine learning as trend topics between 2021 to 2022, indicating again that the COVID-19 pandemic, human and network security are the trending topics.

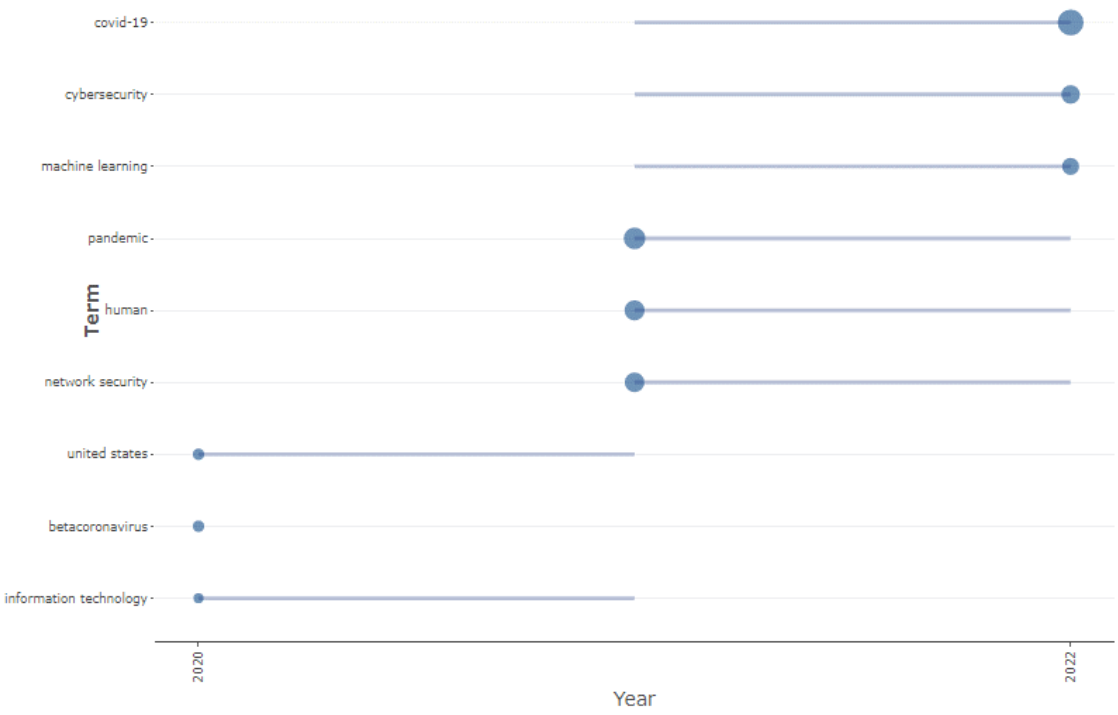

Figure 10.
Trending topics between 2020-2022.

4.2. Analysis of Knowledge Structures

The analyses of knowledge structures are presented using Tables and Figures with accompanying descriptive analysis covering clustering (i.e., clustering by coupling), conceptual structures (co-occurrence network, thematic map, thematic evolution) and intellectual structures (e.g., co-citation network).

Table 5 illustrates the three groups of different clusters. Group 1 consists of Keywords such as COVID-19, pandemic, human with their associated confidence values. Group 2 consists of cyber security, and network security with their associated confidence values and Group 3 consists of COVID-19, the internet of things, and health care within a cluster.

Table 5.
Clustering by coupling.

Label	Group	Frequency	Centrality	Impact
covid-19 - conf 43.5% pandemic - conf 85.4% human - conf 100%	1	79	0.606319906421923	1.24394998719323
cyber security - conf 95.6% network security - conf 87.2% cybersecurity - conf 85.7%	2	71	0.283312879351001	1.73180116361935
covid-19 - conf 48.8% internet of things – conf 37.5% health care - conf 34.4%	3	100	0.319855129587471	1.07463842975207

Figure 11 illustrates four quadrants, and each shows the level of centrality and impact. The upper-right quadrant contains clusters with both significant impact and high centrality. Thus, the cluster is considered as developed and important within the field of research. Cluster in the upper-left have high impact but less centrality. Thus, this cluster is considered as only marginal important. Cluster in the lower-left are both weakly developed and marginal too. Thus, the cluster have low impact and low centrality. Finally, the cluster in lower-right are important for research field but not developed, thus, contains transversal and general basic themes.

The x-axis is the centrality of the cluster using the Callon's centrality index, whereas y-axis is the impact by mean normalised local citation score. Callon's centrality measures the intensity of links between a given community and other communities where the value is measured in terms of importance of a cluster in the whole dataset. Normalised citation score of documents is actual count of citing items over the expected citation rate for the documents with the same publication year.

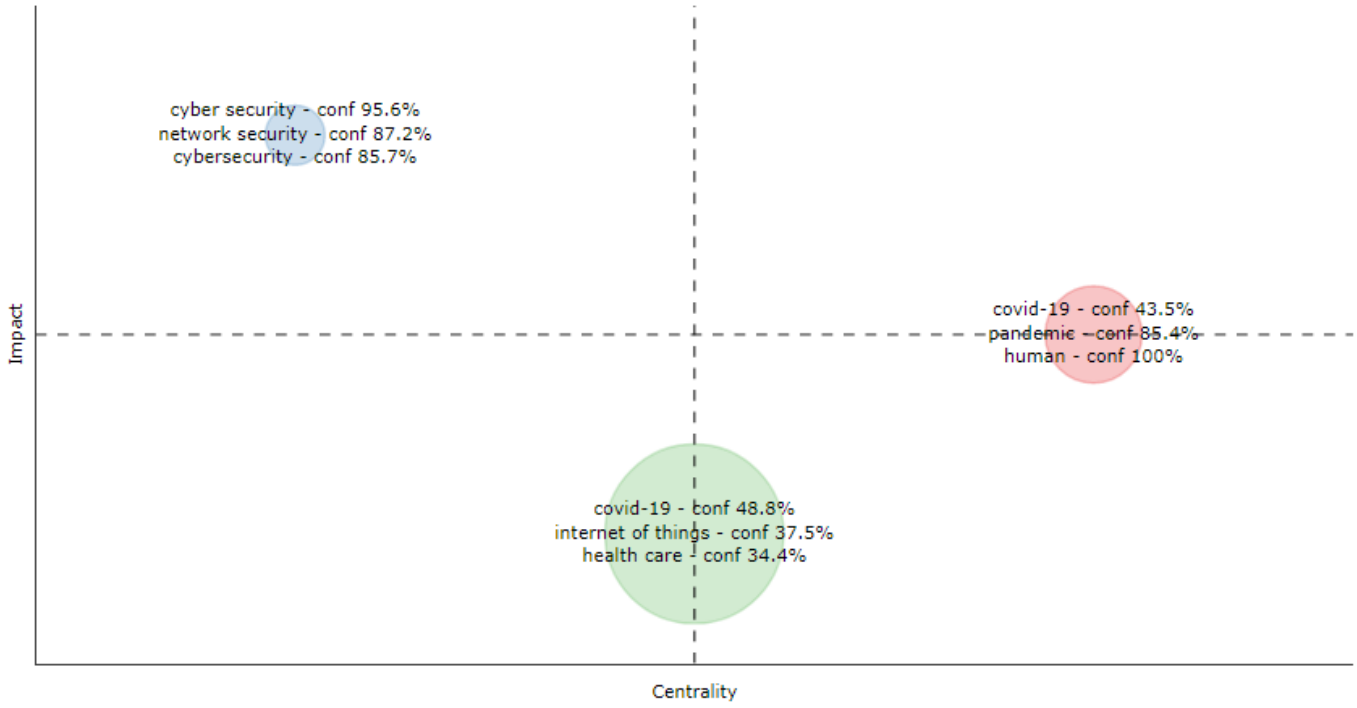

Figure 11.
Clustering by coupling.

From Figure 11, it is observed that the cluster consisting of cyber security and network security are considered as only marginal importance, because it has, from Table 5, high impact (1.73) and less centrality (0.2833). Again, the cluster consisting of COVID-19 pandemic and humans can be considered either developed, important, or at the same time contains transversal and general or basic theme because it has high centrality (0.61) and less impact (1.244). Furthermore, clusters containing COVID-19, internet of things and health care has centrality (0.32) and impact (1.07), either low impact and low centrality or contains transversal and general. Appendix A2 shows the co-occurrence network for only Group 1, for the first 10 Keywords Plus, betweenness, closeness and PageRank.

Meanwhile, Figures 12 and 13 show authors collaborations co-occurrence network map. The circle denotes the Keywords Plus where the connecting lines represent the strength of the writers' collaboration. The colours represent the various groupings and a larger circle represents the frequency of contributing keyword.

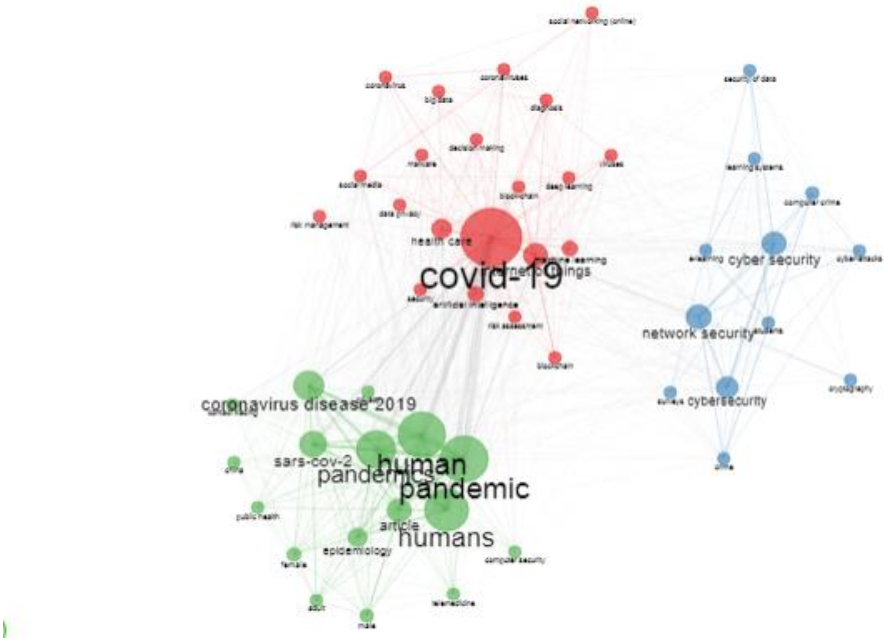

Figure 12.
Authors' collaboration co-occurrence network using network approach.

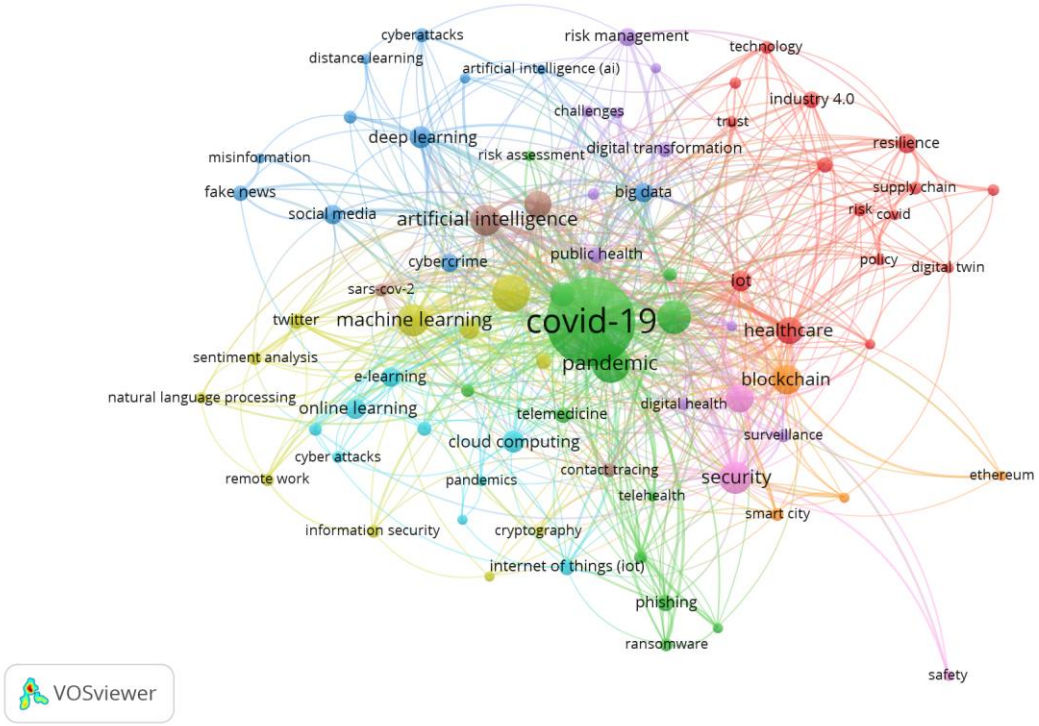

Figure 13.
Authors collaboration alternative co-occurrence network using network approach via VOSviewer.

Figure 14 and Appendix A3 show the Thematic map with three clusters. From Appendix A3, COVID-19 has high Callon Centrality (12.00) and low Callon Density (21.719), whereas network security has 5.67 Callon Centrality and 23.57 Callon Density. This suggests that COVID-19 has the highest rank density followed by network security. Figure 14 illustrates four quadrants on Thematic map namely basic themes, motor themes, niche themes and declining or emerging themes.

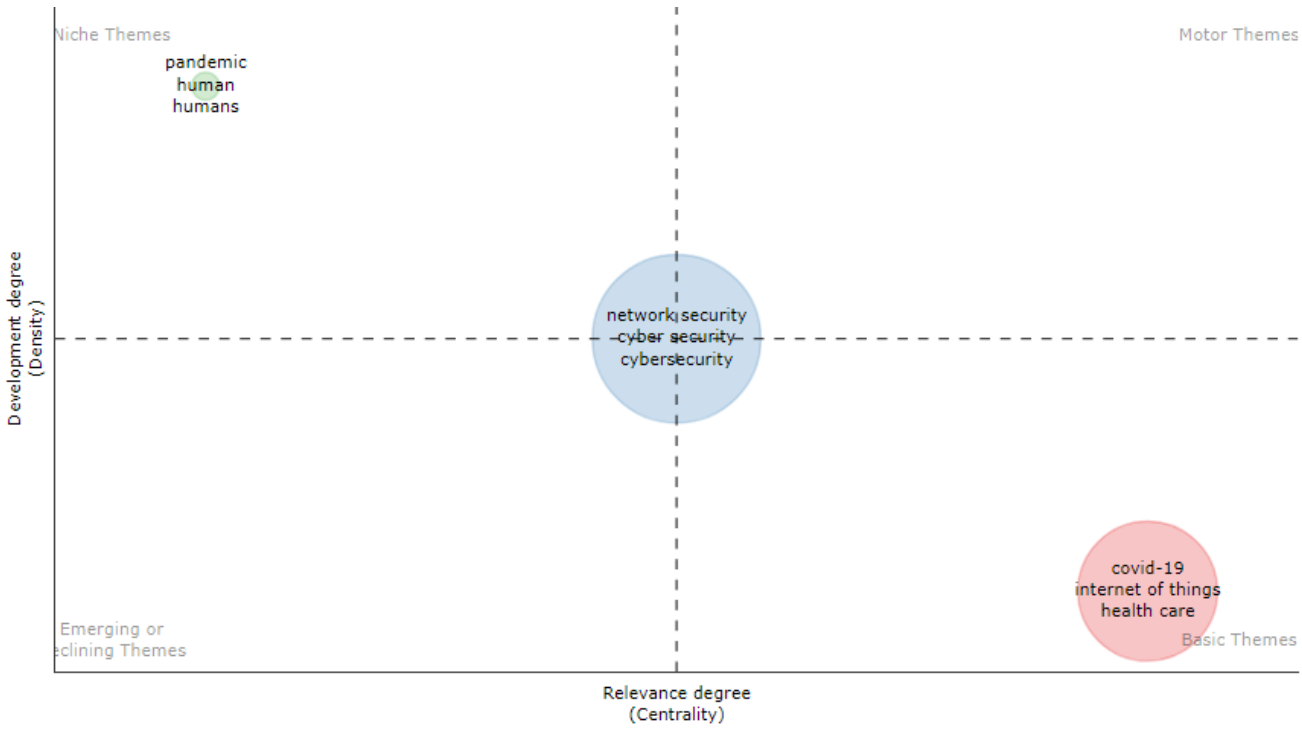

Figure 14.
Thematic map (Network approach).

Figure 14 indicates the thematic map showing that network security, cyber security themes appear in all quadrants, whereas COVID-19, Internet of things, health care were important for research field but are not developed as it contains transversal and general basic themes. Moreover, pandemic and human(s) were themes with well-developed internal ties but

unimportant external ties, which shows marginally importance for the research on bio-inspired computational cyber security. Thence, pandemic and human(s) were very specialised, highly developed, and isolated.

Figure 15 shows the thematic evolution which indicates that COVID-19 pandemic and human were highly developed themes during 2020 and 2022, and isolated. It is also observed that cyber security, network security and internet of things were evolving themes that appear in all quadrants. Again, health care, risk assessment and artificial intelligence are basic and transversal themes, which suggest that these themes are important for research field but are not developed as they contain transversal and general basic themes.

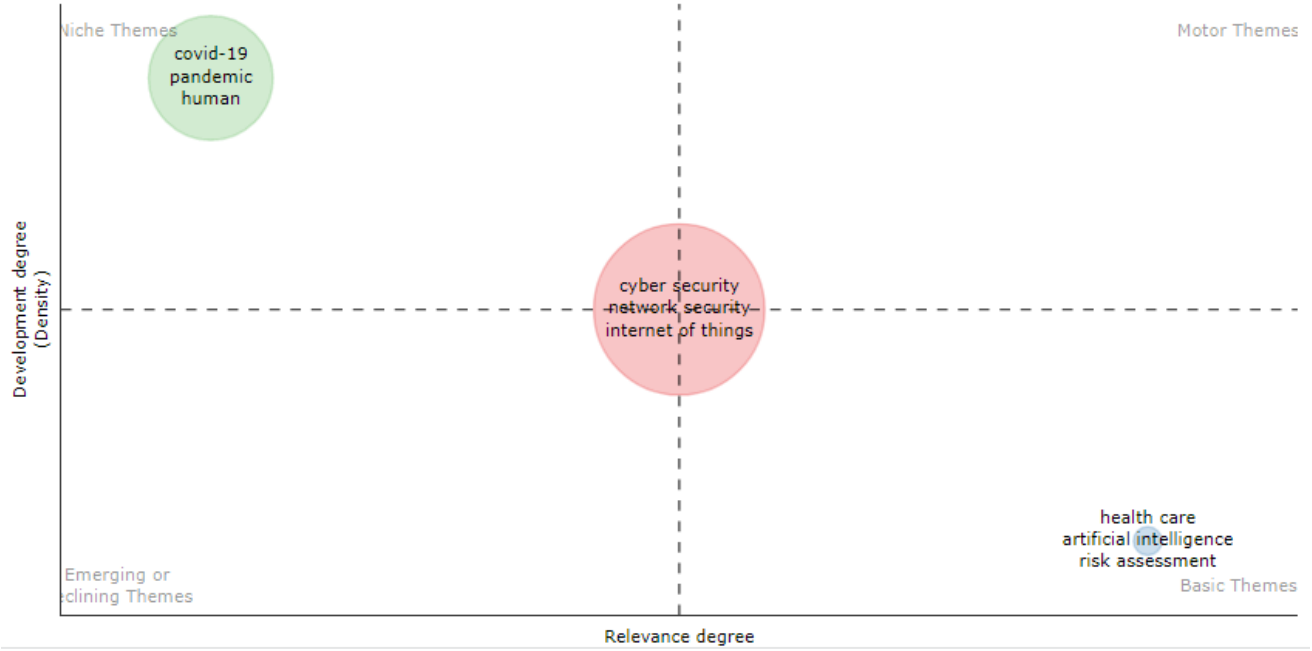

Figure 15.
Thematic evolution of themes in research areas.

Figure 16 shows that the thematic evolution analysis is a method that combines performance analysis and scientific mapping to indicate field development and quantify the evolution of the research area. The raw data is divided into distinct groups of years to make it possible to analyze the growth of the research field. The main objective is to conceptually find and identify essential terminology used between 2020 and 2022, including thematic change. Figure 16 suggests that between 2020 and 2021, COVID-19, health care, and cyber security were more represented as evolution themes, while in 2021-2022 COVID-19 pandemic, cyber security, e-learning and deep learning were more represented as evolution themes thus, suggesting evolving themes like e-learning and deep learning.

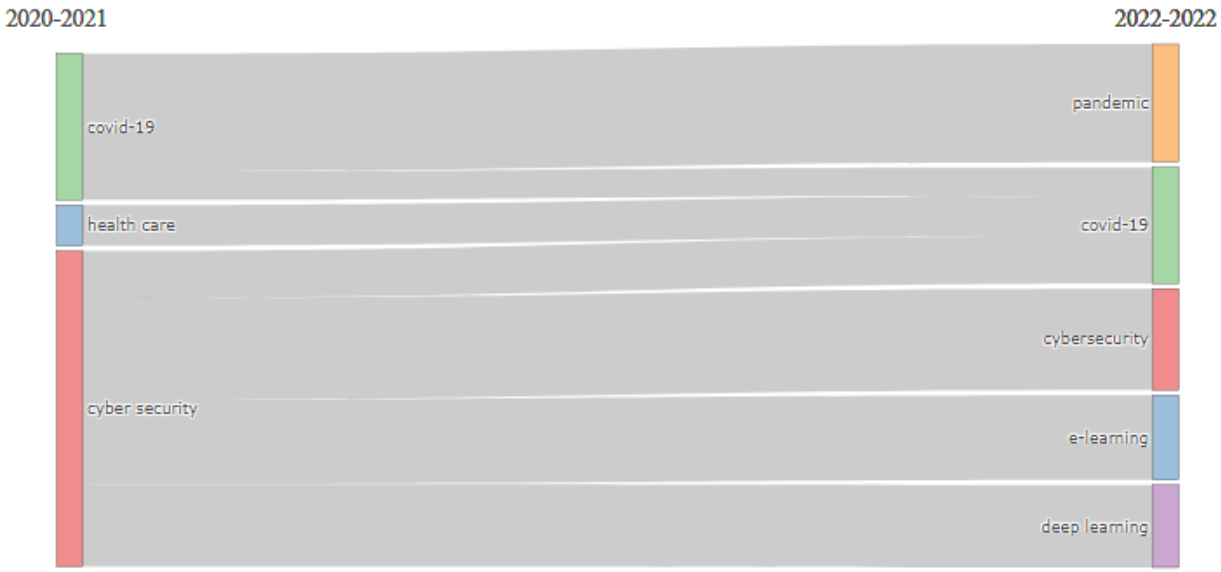

Figure 16.
Thematic evolution of bio-inspired computation intelligence keywords between 2020-2022.

In Figure 17, the conceptual structure map with Multiple Correspondence Analysis (MCA) of Keywords Plus is shown. MCA identifies cluster of documents that expresses common concepts regarding the research topic. Again, it examines the interdependence among the Keywords Plus and thus, the closer the words, the more similar they are. Therefore, MCA technique helps to visualise the relationship by transforming the keywords into two dimensional plot, with nodes, clusters and their relationship. This analysis provides insight to understand the relationship between the main research topic, keywords and other emerging subfields on the research topic. Furthermore, nodes on the conceptual map represent keywords, research topic or published articles. In this current research, an example of such node is "crime". Moreover, nodes with connecting edges indicate the relationship or co-occurrences whereas the strength of connection is determined by the closeness of each node on the plot. For instance, "cyber-attacks" and "computer crime" show some closeness. Thus, nodes that are closer to another are conceptually related, whereas nodes that are further apart are otherwise. The advantage using the conceptual map is that it showed the change on how the topic has evolved over time or research trends, which helped to track authors' contribution on the research topic.

Furthermore, a cluster consists of group of nodes that are closely related and can be visualised with different colours (blue or red). Each cluster has keywords or research topics related to each other. Hence, in the blue cluster, words such as pandemic, human, epidemiology, human(s) and SARS cov2 are more similar representing closely related topics. Thus, they contribute by providing more insight into other subfields. The red cluster is the largest network of Keywords Plus providing insight on the main research topic of cyber security including network security, cyberattacks, malware, cryptography, crime, etc.

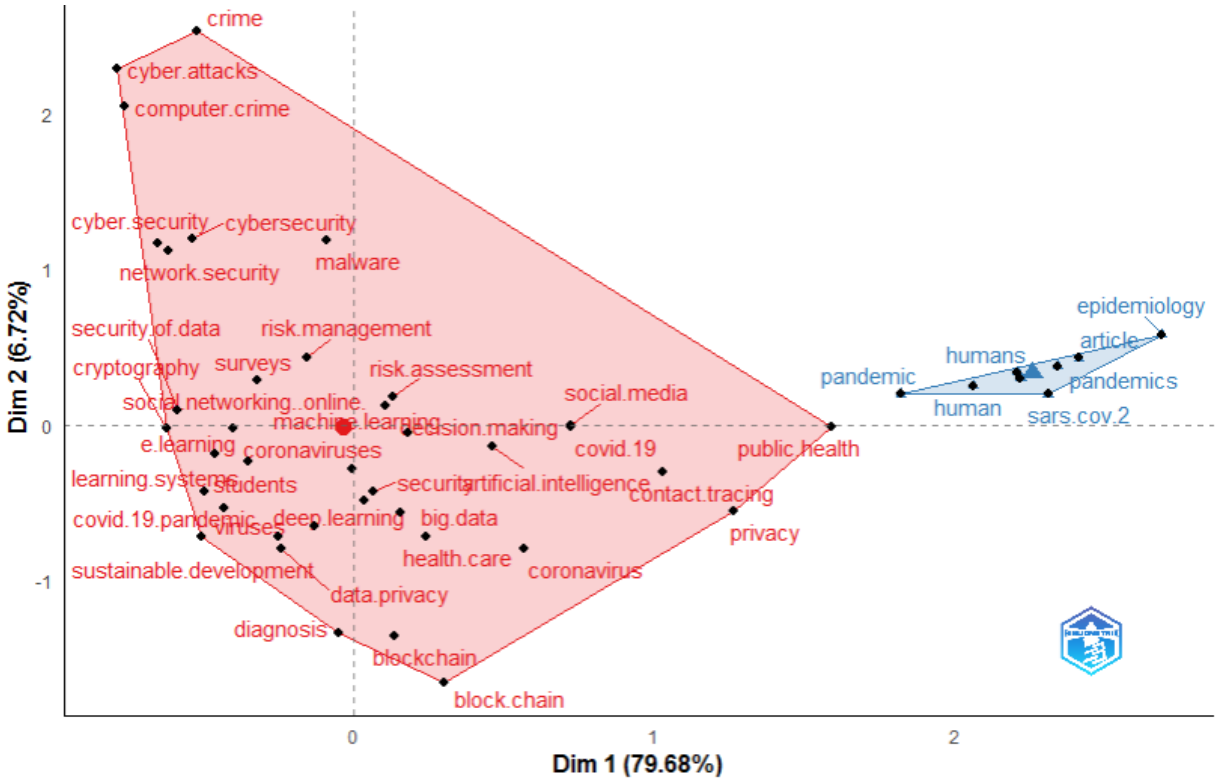

Figure 17.
Conceptual structure map on relationship between topics in the research domain.

Table 6 shows the summary of literature on work from home (WFH).

Table 6.
Summary of literature on work from home.

Author	Focus	Cyber risk
Goucher [35]	online lessons on story telling via Zoom, Skype, and Instagram	The use of computer for email, shopping and card games created cyber risk.
Chapman [36]	Workforce migrating to remote working put most IT staffs under pressure.	Cyber criminals exploited the pandemic which lead to a rise in phishing and other forms of attacks.
Ahuja, et al. [37]	Work from home cyber security model.	High risk of the privacy and security of computer resources.
Trifonov, et al. [38]	Cyber trends in industrial control systems	increase in cyber-attacks
Sipior [39]	Enhancing transparency and accountability in work environment using monitoring software, including emotion recognition software, to track employee productivity and compliance with information security policy.	-
Mwagwabi and Jiow [40]	Compliance to security measures by children	danger of clicking on malicious links on their parents' computers
Bakshi and Bhattacharyya [41]	create a technologically inclusive society for the older people	complicated technical instructions and lack of supportive learning environment
Klein and Zwilling [42]	The number of employees working remotely from home increased substantially	cyberattacks have grown in quantity and strength and human factor remains main weak

5. Discussion of Findings

One of the risks experienced during the COVID-19 pandemic was the collection of medical and health-related data from people for insight into the spread of the pandemic. Unfortunately, this lead to exposure of private data on compromised computers and other electronic devices thus making unpatched network system vulnerable to hackers. Again, small medium enterprises (SME) were also impacted, unfortunately, many SMEs were not so concerned with cyber security issues and were not motivated to address these concerns [43]. Employees who sent organizations' sensitive data to their email and devices hitherto exposed their organizations to cyber-attacks. When the necessary security settings are not in place, most personal devices may be infected with a computer virus and other harmful programs which require vetting before integrating into a corporate network. WFH was a daunting task that required extensive personal, organizational, and social adjustment. In spite of this, most workers and employers had to innovate and improve productivity from their respective homes [44]. Unfortunately, the digital divide and uneven ICT penetration and distribution was experienced across urban-rural communities in developing nations [45].

This study posed three research questions and based on the analyses the findings are discussed as follows:

5.1. Research Question One: What Are the Research Trends of Bio-Inspired Cyber Security Applications?

The use of advanced technologies such as Internet of Things devices ensures mutual interactions among network devices; however, security-related issues involved in a communication network are drastic thus suggesting the need to enhance existing authentication and authorization of network systems. One of the methods of enhancement is the utilization of AI models that monitor internet of things (IoT) communication networks. Again, bio-inspired computational algorithm-assisted blockchain technology are applied for authentication and authorization in IoT communication networks [46]. Mission-critical applications are also affected by cyber security attacks thus leading to the creation of a swarm robot system which is a bio-inspired cyber security architecture that can identify abnormal behavior caused by cyber security attacks.

The proliferation of digital technologies during COVID-19 for example within the supply chain sector facilitated information sharing on products; however, it led to cyber threats which affected most businesses within the supply value chain, in terms of leak of business data, disruption of business operations, and loss of finance. Notably, wireless sensor networks or mobile ad hoc networks were key during the pandemic. The challenge with wireless sensor networks is the bandwidth limitations, which are addressed using a meta-heuristic multipath routing Ant-based algorithm based on bio-inspired or nature-inspired. To this end, the drive for innovation created a remarkable advance in the use of digital health technologies during the COVID-19 pandemic. These approaches are in three broad categories: "digital communication strategies, digital educational initiatives and digital patient management solutions" [47].

Digital communication strategies require mutual interaction among devices for efficient management solutions in sectors such as education and health care where COVID-19 had some major impacts. Other economic sectors are identified by Agbehadji, et al. [15] as having been affected by the pandemic which required policy intervention to avert challenges of innovative approaches. Although bio-inspired designs for cyber security have yielded many feasible outcome to challenging problems in various fields, efforts have been more ad hoc between natural and human-designed systems [48]. Unfortunately, searching a vast diversity of existing natural algorithms for closely resembling new cyber security challenges can be replicated in cyber security system design that can be achieved using functional abstraction protocol.

This protocol extracted features of the natural algorithm that provide efficiency/effectiveness, and then used those abstracted features as design components to build purposeful, tailored and optimized solutions. The effectiveness was due to the differential weighting of shared information to a network layer, and dynamic individual thresholds for the independent analysis.

Existing cyber security architectures had many inherent aforementioned limitations making maintenance and devices unscalable thus providing the adversary with asymmetric advantages. Unfortunately, traditional standalone access control models for cyber security are unable to defend complex and large organization thus increasing insider attacks and security incidence [49]**.** Bio-inspired integrated access control policy regulation framework not only facilitates understanding of the anomalous behaviour of an insider but also provides theoretical background that links behavioural anomalies to the access control regulation. This approach allows access control models to focus on auto-resiliency, integration, and fast response time to promptly react against insider attacks.

Some examples of cyber security assaults are credit card fraudulent activities, net banking foraging, firewall cracking and so on. These fraudulent activities can be detected by finding the patterns of theft activities, which can be attained by analysing and learning the transaction records collected from the users in different periods. Though approaches such as machine learning algorithms using Support Vector Machine (SVM) have been introduced to predict cyber security threats, SVM tends to have more computational overhead and better performance, as it adjusts the configuration parameter values. The introduction of a big data cyber security framework (BDCSF) for credit card transactions is considered for the cyber security application. This dataset is pre-processed using an entropy-based discretization procedure and the artificial bee colony algorithm is consequently utilized to perform the feature selection process while the selected features are then learned using the SVM algorithm [50]. In addition, machine learning method has also been applied for malicious activity detection in enterprise security logs applied operators to extract features from raw data [51]. This method of feature re-engineering isolates malicious activities to form clusters of malicious attacks. The isolation enables a small number of features on raw data to be retained for interpretability which is an important consideration in cyber security applications. Similarly, SVM has been applied as a model for cross-site scripting to enable legitimate browser extensions installed from secure web stores [52]. In other studies, deep learning methods have been applied to cyber security applications to mitigate attack types including malware, spam, insider threats, network intrusions, false data injection, and malicious domain names used by botnets [53].

In another vein, digitalisation/digitisation or evolution of computing, communications and sensing technologies was rapid as organizations and individuals rely heavily on new applications such as fog and cloud computing, smart cities, IoT, collaborative computing and the virtual and mixed reality environments [54]. For instance, rapid deployment of IoT technology to support contact tracing applications [55] IoT platforms for non-pharmaceutical interventions (NPI) such as COVID-19 symptom diagnosis, quarantine monitoring, and contact tracing [56]. These interventions generated a massive volume of data which makes the feasible extension of COVID-19 NPI into people's daily lives thus highlighting the need for intelligent and effective prevention and control of data. Security, trustworthiness and resilience to cyberattacks are crucial to ensure resilient solutions, leading to computing algorithms that are based on bio-inspired cyber security [57]**.**

Attacks on IoT devices were commonplace during the global COVID-19 pandemic and one such attack is Trojan attack. It is noteworthy that Internet of Things (IoT) and Cyber-Physical Systems (CPS) influenced interaction between individuals and enterprises. A bio-inspired approach for hardware Trojan detection using unsupervised learning methods was developed to enable the tuning of security requirements for high-alert systems for safety-critical mission [58]. The IoT-CPS-based Trojan detection circuit was resilient to a range of faults and attacks, both intentional and unintentional. Often, security metrics focus on software, network, and cloud security. However, the global COVID-19 pandemic revealed the need to also focus on the security of Cyber-Physical Systems.

The study Verma and Bridges [59] indicated that host logs, in particular windows event logs, are a valuable source of information often collected by security operation centres (SOCS). Manual inspection of volumes of logs is impossible because host logs require automated analytics at each possible time. Time-series and sequential data algorithms for most cyber security applications have been proposed. However, a concise similarity metric on system logs need to be built to limit the digital gap in existing sequential data mining methods. It is evident that technologies are available to ensure controls in systems, programs, devices and networks.

Africa, as a continent, has had its share of digitalization, ranging from contact tracing applications in South Africa, Ghana, Nigeria, Morocco just to mention a few. Despite this, there is not a specific application that has an underlying bio-inspired computational model to ensure the security of such applications. Disclosing an organization's security architecture can be a subject for cyber-attack; hence, literature on bio-inspired-based computational models that were deployed on advanced technologies within the African context was a limitation. Moreover, some African countries likely have used IoT-CPS-based Trojan detection circuits during the pandemic.

Among many biological-inspired methods, the following techniques are mostly used in the cyber security domain or Cyber applications of AI-base: genetic algorithms (GA), evolution strategies (ES), ant colony optimization (ACO), particle swarm optimization (PSO), and artificial immune systems (AIS) [60]. Based on the bibliometric data analysis, the finding suggests that the COVID-19 pandemic, cyber security, machine learning, and human and network security were trending topics from 2021 to 2022. This finding indicates that while cyber security and machine learning models were trending topics it was not clear which bio-inspired computational intelligence algorithms or models underpin them.

5.2. Research Question Two: What is the Extent of Knowledge Structures on Bio-Inspired Cyber Security Applications and Architecture?

Based on the analysis, the knowledge structures cover clustering (i.e., clustering by coupling), conceptual structures (co-occurrence network, thematic map, thematic evolution) and intellectual structures (e.g., co-citation network, historiography). Clustering by coupling suggests that cyber security and network security had a high impact (1.73) and low centrality (0.28). In terms of Thematic map structure, COVID-19 has high Callon Centrality (12.00) and low Callon Density (21.72) indicating a cluster frequency of 1298 among the three (3) clusters. Thematic evolution analysis within the field of development in the research area indicates that between 2020 and 2021, COVID-19, health care, and cyber security were represented as evolution themes whereas, in 2022 alone, COVID-19 pandemic, cyber security, e-learning and deep learning were more represented as evolution themes. It was noted that the educational sector was also negatively impacted as evidenced for instance, by the attack on components of the Croatian e-learning system [61]. This highlight security loopholes in online applications that might have not used or developed with a more robust security architecture.

Thus, suggesting another evolving theme like e-learning and deep learning. This revelation confirms the literature on cyber-attacks on e-learning systems by Chen and Yang [60] resulting in the application of deep learning models to address cyber security attacks. The bibliometric analysis again suggests non-existing literature from Africa in the context of countries' scientific production over time (Tables 3 and 4). Thus, this suggests a research gap that needs to be bridged in Africa through collaboration with leading countries like the USA, India and China.

Furthermore, the thematic map shows that network security, and cyber security themes appear in all quadrants. Again, COVID-19, the Internet of Things, and health care are important in the research field that is yet to be developed. Furthermore, thematic evolution indicates that the COVID-19 pandemic and humans were highly developed and isolated themes during 2020 and 2022 while cyber security, network security and the internet of things appear in all quadrants. Also, health care, risk assessment and artificial intelligence themes are important for the research field but are not developed. Furthermore, thematic evolution between 2020 and 2021, suggests that COVID-19, health care, and cyber security are evolution themes. However, in 2020-2022, COVID-19 pandemic, cyber security, e-learning and deep learning were more represented as evolution themes.

In another vein, conceptual structure map with multiple correspondence analysis (MCA) suggests that pandemic, human, epidemiology, human(s) and SARS cov2 are more similar in distribution as these Keywords Plus are closer to each other. Though "work from home" and "social distance" were among the common phrases used during the COVID-19, it was not shown on the conceptual map plot and thematic map. Thus, knowledge structures underpinning bio-inspired cyber security applications and architecture during the COVID-19 pandemic cover themes on cyber security, network security, the Internet of Things, health care, e-learning and deep learning. On the other hand, Sustainability publications recorded the highly (28) cited articles, followed by Lecture Notes in Networks and Systems (24), IEEE access (23) and many others.

The most relevant authors and their impact are Javaid (impact of 7), Choo (6), Haleem (6), etc. as India tops the countries' production of articles over time with 423 articles in 2022 and is also the most cited country having approximately 1094 citations, followed by the USA (905), the United Kingdom (741) and others.

5.3. Research Question Three: What is the Extent of Bio-Inspired Cyber Security Application Utilized During the COVID-19 Pandemic?

Table 5 shows that high frequency (100) on cluster with "covid-19, internet of things, health care" and another cluster has "cyber security, network security, and cyber security" with frequency of 71. Figure 11 shows the centrality of these clusters and Figure 14 further shows the point of convergence of the cluster on "cyber security, network and cybersecurity" and the cluster on "covid-19, internet of things, and health care" shown as "Basic Themes". Figure 15 shows a cluster on "cyber security, network security, and internet of things" as the cardinal point for researchers. Also, Figure 17 shows clusters and how each keyword relates with another in the cluster. These findings demonstrate non-representation of "bio-inspired algorithm" or "bio-inspired" among clusters. It could be due to lack of interest to research on bio-inspired algorithm as a standalone algorithm without associating it with an application domain. Meanwhile, bio-inspired algorithms are an integral part of network security and cyber security frameworks. Bio-inspired algorithms are utilized at the network level to fine-tune security parameters. This suggests that having a strong network security protocol forestalls any attack on online applications. It is revealed from this review that the Internet of Things (IoT) constitutes 77% of the occurrence of keywords hence confirming the proliferation of IoT devices during 2020 and 2022 as suggested by Ahmed, et al. [55]. IoT devices ensure interaction among network devices to enforce existing authentication and authorization of network systems. Fortunately, bio-inspired computational algorithm-assisted blockchain technology facilitated such IoT communication networks [46]. To this end, though attacks on IoT devices were commonplace during the global COVID-19 pandemic, a bio-inspired approach combined with an unsupervised learning method was utilized in hardware Trojan detection to fine-tune security requirements for high-alert systems [58]. However, literature suggests that biological-inspired methods such as genetic algorithms (GA), evolution strategies (ES), ant colony optimization (ACO), particle swarm optimization (PSO), and artificial immune systems (AIS) are utilized in cyber security systems or applications. Machine learning methods for malicious activity detection in enterprise security logs applied operators to extract features from raw data. This method of feature re-engineering isolates malicious activities to form clusters of malicious attacks. The isolation enables a small number of features on raw data to be retained for interpretability which is an important consideration in cyber security applications. Thus, bio-inspired computational algorithms are quite robust because of their usage in different layers ranging from the application layer, transport layer, network layer, and physical layer of the open systems interconnection (OSI) model as cyber-security systems embody these layers.

Furthermore, the reviewed literature suggests among others that poor device self-awareness in architectures and misconfiguration in security infrastructures were the issues with current cyber security architectures. IoT devices are the

possible source of some of these misconfigurations which calls for more deployment of bio-inspired algorithms to resolve this issue [16]. IoT devices have different security parameters that need to be set for any network configuration and thus, bio-inspired algorithm is capable of providing this parameter tuning for a security network [62].

Despite the rise of IoT applications, it is unclear the extent to which penetration testing was conducted by organizations whose employees worked from home. Though, bio-inspired algorithm was applied at the hardware level to detect Trojan [58] its application to detect email phishing needs more attention. Bio-inspired algorithms can be beneficial in feature extraction or selection to detect malicious activities on security log [51]. Several researchers including [63] have demonstrated the feature selection capabilities of bio-inspired algorithms. This current review highlighted that employees used their personal emails and devices to work remotely thus leading to cyber-attacks, and fortunately, bio-inspired algorithm-based devices can detect Trojans thereby providing some level of security at the network layer or physical layer. Thus, suggesting the application of bio-inspired algorithm to address a thematic area such as network security and IoT.

5.4. Impact of COVID-19 Pandemic

COVID-19 impacts many developing nations, where a notable increase in cyber threats was observed during the pandemic. Cybercriminals exploited the surge in remote work, targeting employees using phishing attacks and ransomware. This led to a significant rise in data breaches and financial losses for organizations. In Nigeria, organizations experienced a surge in cyber-attacks with a focus on exploiting vulnerabilities in health care systems and financial institutions. The increased reliance on online services created opportunities for fraud, leading to financial losses and disruptions in critical sectors. In Kenya for instance, there were challenges in securing e-learning platforms during the pandemic, with reports of unauthorized access and data breaches affecting students and educational institutions [64]. Also, the health care sector in Egypt witnessed a spike in cyber threats, with attacks targeting medical facilities and research institutions involved in COVID-19 research. These incidents underscored the importance of securing critical infrastructure in the face of global health crises. Meanwhile, Ghana experienced an increase in social engineering attacks, including scams related to COVID-19 relief funds. Cybercriminals exploited the uncertainty and fear surrounding the pandemic to deceive individuals and organizations, hence emphasizing the need for cyber-security awareness. In Morocco, businesses encountered challenges in securing their supply chains during the pandemic as disruptions in logistics and increased reliance on online transactions led to cyber threats targeting the integrity of supply chain operations, thus necessitating a re-evaluation of cyber-security strategies. These illustrate the diverse challenges faced by African countries in the cyber-security domain during the COVID-19 pandemic. Also, these underscore the urgency for robust cyber-security measures and the relevance of bio-inspired computational intelligence in addressing the evolving threat within the cyber-physical landscape in the African continent.

The global digital shutdown and global COVID-19 pandemic led shutdown both created some economic impacts. With a global digital shutdown, electronic communication and data transfers would be impossible and social contacts would only be by personal visits. While a single day without internet is estimated to cost more than USD50 Billion and a 21-day global cyber lockdown could cost over USD1 trillion. It would also be very tedious to replace numerous connected devices and recover from the widespread destruction of digital systems following a cyber-attack-induced global shutdown. To prepare for a “cyber pandemic”, organizations should anticipate cyber-attacks and respond appropriately. As such, digital rollback and continuity plans are very important for organizations to continue to operate in the event of a sudden loss of digital tools and networks.

During the global COVID-19 pandemic, many countries relied on another nations to procure diagnostic devices in order to support their health sector. Unfortunately, this can lead to industrial espionage or local industry interference to produce a tactical advantage on the international market soon. Again, this could result in the disclosure of confidential information that can destabilize a government or election [54]. Highlighting an impact on industries and politics which might seem to be beyond the possibilities of the cyber domain. The COVID-19 pandemic also revealed some of the vulnerabilities in educational systems such that many cyber-attacks on e-learning systems have created severe demands for specialized technology solutions to protect the security of e-learning systems. Emails of educational organizations were noted to be attacked daily by spam, and phishing campaigns [60] during the pandemic. This led to the development and deployment of a deep learning attention mechanism to protect the email systems of educational organizations.

The goal of phishing for instance is to trick online users to obtain sensitive information to compromise a system. Email phishing increased during the COVID-19 pandemic and created more security concerns in many economic sectors. Unfortunately, the pandemic was unexpected and some users who are not digitally inclined on how to identify phishing were the victims of phishing attacks [22]. Furthermore, the widespread panic caused by the pandemic resulted in global initiatives to limit its spread and also created mass violations of citizens’ privacy, thus leading to people’s hesitation to adopt some of the global initiatives like contact tracing applications by some countries [65]. This is because phishing was used on health care workers to enable hackers to compromise health care systems.

The COVID-19 pandemic also increased the pace of data fusion in Africa, and the generation of huge volumes of data from different medical devices thus securing medical data in an exponentially-pacing computation world is paramount to ensure system’s reliability [66]. Consequently, any attack on the communication network can cause damage to critical resources and infrastructure. The COVID-19 pandemic did not entirely change citizens’ habits, however, that significantly impacted the scientific community. For instance, the use of virtual conferences has some technical and organizational challenges. From a technical point of view, sessions may be hijacked by “Internet trolls” or “Zoom bombed” [67]. From the organization's perspective, it resulted in low engagement of audience. These notwithstanding, researchers have also

leveraged the pandemic to explore methods to secure web conference platforms that work efficiently in low bandwidth for different devices.

5.5. Environmental Policies and Cyber-Security Issues

Figure 17 presents the conceptual map and it is evident in the red cluster on occurrence of topics such as sustainable development, social media, data privacy, public health, computer security, cyber-attacks, network security, risk management, etc. These topics are key in creating an eco-system which are regulated by laws and policies. As environmental monitoring and management systems rely more on digital infrastructure, including IoT sensors, remote sensing platforms, smart grids, and AI-driven predictive models, they are increasingly vulnerable to cyber-attacks [68]. Public trust, legal compliance, and scientific accuracy all depend on the availability, confidentiality, and integrity of environmental data. Bio-inspired computational algorithms for cyber-security offer robust, adaptable, and intelligent defence to safeguard ecologically critical systems [69]. For instance, real-time data transmission across networks is a common feature of contemporary environmental infrastructure, including satellite data feeds, water quality sensors, and air quality monitoring stations. The processes of enforcing environmental laws and formulating policy depend on these systems. However, because of their connectedness, they are also vulnerable to cyber threats such spoofing, denial-of-service (DoS) attacks, data tampering, and illegal access.

Increasingly, digital data infrastructures around the world are supporting environmental regulations, and regulatory compliance now automatically includes security. For enforcement and policy implementation, South African frameworks like the National Environmental Management Act (NEMA) and the Air Quality Act mostly rely on reliable data. Laws such as the Protection of Personal Information Act (POPIA) and the Cybercrimes Act 2020, which require the protection of digital systems, particularly those handling environmental data, also fall under the purview of cyber-security compliance. Meanwhile, internationally, laws such as the EU General Data Protection Regulation (GDPR) and the Aarhus Convention highlight the public's right to accurate environmental information, which is contingent upon cyber-security integrity. Moreover, cyber-security is acknowledged as the cornerstone of reliable governance systems, particularly those that uphold environmental protection, under the UN Sustainable Development Goals (SDG 16: Peace, Justice, and Strong Institutions). Issues of regulatory compliance and privacy concerns were topical among the health care community thus suggesting a more robust approach toward effective pathology systems and new methods to strengthen the security of online applications.

Africa, with its vibrant and growing Science and Technology sector, faces distinctive challenges that amplify the complexities introduced by the global pandemic. As nations in Africa navigate the digital landscape, the importance of robust cyber-security strategies becomes even more pronounced. Within the African context, it is crucial to acknowledge and understand that regional differences shape the landscape in terms of the diverse socio-economic conditions, regulatory environments, and levels of internet infrastructure development, influencing the dynamics of cyber-security. Table 7 shows key environmental and cyber security-related issue.

Table 7.
Key environmental and cyber security issue.

Author	Focus	Environmental policy relating cyber security
Bulgurcu [70]	Societies respond to technological changes or work processes without recourse to best work practices	Developed cyber resilience guidelines, policies and cyber-security principles, awareness and training programs.

6. Limitations, Policy and Practical Implication

The opportunities presented by bio-inspired computational algorithms require policymakers to consider its use in cyber-based applications. For example, its integration into access control policy regulation, hardware level to detect Trojans, and many more. In this current research study, although vast research publications were available in Scopus, there was research data limitation within the African context. Thus, suggesting the need for Africa's research institutions to intensify their research output in the scope of bio-inspired cyber-security applications.

Again, it calls for policy reforms and training of bio-inspired cyber security practitioners to understand the theoretical underpinning of bio-inspired search methods as a way to bridge the gap between theory and practice in order to address the issue of poor IoT device misconfiguration in security infrastructure. Indeed, COVID-19 impacted many sectors, and this research calls on academia and businesses to work together to develop a robust bio-inspired cyber-security computational model that can stand a test-of-time.

In the digital age, cyber-security and environmental sustainability are closely related. Computational algorithms inspired by nature offer a natural solution to contemporary cyber-security issues in environmental systems. These algorithms guarantee the integrity, transparency, and resilience of the enforcement of environmental laws and international agreements by safeguarding the digital foundation of environmental governance. As researchers construct increasingly networked and data-dependent environmental infrastructures, the implementation of such intelligent systems by technology developers are essential. Thus, highlights of this research would help practitioners know the trending themes and help to align their practical needs to current cyber security demands.

7. Conclusion and Future Direction

This current research study highlights issues on bio-inspired computation for cyber security systems during the COVID-19 global pandemic. The bibliometric analysis was adopted to find research trends in publications. The findings show that, though machine learning was a trending topic in 2022, more research studies are required to identify bio-inspired methods for malicious activity detection in enterprise security logs. Again, through this study, we unearthed thematic areas namely cyber security, network security, e-learning, health care, deep learning and machine learning for consideration ,in the development of strong network architecture for IoT devices and applications. The challenges imposed by the choice of the methodology include the year, as documents not within the year range utilized might have very relevant information on research trends and knowledge structures. Furthermore, the Scopus dataset was chosen due to its wider coverage and other datasets like the Web of Science are not considered in this study, which might be a limitation regarding database choices. This study implies that cyber security professionals should focus on and prioritize strengthening the utilization of bio-inspired computational intelligence in cyber security applications in their organizations. The outcome of this study suggest that future directions should focus on research collaboration among African research institutions and institutions from the developed nations, as this would help to strengthen the use of bio-inspired computational methods in the cyber security space.

References

[1] R. Gafni and T. Pavel, "Cyberattacks against the health-care sectors during the COVID-19 pandemic," *Information and Computer Security*, vol. 30, no. 1, pp. 137-150, 2022. https://doi.org/10.1108/ICS-05-2021-0059

[2] Interpol, INTERPOL report shows alarming rate of cyberattacks during COVID-19, 2020. Retrieved: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

[3] C. G. Iwu, O. E. Okeke-Uzodike, E. Anwana, C. H. Iwu, and E. E. Esambe, "Experiences of academics working from home during COVID-19: A qualitative view from selected South African universities," *Challenges*, vol. 13, no. 1, p. 16, 2022. https://doi.org/10.3390/challe13010016

[4] M. B. Mutanga and A. Abayomi, "Tweeting on COVID-19 pandemic in South Africa: LDA-based topic modelling approach," *African Journal of Science, Technology, Innovation and Development*, vol. 14, no. 1, pp. 163-172, 2022.

[5] N. Alharbe, "Security and privacy of telehealth apps in the era of COVID-19 pandemic: Saudi Arabia perspective," presented at the In The 23rd International Conference on Information Integration and Web Intelligence (iiWAS2021), Linz, Austria, 2021.

[6] F. K. Kaiser, M. Wiens, and F. Schultmann, "Use of digital healthcare solutions for care delivery during a pandemic-chances and (cyber) risks referring to the example of the COVID-19 pandemic," *Health and Technology*, vol. 11, pp. 1125–1137, 2021. https://doi.org/10.1007/s12553-021-00541-x

[7] A. Tyagi and M. S. Gaur, "COVID-19 pandemic and post-pandemic: Impact and technical threats in India. In: Agrawal, R., Kishore Singh, C., Goyal, A. (eds)," in *Advances in Smart Communication and Imaging Systems. Lecture Notes in Electrical Engineering, vol 721. Springer, Singapore*, 2021.

[8] A. Livara and R. Hernandez, "An empirical analysis of machine learning techniques in phishing e-mail detection," in *2022 International Conference for Advancement in Technology, ICONAT 2022*, 2022.

[9] L. Waizenegger, B. McKenna, W. Cai, and T. Bendz, "An affordance perspective of team collaboration and enforced working from home during COVID-19," *European Journal of Information Systems*, vol. 29, no. 4, pp. 429-442, 2020. https://doi.org/10.1080/0960085X.2020.1800417

[10] I. Mukhopadhyay, "Cyber threats landscape overview under the new normal," in *ICT Analysis and Applications. Lecture Notes in Networks and Systems, vol 314. Springer, Singapore*, 2022.

[11] G. Vira Yudha and R. Wisnu Wardhani, "Design of a snort-based IDS on the raspberry Pi 3 Model B+ Applying TaZmen sniffer protocol and log alert integrity assurance with SHA-3," in *2021 9th International Conference on Information and Communication Technology, ICoICT 2021*, 2021.

[12] R. R. R. M. Ratnayake, G. A. J. Perera, R. Ponnamperuma, G. D. N. D. K. Abeysiriwardhena, A. Senarathne, and B. A. Ganegoda, "ARGUS - An adaptive smart home security solution," in *4th International Conference on Advancements in Computing, ICAC 2022 - Proceeding*, 2022.

[13] I. E. Agbehadji, B. O. Awuzie, A. B. Ngowi, and R. C. Millham, "Review of big data analytics, artificial intelligence and nature-inspired computing models towards accurate detection of COVID-19 pandemic cases and contact tracing," *International Journal of Environmental Research and Public Health*, vol. 17, no. 15, p. 5330, 2020. https://doi.org/10.3390/ijerph17155330

[14] I. E. Agbehadji, A. Abdultaofeek, M. B. Mutanga, B. O. Awuzie, and A. B. Ngowi, "Bio-inspired search approach cross-domain location mapping for smart mobile service system," *Journal of Computer Science*, vol. 18, no. 4, pp. 281-296, 2022. https://doi.org/10.3844/jcssp.2022.281.296

[15] I. E. Agbehadji, B. O. Awuzie, and A. B. Ngowi, "COVID-19 pandemic waves: 4IR technology utilisation in multi-sector economy," *Sustainability* vol. 13, p. 10168, 2021. https://doi.org/10.3390/su131810168

[16] A. Hernández-Herrera, E. R. Espino, and P. J. Escamilla Ambrosio, "A bio-Inspired cybersecurity scheme to protect a Swarm of Robots. In I. Batyrshin (Ed.)," in *Advances in Computational Intelligence: 17th Mexican International Conference on Artificial Intelligence (MICAI 2018) — Lecture Notes in Artificial Intelligence, Vol. 11289 (pp. 318-331). Cham, Switzerland: Springer*, 2018, doi: https://doi.org/10.1007/978-3-030-04497-8_26.

[17] A. Mugwagwa, C. Chibaya, and E. Bhero, "A survey of inspiring swarm intelligence models for the design of a swarm-based ontology for addressing the cyber security problem," *International Journal of Research in Business and Social Science*, vol. 12, no. 4, pp. 483-494, 2023. https://doi.org/10.20525/ijrbs.v12i4.2473

[18] E. O. Anwana and O. J. Aroba, "African women entrepreneurs and COVID-19: Towards achieving the African Union Agenda," *HTS Teologiese Studies/Theological Studies*, vol. 78, no. 2, pp. 1-7, 2022.

[19] G. C. Jayakrishnan, V. Banahatti, S. Lodha, G. Sirigireddy, and S. Nivas, "Housie: A multiplayer game for cybersecurity training and evaluation," in *CHI PLAY 2022 - Extended Abstracts of the 2022 Annual Symposium on Computer-Human Interaction in Play*, 2022.

[20] N. K. Upadhyay and M. Rathee, "A critical analysis of cyber security threats posed by Covid-19: Designing a roadmap for future," *Medicine, Law and Society*, vol. 15, no. 1, pp. 89-106, 2022. https://doi.org/10.18690/mls.15.1.89-106.2022

[21] M. Candela, V. Luconi, and A. Vecchio, "Impact of the COVID-19 pandemic on the Internet latency: A large-scale study," *Computer networks*, vol. 182, no. 107495, 2020. https://doi.org/10.1016/j.comnet.2020.107495

[22] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Privacy-preserving COVID-19 contact tracing blockchain," *IEEE Access*, vol. 9, pp. 121916 - 121929, 2021. https://doi.org/10.1109/ACCESS.2021.3109091

[23] A. Choudhary, G. Choudhary, K. Pareek, C. Kunndra, J. Luthra, and N. Dragoni, "Emerging cyber security challenges after COVID pandemic: A survey," *Journal of Internet Services and Information Security*, vol. 12, no. 2, pp. 21-50, 2022. https://doi.org/10.22667/JISIS.2022.05.31.021

[24] S. S. Goswami, S. Sarkar, K. K. Gupta, and S. Mondal, "The role of cyber security in advancing sustainable digitalization: Opportunities and challenges," *Journal of Decision Analytics and Intelligent Computing*, vol. 3, no. 1, pp. 270-285, 2023. https://doi.org/10.31181/jdaic10018122023g

[25] O. J. Aroba, N. Naicker, T. T. Adeliyi, and A. Gupthar, "A review: The bibliometric analysis of emerging node localization in wireless sensor network," *International Journal of Computer Information Systems and Industrial Management Applications*, vol. 15, pp. 141-153, 2023.

[26] M. Javaid and A. Haleem, "Additive manufacturing applications in medical cases: A literature based review," *Alexandria Journal of Medicine*, vol. 54, no. 4, pp. 411–422, 2019.

[27] K.-K. R. Choo, "The cyber threat landscape: Challenges and future research directions," *Computers & Security*, vol. 30, no. 8, pp. 719–731, 2011.

[28] A. Haleem, M. Javaid, and R. P. Singh, "3D printing applications in bone tissue engineering," *Journal of Clinical Orthopaedics and Trauma*, vol. 10, no. 2, pp. 380–386, 2019.

[29] A. Kumar, S. Luthra, S. K. Mangla, and Y. Kazançoğlu, "COVID-19 impact on sustainable production and operations management," *Sustainable Operations and Computers*, vol. 1, pp. 1-7, 2020. https://doi.org/10.1016/j.susoc.2020.06.001

[30] S. Misra, A. Adewumi, R. Maskeliūnas, and R. Damaševičius, "Artificial intelligence for healthcare applications," *Journal of Healthcare Engineering*, vol. 2019, pp. 1–2, 2019.

[31] Y. Wang, L. A. Kung, and T. A. Byrd, "Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations," *Technological Forecasting and Social Change*, vol. 126, pp. 3–13, 2018.

[32] K. M. Carley, "Dynamic network analysis. In R. Breiger, K. Carley, & P. Pattison (Eds.), Dynamic social network modeling and analysis." Washington, DC: National Academies Press, 2003.

[33] M. Gupta and A. Kohli, "Enterprise resource planning systems and its implications for operations function," *Technovation*, vol. 26, no. 5, pp. 687-696, 2006. https://doi.org/10.1016/j.technovation.2004.10.005

[34] S. Hakak, W. Z. Khan, M. Imran, K. K. R. Choo, and M. Shoaib, "Have you been a victim of COVID-19-related cyber incidents? Survey, Taxonomy, and mitigation strategies," *IEEE Access*, vol. 8, pp. 124134-124144, 2020. https://doi.org/10.1109/ACCESS.2020.3006172

[35] W. Goucher, "Once upon a time... Storytelling for cybersecurity," *ITNOW*, vol. 62, no. 3, pp. 24-25, 2020. https://doi.org/10.1093/itnow/bwaa069

[36] P. Chapman, "Are your IT staff ready for the pandemic-driven insider threat?," *Network Security*, Article vol. 2020, no. 4, pp. 8-11, 2020. https://doi.org/10.1016/S1353-4858(20)30042-8

[37] L. Ahuja, A. Rana, and S. Gupta, "Security privacy model for work from home paradigm," in *ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, 2020.

[38] R. Trifonov, G. Tsochev, S. Manolov, R. Yoshinov, and G. Pavlova, "Cyber trends in industrial control systems," in *Proceedings - 25th International Conference on Circuits, Systems, Communications and Computers, CSCC 2021*, 2021.

[39] J. Sipior, "Monitoring remote employees at FinPro," *Communications of the Association for Information Systems*, vol. 49, pp. 304-320, 2021. https://doi.org/10.17705/1CAIS.04912

[40] F. Mwagwabi and J. H. Jiow, "Compliance with security guidelines in teenagers: The conflicting role of peer influence and personal norms," *Australasian Journal of Information Systems*, vol. 25, pp. 1-25, 2021. https://doi.org/10.3127/ajis.v25i0.2953

[41] T. Bakshi and A. Bhattacharyya, "Socially distanced or socially connected? Well-being through ICT usage among the Indian elderly during COVID-19," *Millennial Asia*, vol. 12, no. 2, pp. 190-208, 2021. https://doi.org/10.1177/0976399621989910

[42] G. Klein and M. Zwilling, "The weakest link: Employee cyber-defense behaviors while working from home," *Journal of Computer Information Systems*, vol. 64, no. 3, pp. 408-422, 2024. https://doi.org/10.1080/08874417.2023.2221200

[43] R. Hricová, "A view on the digitization of small and medium-sized enterprises," in *EAI/Springer Innovations in Communication and Computing*, 2023.

[44] A. Enaifoghe and N. Zenzile, "The rapidly evolving situation of employee work-from-home productivity and the integration of ICT in Post-COVID-19 pandemic," *Scientific African*, vol. 20, p. e01709, 2023. https://doi.org/10.1016/j.sciaf.2023.e01709

[45] S. Rasdi, The future after the covid-19 pandemic: Romote work in South Africa, 2020. Retrieved: https://kujenga-amani.ssrc.org/2020/10/29/the-future-after-the-covid-19-pandemic-remote-work-in-south-africa/

[46] R. Alroobaea, R. Arul, S. Rubaiee, F. S. Alharithi, U. Tariq, and X. Fan, "AI-assisted bio-inspired algorithm for secure IoT communication networks," *Cluster Computing*, vol. 25, pp. 1805-1816, 2022. https://doi.org/10.1007/s10586-021-03520-z

[47] T. Robbins *et al.*, "COVID-19: A new digital dawn? ," *Digital Health*, vol. 6, p. 2055207620920083, 2020. https://doi.org/10.1177/2055207620920083

[48] G. P. Su´arez, L. K. Gallos, and N. H. Fefferman, "A case study inTailoring a bio-inspired cyber-security algorithm: Designing anomaly detection for multilayer networks," *Journal of Cyber Security and Mobility*, vol. 8, no. 1, pp. 113-132, 2018. https://doi.org/10.13052/2245-1439.815

[49] U. Rauf, M. Shehab, N. Qamar, and S. Sameen, "Bio-inspired approach to thwart against insider threats: An access control policy regulation framework," presented at the International Conference on Bio-inspired Information and Communication (pp. 39-57). Cham: Springer International Publishing, 2019.

[50] M. Ahmed and M. B. G. Rama, "Cyber security framework for big data environment using support vector machine," *Journal of Advanced Research In Dynamical and Control Systems*, vol. 11, no. 10, pp. 1-8, 2019. https://doi.org/10.5373/JARDCS/V11I10/20192999

[51] J. Duan, Z. Zeng, A. Oprea, and S. Vasudevan, "Automated generation and selection of interpretable features for enterprise security," presented at the IEEE 2018.

[52] T. P. Fowdur and S. Hosenally, "A real-time machine learning application for browser extension security monitoring," *Information Security Journal: A Global Perspective*, vol. 33, no. 1, pp. 16-41, 2022. https://doi.org/10.1080/19393555.2022.2128944

[53] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, "A survey of deep learning methods for cyber security," *Information*, vol. 10, no. 4, p. 122, 2019. https://doi.org/10.3390/info10040122

[54] A. Bobbio, L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroiann, "A cyber warfare perspective on risks related to health IoT devices and contact tracing," *Neural Computing and Applications*, vol. 35, pp. 13823–13837, 2021. https://doi.org/10.1007/s00521-021-06720-1

[55] N. Ahmed *et al.*, " A survey of covid-19 contact tracing apps," *IEEE Access* vol. 8, pp. 134577–134601, 2020. https://doi.org/10.1109/ACCESS.2020.3010226

[56] S. Flaxman *et al.*, "Estimating the effects of non-pharmaceutical interventions on covid-19 in Europe," *Nature*, vol. 584, pp. 257–261, 2020. https://doi.org/10.1038/s41586-020-2405-7

[57] E. El-Alfy, M. Eltoweissy, E. W. Fulp, and W. Mazurczyk, *Nature-inspired cyber security and resiliency: Fundamentals, techniques and applications*. London, UK: Institution of Engineering & Technology, 2019.

[58] A. P. Johnson, H. Al-Aqrabi, and R. Hill, "Bio-inspired approaches to safety and security in IoT-enabled cyber-physical systems," *Sensors*, vol. 20, no. 3, p. 844, 2020. https://doi.org/10.3390/s20030844

[59] M. E. Verma and R. A. Bridges, "Defining a metric space of host logs and operational use cases," Proceedings of the 2018 IEEE International Conference on Big Data (BigData 2018) (pp. 5068-5077). Seattle, WA, USA: IEEE, 2018.

[60] Y. Chen and Y. Yang, "An advanced deep attention collaborative mechanism for secure educational email services," *Hindawi: Computational Intelligence and Neuroscience*, vol. 2022, no. 1, p. 3150626, 2022. https://doi.org/10.1155/2022/3150626

[61] I. Cvitić, D. Peraković, M. Periša, and A. D. Jurcut, "Methodology for detecting cyber intrusions in e-learning systems during COVID-19 pandemic," *Mobile Networks and Applications*, vol. 28, pp. 231–242, 2021. https://doi.org/10.1007/s11036-021-01789-3

[62] I. E. Agbehadji, R. Millham, S. Fong, and H.-J. Hong, "Kestrel-based Search Algorithm (KSA) for parameter tuning unto Long Short Term Memory (LSTM) Network for feature selection in classification of high-dimensional bioinformatics datasets," in *Proceedings of the 2018 Federated Conference on Computer Science and Information Systems (FedCSIS 2018)*, 2018.

[63] I. E. Agbehadji, R. Millham, S. J. Fong, and H.-J. Hong, "Integration of Kestrel-based search algorithm with artificial neural network for feature subset selection " *International Journal of Bio-Inspired Computation*, vol. 13, no. 4, pp. 222-233, 2019. https://doi.org/10.1504/IJBIC.2019.100151

[64] M. K. Chizanga, J. Agola, and A. Rodrigues, "Factors affecting cyber security awareness in combating cyber crime in Kenyan public universities," *International Research Journal of Innovations in Engineering and Technology*, vol. 6, no. 1, pp. 54-57, 2022. https://doi.org/10.47001/IRJIET/2022.601011

[65] S. Tahir, H. Tahir, A. Sajjad, M. Rajarajan, and F. Khan, "Privacy-preserving COVID-19 Contact tracing blockchain," *Journal of Communications and Networks*, vol. 23, no. 5, pp. 360-373, 2021. https://doi.org/10.23919/JCN.2021.000031

[66] P. Nguyen, V. Huynh, K. Vo, P. Phan, M. Elhoseny, and D. Le, "Deep learning based optimal multimodal fusion framework for intrusion detection systems for healthcare data," *CMC-Computers Materials & Continua*, vol. 6, no. 3, pp. 2555 -2571, 2021.

[67] N. A. Karim and A. H. Ali, "E-learning virtual meeting applications: A comparative study from a cybersecurity perspective," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 24, no. 2, pp. 1121-1129, 2021. http://doi.org/10.11591/ijeecs.v24.i2.pp1121-1129

[68] N. C. Uzondu and D. D. Lele, "Challenges and strategies in securing smart environmental applications: A comprehensive review of cybersecurity measures," *Computer Science & IT Research Journal* vol. 5, no. 7, pp. 1695-1720, 2024. https://doi.org/10.51594/csitrj.v5i7.1353

[69] M. Hassan, M. H. Rehmani, and J. Chen, "Bio-inspired techniques in intrusion detection systems: A survey," *Journal of Network and Computer Applications*, vol. 133, pp. 1–34, 2020.

[70] B. Bulgurcu, "Understanding the cyber safety impacts of digital transformation on vulnerable businesses and populations," in *28th Americas Conference on Information Systems, AMCIS 2022*, 2022.

Appendix A.

Appendix A1.
COVID-19, cyber security and machine learning as trend topics between 2021 to 2022.

Item	Freq	Year_q1	Year_med	Year_q3
Betacoronavirus	12	2020	2020	2020
United States	12	2020	2020	2021
Information Technology	10	2020	2020	2021
Pandemic	116	2021	2021	2022
Human	90	2021	2021	2022
Network Security	83	2021	2021	2022
CoVID-19	207	2021	2022	2022
Cybersecurity	68	2021	2022	2022
Machine Learning	49	2021	2022	2022

Appendix A2.
Co-occurrence network using the network approach.

Node	Cluster	Betweenness	Closeness	PageRank
Covid-19	1	249.627865374569	0.0204081632653061	0.0786293632858141
Internet of things	1	29.7536677348306	0.0166666666666667	0.0267521213375485
Health care	1	19.7454423344191	0.0166666666666667	0.0231356458219845
Machine learning	1	7.39289230436387	0.0149253731343284	0.0168758594522377
Deep learning	1	2.85858722911539	0.0133333333333333	0.0128412128277354
Artificial intelligence	1	9.98653340955996	0.0161290322580645	0.0189072059068859
Social media	1	5.78287224683236	0.0128205128205128	0.0135590106640151
Risk assessment	1	3.70159410322583	0.0138888888888889	0.0134030962709113
Viruses	1	2.45980422783772	0.0136986301369863	0.0122199431019577
Blockchain	1	2.89161217814772	0.0133333333333333	0.0130817014203385

Appendix A3.
Thematic map.

Cluster	Callon Centrality	Callon Density	Rank Centrality	Rank Density	Cluster Frequency
Covid-19	12.0068667715666	21.719721977881	3	1	1298
Network security	5.66978715431983	23.5676880172503	2	2	1413
Pandemic	5.55421461642621	48.3221996296282	1	3	932