BIBLIOMETRIC ANALYSIS OF CYBERSECURITY THREATS - WITH SPECIAL REFERENCE TO CHATGPT

Dr. S. Rajeswari

M.B.A., M.C.A., Ph.D. Assistant Professor,

Department of Management Studies,

Takshashila University, Tamilnadu.

The evolution of Artificial Intelligence (AI) on the one side and the growth of the internet on the other side has out thrown a serious complexity of cyber security. As, individuals, business people, government agencies etc., uses the internet as a major platform to share and communicate huge voluminous data. This data used to train the AI models has brought significant changes in various disciplines of life such as healthcare, education, transport, e-commerce, robotics, agriculture, automobiles, chat bots, logistics, marketing, etc., Notably the usage of open AIs'-chat GPT by more than 1 million users just within 5 days, signifies its wide utilization and need. Despite its wide utilization, there raises a question in the minds of every individual, is chat GPT a boon or a bane? Ultimately, the answer lies in how the end user utilizes it. Chat GPT developed with proper security measures and standards couldn't be used for illegal activities directly. But still, if utilized in a tricky way, it generates the text to be used for one of the major cyber threat activities (phishing). Hence it throws immense responsibility on cyber security professionals to utilize chat GPT in the right way by identifying the vulnerable threats and unauthorized access to the system. Thus, the study broadly portrays the need for cyber security, the emergence of various generative AI models, bibliometric analysis on cyber security and chat GPT, and the pros and cons of chat GPT from an organizational perspective.

Keyword: Cyber security, Artificial Intelligence, Cyber Threats, Phishing, Chat GPT.

Although Artificial Intelligence (AI) has been a buzzword in the past decade, its success dates back to 1950 with programs such as General Problem Solver and ELIZA. However, owing to its limitations in terms of Investment in AI and processing capacity, it has entered a stagnant stage. AI refers to systems that use input data to train the model and generate the output used to achieve the goals or targets of the organizations. In 2015, AI made its entry through ALPHA GO, and again, the release of chat GPT by Open AI in 2022 has out thrown ample opportunities for individuals and businesses. The drastic development of AI over the last decade has enabled firms to induce real-time interactions with their customers [10]. Chat GPT, a generative pre-trained transformer (GPT), is a large language model that uses voluminous data to train deep learning algorithms [6]. The main purpose of creating chat GPT is to create a human-like response i.e. conversational AI model. It is expected that the emergence of this new form of GPT will bring a new form in the way of learning, communicating, working, etc.,

In general, AI learns from huge amounts of input data, such as text, video, and audio, and predicts the output using various machine learning algorithms. GAI sets an example for an unsupervised machine learning algorithm, as there is no target variable for most unstructured input data. Firms rely on AI models to create flawless, accurate, and relevant content. It imposes a great challenge to differentiate between the content generated by GAI models and human-generated content.

GAI creates new types of content with different types of input data, like text, images, and other forms of media [30]. Notably, chat GPT, a GAI model, is widely used in various operations, such as human resources, marketing, finance, information technology, and risk [9]. As chat bots are used to enhance machine-human interaction, chat GPT is also used to perform human tasks such as collaborating on company projects and generating content for campaigns [12]. The customized data created by GAI models in the form of text, video, image, etc., are used by marketing professionals to optimize their content generation process [5]. Notably, with the wide recognition of generative AI usage in content creation, the marketing industry uses it to create personalized and synthetic advertisements for its target customers. Synthetic advertisements pave the way for marketers to reduce their advertising costs, time, and resources, as they do not consume much equipment, actors, or locations to create synthetic advertisements. It enhances the personalized experience of customers and optimizes the creation of multimedia content [27]. Organizations should take considerable measures for employees to collaborate and use generative AI models to increase productivity. The use of Chat GPTs in business has both pros and cons, similar to any other technology. On the positive side, when used effectively, Chat GPTs can enhance operational efficiency, reduce costs, and increase profits [14].

However, there is a downside to this technology as well. Since chat bots like chat GPT rely on large amounts of training data that can be sourced from public sources, organizations should refrain from sharing confidential information with them as it may become public [12]. To prevent the use of chat GPT models with sensitive data, conversation history should be turned off to ensure it cannot be used for training. The growing concern over data privacy has led to increased bans on chat GPT by both organizations and countries [28]. In today's information age, the proper use of technology has greatly improved business operations. To ensure the successful implementation of Chat GPTs in business, it is essential to put strict security measures in place to identify fake data and protect data. Organizations should focus on maximizing benefits while minimizing losses. Generative AI created whitecaps in the minds of experts with the introduction of the GPT-2 in 2019. In particular, chat GPT text-generating AI systems have brought about a new dynamic transition in AI.

Generative AI:

Additionally, as the AI market size is expected to grow to $2025.12 billion by 2030 from $515.31 billion in 2023 [13], it is important for organizations to wisely use technology such as Generative AI models, which is the key drive of upcoming AI technology. However, it is also important to note that the forced adoption of AI can have negative consequences [16]. The use of Generative AI models has a wide range of applications across industries, from product development and design in manufacturing to medical simulation and chat bots in healthcare. In IT and telecom, Generative AI models are used for network optimization and security, intelligent infrastructure, and predictive maintenance. In marketing and advertising, it is used for targeted advertising and campaign analytics, while in the transportation industry, it is used for traffic monitoring and road condition detection. This technology has a significant impact in terms of forecasting energy and optimizing storage. To maximize its potential, organizations should utilize Generative AI models, which are expected to drive AI technology in the future. However, the adoption of AI may be forced upon organizations [16]. Despite its widespread use, this technology has been applied extensively in various areas such as supply chain management, customer interaction, marketing, and advertising. While chat GPT could potentially enhance the supply chain process, it may not be an immediate game changer in this complex area [3]. However, [20] suggests that chat GPT could improve customer satisfaction by streamlining interactions with stakeholders. The supply chain and logistics industry face several challenges, such as the need for effective route optimization, enhanced customer service with chat bots, and identifying wasted time to reduce costs. [23] suggests that the use of chat GPT can support and enhance customer service operations effectively. Studies indicate that chat GPT will play a key role in supporting and improving automation processes, inventory management, and communication with stakeholders [24]. Specifically, its ability to communicate and interact with stakeholders can enhance its efficiency. AI and Generative AI (GAI) have made significant contributions to marketing, with the latter having a positive impact on marketing [18].

The emerging technologies of AI enable organizations to enhance their customer experience by providing timely and relevant communication through the right platform [4]. Customer experience drives customer engagement toward products and accounts for the positive impact of customer loyalty [2]. GAI, a dynamic wave of digital technology has a significant contribution towards marketing processes than the previous digital technologies [18]. GAI empowers brands to create personalized messages and increase customer experience and engagement [18].

LLM

In large Language Models (LLMs,) a huge amount of data is trained using neural networks with more than billions of parameters and their corresponding weights [15]. The generative pre-training model one type of LLM uses a huge corpus of data to train the NLP neural network model and predict the possibility of the next word in the sentence [26]. The generative pre-training model is a long-established unsupervised machine learning model. In 2017, Google released the Transformer architecture, which uses an attention mechanism to weigh the importance of different words in understanding a piece of text. The Transformer architecture has proven successful in NLP tasks and served as foundational for the first iterations of LLMs, including BERT in 2018 [10] and XL Net in 2019 [26]. Generative Pre-trained Transformers, GPTs are one family of LLMs created by Open AI in 2019, and are used as a framework for creating GAI applications. Chat GPT, one type of chat bot application is built on top of Open AI's GPT-3.5 and GPT-4. Initially, Chat GPT exclusively used GPT-3.5 and continues to do so for the freely accessible tier, Paid subscribers, or Plus members. In addition to GPT3.5, GPT-4 also facilitates several additional plugins such as including web browsing (live up-to-date data retrieval), code optimization, etc., and it is made available through a limited alpha program.

Open AI hasn't declared much detail about GPT-4's architecture, model size, hardware, training compute, dataset construction, or training methods due to commercial competitiveness reasons. Despite the varied advantages of AI and GAI, the threats to the adoption of these tools impose a great challenge for organizations in terms of data security. To be stated in particular, AI provides a lot of opportunities in various fields like business, healthcare, education, technology, etc. along with emerging security threats.

Chat GPT:

[15] has stated on the Bloomberg website, that chat GPT was mostly used by school-going students, i.e it witnessed a drastic upward phase till March and a downward phase from March to June, which signifies that students were the major respondents of chat GPT. Though the students seem to be the major respondents, chat GPT has wide applicability in organizations. So, the ultimate responsibility lies in the hands of the user who uses it. In addition to its advantage of wide use in business, the major disadvantage is that it is also utilized by cyber attackers to hack the data of individuals, governments, and private organizations. As GAI models rely on huge input data to train the model, it serves as a boon for cyber attackers to use those data. Cyber attack is not a new threat, because it has been in existence since the inception of technology, so data breach is not an exception. The generative AI models have out thrown the opportunities for cyber attackers to create phishing emails with fewer or no grammatical errors.

The overwhelming response to chat GPT across the world has created a serious challenge and threat to employees and individuals because chat GPT uses the data and shares the information publicly. The research by Cyber haven states that, the data copied from chat GPT is twice that of the data pasted into chat GPT. In particular, data collected in 2023 from feb-26 to mar-4 reveals that incident per 1,00,000 employees, sensitive data i.e confidential and very secure data are shared by the employees into the AI bots 199 times, followed by client data 173 times, source code 159 times, regulated personal data 102 times, health data 94 times and project planning files 57 times [21].

Chat GPT, though not considered a legal entity is assured not to engage in illegal activities, share personal information and not to extract the IPR details, and finally not mimic an individual or an organization. If chat GPT is used to create phishing messages it states that it has no moral right to execute it. Open AIs' chat GPT designed with proper security compliances doesn't allow the attackers to create the phishing messages directly, rather it is the tactics used by the hacking professionals to trick it and create the hacking messages that have emerged as a serious threat to organizations. But with due consideration and the significant role of chat GPTs in organizations to increase profit and reduce cost, they could not be banned but could be regulated. Thus, the ultimate responsibility of the organizations is to ensure the proper implementation of security measures before the inclusion of these technologies.

Cyber Security Threats:

Despite various cyber security threats, this study focuses on the threats related to the use of the GAI model in creating malicious programs such as malware, ransom ware, phishing emails, Business Email Compromise, etc., In malware, the attacker tries to gain unauthorized access to other computer systems by exploiting their highly secured infrastructure. Phishing uses various modes of communication such as email messages, pop-up messages, instant messages, etc., to obtain highly sensitive information about Internet users [16].

Ransom ware:

Worldwide ransom ware has emerged as a dangerous threat to computer and network security [7]. It has been in existence for more than 35 years and has its widespread across various sectors. In addition, the [29] comparison of ransom ware attacks across countries in 22022 and 2023, indicates that the ransom ware attacks have increased in countries like Singapore, Austria, Australia, South Africa, Switzerland, the United States, and Spain but have in countries like India, France, Germany, Japan, and the United Kingdom. However, all the countries with decreased ransom ware attacks other than India were lower than the global average. In India, though the ransom ware is slightly less in 2023 than in 2022, the attack is still greater than the global average. In particular, ransom ware attacks across countries from July 2022 to June 2023 are as follows the US hits the tops with 1462 attacks followed by the UK (196) attacks, Canada (159), Germany (124), Italy (120), France (118), Spain (0), Brazil (77), Australia (74) and India with 64 attacks [31]. Ransom ware broadly classified into crypto-ransom ware and locker ransom ware enables the attackers to get access to the data in the host computer. Crypto-ransom ware encrypts data and makes it useless [19]. Locker ransom ware locks the user interface. These threats lead to a huge loss in finance and the reputation of the organization.

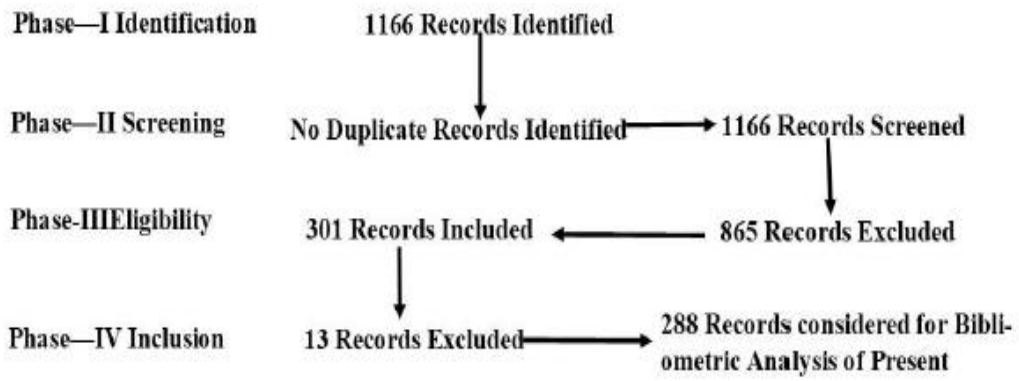
Despite its presence since 1989, it has hit the headlines in 2021 for eg: the Kasey a attack in 2021 which targeted the entire supply chain rather than a single person or business activity. Ransom ware attacks are enabled through RaaS i.e. Ransom ware-as-a-Service, which provides a platform for attackers to generate the code for ransom ware campaigns. Earlier, the attackers used to demand an amount to give the decryption key, but in recent times they have used it as double extortion, by storing data in a separate location and creating a threat of leaking to the public at any time. From 2022 onwards, they have started to attack unpatched systems.

Among various methods used to create ransom ware, one of the most commonly used methods for ransom ware is phishing. The IC3 2021 report represents that phishing occupies the top position in crime types [1]. Verizon 2022 report states that ransom ware and phishing attacks will occur every 11 seconds [22]. BEC phishing scam is the other most important and rapidly evolving phishing that targets not just financial data but also the personally identifiable data and wage and tax forms of individuals and businesses i.e. from small size to large corporations. BEC an erudite scam targets both individuals and business people. Particularly in the AI era, the generative AI model is used by cyber attackers to create BEC, spear phishing, and credential phishing.

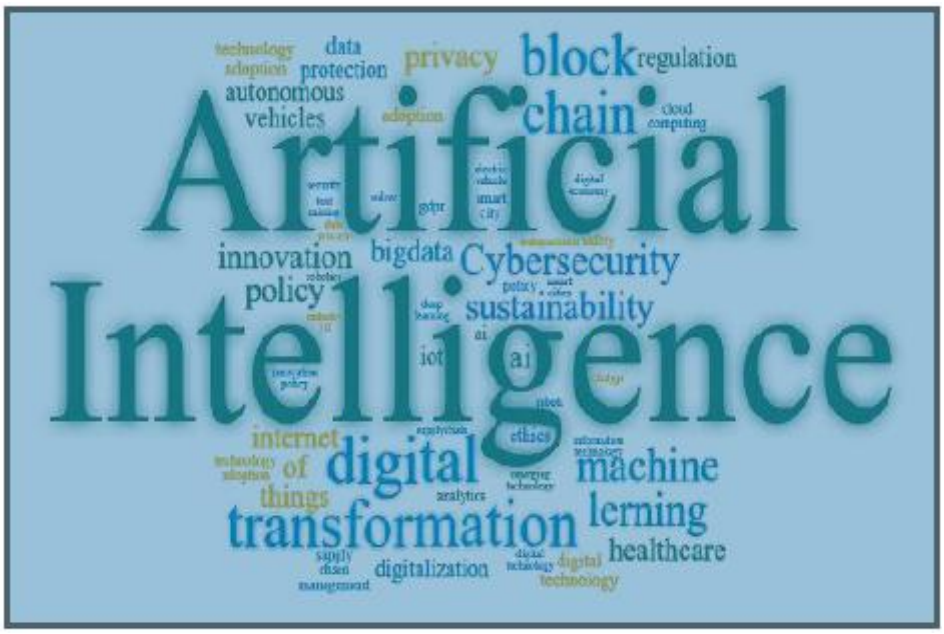
To identify the contribution of research in cyber security challenges in the management area, the study performed bibliometric analysis using VOS viewer.

Bibliometric Analysis:

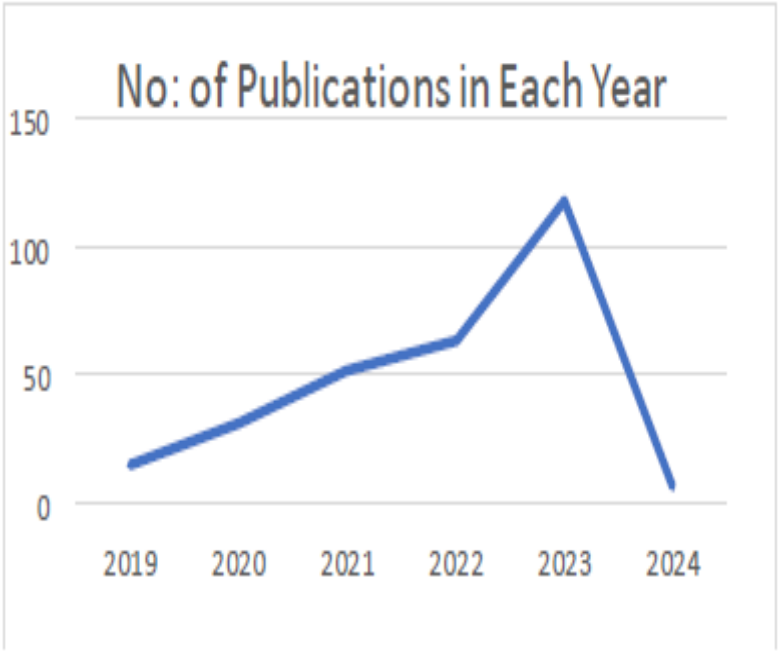
The bibliometric analysis uses a systematic approach to identify the contribution of research articles, books, etc., in a particular subject area, for a particular period, in a particular title, and so on.,. As the term cyber security has evolved along with the rise of the internet and other emerging technologies, there have been significant research contributions since 2000 from various subject areas such as computer science, engineering, technology, information systems, etc., But had only little and emerging contributions since past decade in the management area. Thus, to identify the contribution of studies related to the present study, the “Cyber security challenges in the AI age” keyword was used to search the records in the Science of Direct database. In phase I (identification phase) 1166 records were identified. In phase II (screening phase), the articles were screened for duplicate records, as no such records were found all the 1166 articles were included. In phase III (Eligibility phase), the records relevant to the study were identified in a step-by-step process, as a first step, the study focused on only business, management accounting, and social sciences as a result 350 records were included and the rest of the records were excluded. In the second step, as the study considered only research articles and books 301 records were included and the rest were excluded. In the next step, as the study considered only records from 2019 onwards 288 records were included and the rest were excluded (Figure 1). Finally, all the selected 288 records were downloaded in ris format and bibliometric analysis was executed using Vos viewer.



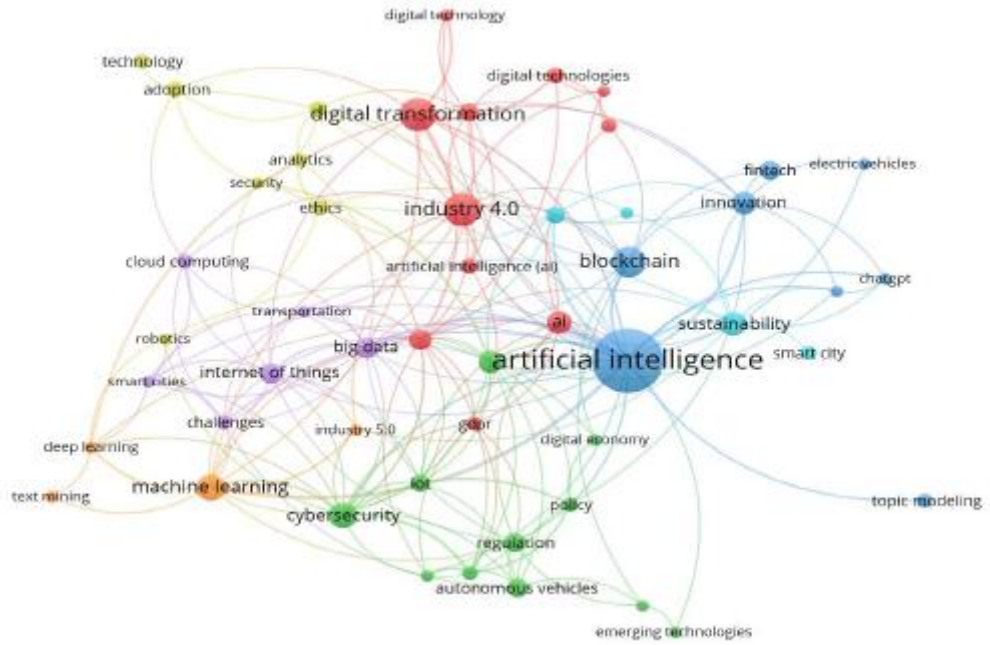
To perform the bibliometric analysis, the study opted for the co-occurrence of keywords in Vos viewer, and it was noted that out of 1213 keywords, 26 met the threshold with the minimum occurrence of keywords for five times, but the study set the minimum number of keywords to 3 and finally identified that 65 keywords met the threshold. Finally, in the keyword list, a few keywords based on the minimum number of occurrences and low link strength were excluded and the rest were included. For example, artificial intelligence occurred 51 times with a total link strength greater than 30, followed by cyber security 11 times, big data 8 times, machine learning 12 times, and so on.



A word cloud or tag cloud (Figure 2) was generated for the finally selected keywords because it signifies only the occurrence of a word and not its importance. Word cloud represents the textual data in graphical form i.e., a higher frequency indicates a greater number of occurrences and not its importance. Concerning the major keywords of the study, it could be observed that artificial intelligence has occurred more times followed by cyber security and chat GPT which have a very low number of occurrences than the other two keywords.



The number of records (research articles and books) from the selected subjects (business, management and accounting, social sciences) for the period of 6 years i.e. from 2019 to 2024 is represented in Figure 3. It could be observed that there has been a significant contribution of publications from 2019 to 2022, i.e from 15 publications in 2019 to 64 publications in 2022 and a drastic increase in the number of publications in 2023 with 118 publications, the study also considered 2024, to identify the contribution of studies to the area of study during this period signifying its relevance and importance. To identify and understand the relation between the items, a network map was generated. It could be observed from the network output five clusters were generated. in Figure 4, that the items are represented in circle or square, and a link established between the items is based on the strength of their relation, The network map in figure 6, represents five clusters based on the association between the items.



As cluster 1 represents the strong association between the technology items it is coined as technology, cluster 2 with a strong association between the items based on the privacy issues due to advanced technology components such as IOT in the automation process, which is named privacy and regulation. Cluster 3 is termed as AI innovation based on the association between AI and its association with other emerging AI technologies such as chat GPT, Block chain, Fin tech, Electric Vehicles, and Topic modelling, etc., Cluster 4 with 7 items i.e adoption, technology, robotics, technology adoption, analytics, ethics, and security is coined as technology adoption. Cluster 5 with a strong association between items that act as sources for big data, is termed a source of big data. Cluster 6 was coined as sustainability with 4 items and Cluster 7 is an AI algorithm because of its strong relevance towards advanced AI algorithms like deep learning, machine learning, and text mining.

Table: 1 Cluster details

Cluster Number	Cluster Name	Cluster Items
1	Technologies	AI, Artificial intelligence, Digital technologies, Digital technology, digital transformation, Digitalization, GDPR, Healthcare, Industry 4.0, Supply chain, Supply chain management
2	Policy and Regulation (11 items)	Autonomous vehicles, Cyber security, Digital Economy, Emerging Technologies, Innovation policy, IoT, Policy Privacy, Regulation, Robots, Safety
3	AI Innovation (8 items)	Artificial intelligence, Blockchain, ChatGPT, Electric vehicle, EU law, Fintech, Innovation, Topic Modelling
4	Technology Adoption (7)	Adoption, Analytics, Ethics, Robotics, Security, Technology Technology Adoption
5	Sources of big data (6 items)	Big data, Challenges, Cloud computing, Internet of Things Smart cities, Transportation
6	Sustainability – smart city (4 items)	Data protection, Information technology, Smart city, Sustainability
7	AI algorithms (4 items)	Deep learning, Industry 5.0, Machine learning, Text mining

The network diagram in figure: 5 represents the association between clusters and within clusters, the relation between the items is represented by links which represent its association based on the thickness of the link, the thicker the link stronger the association, and vice versa. To depict the relation, the study considered cluster1 relation within the same cluster items and with other cluster items.

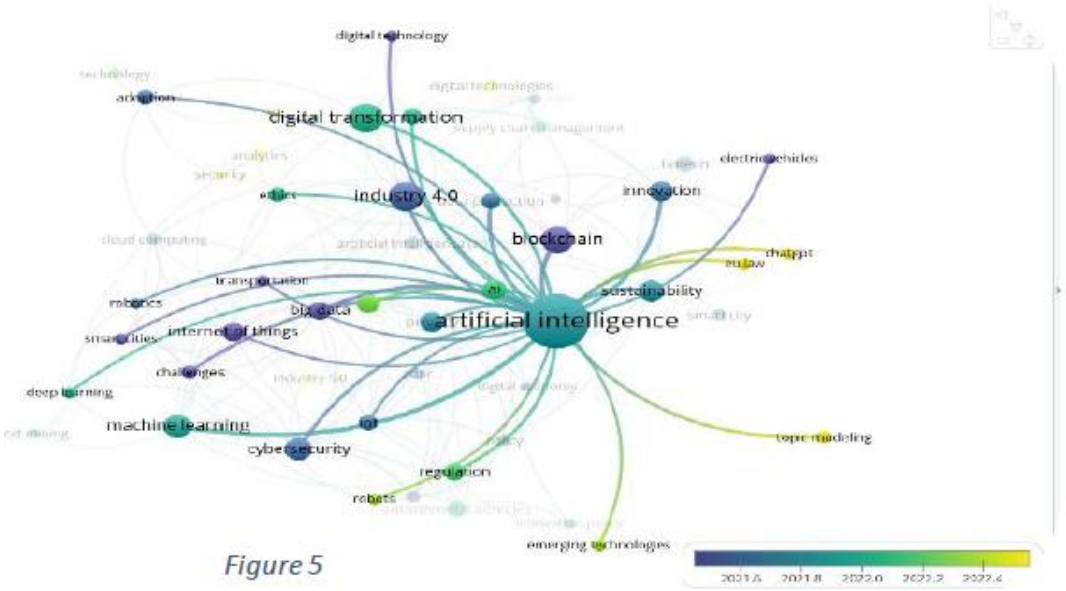


Figure 5

Artificial intelligence the important item of cluster 1 has a strong association with machine learning than with emerging technologies such as chat GPT, topic modelling, and so on. The strong association between AI and ML represents there exist more studies based on those items and the lighter association between AI and chat GPT, indicates that as chat GPT is an emerging technology the contribution of studies is in the emerging phase.

The network map in Figure 6 represents the items that have evolved over some time, use of varied colors for items indicates their utilization and importance during that period. For example, items such as technology, IOT, industry 4.0, and cyber security had more importance in 2021, artificial intelligence the key component had major importance in 2022 and the items like chat GPT, and topic modelling are considered emerging items or trending items since April 2022. This enables the researcher to identify the future area of research concerning technology.