RESEARCH PAPER

Cyber Crime Threats and Current Challenges: A Survey and Future Research Pathway

Satu Baruri[1], Pro K Sitamanikyam[2]

[1]Research Scholar, Dr B R Ambedkhar College of Law, Andhra University, Visakhapatnam-530003

[2]Principal, Dr B R Ambedkhar College of Law, Andhra University, Visakhapatnam-530003

ABSTRACT

The main aim of the present study is to analyses current trends within domain of cybercrimes and provide a future research agenda. This specific research utilized the established framework called Scientific Procedures and Rationales for Systematic Literature Reviews or Scientific Procedures and Rationales for Systematic Literature Reviews, to systematically review the numerous articles published in the Scopus database. Out of an initial pool of 1464 searches conducted, 269 articles that met the specified inclusion and exclusion criteria were carefully selected for inclusion in the final analysis within the study. The results from this broad survey indicate several different trends analyzed based on year, such as the countries that contributed their work, the lead authors of the research, the institutions represented, the influential journals where the work was published, and the number of citations for these articles. As such, this paper conducts a bibliometric analysis to identify and emphasize the most influential keywords within the field, focusing specifically on aspects of co-occurrence and bibliometric coupling with understanding relationships between various research themes. A total of six different clusters is identified for the thematic analysis. It represents a specific area of focus worthy of further exploration.

Keywords: Cyber Security; Bibliometric Analysis; Cyber Crimes; Society.

How to cite this article: Baruri S, Sitamanikyam PK. Cyber Crime Threats and Current Challenges: A Survey and Future Research Pathway. Int J Drug Deliv Technol. 2026;16(55s): 422-423. DOI: 10.25258/ijddt.16.55s.46

Source of support: Nil.

Conflict of interest: None.

1. INTRODUCTION

Remarkable advancement of information and communication technology, popularly known as ICT, has made life in the modern world considerably more convenient and efficient. Besides these benefits, an essential social problem appears to have surfaced, presenting itself as an alarming increase in crimes that take advantage of such advanced technology[1]. This kind of crime is dubbed "cybercrime," embracing a broad range of illegal activities carried out in cyberspace through computer-based systems that permit the perpetration of such illicit acts. In addition, a crime can be committed using any number of computer-based systems, personal computers, tablets, and smartphones, and now an exponentially increasing network, the Internet of Things [2], [3]. Moreover, it is possible or likely that a person will be a victim of cybercrime as other people are in contact with these new information technologies. Recently, there has been an increasing trend worldwide regarding the volume and sophistication of cybercrimes. The easy access to digital eco-space has made criminals commit more and more cybercrimes. Any person can be a cybercriminal, be it script kiddies or hackers, and may be an organized group or certain state governments [4]. There are many kinds of cybercrimes. Some of the diverse forms of crimes that relate to the Internet include pornography, extortion, data breaches, mail fraud, gambling, phishing, and copyright issues [5]. This, therefore, puts one of the most

[1] Y. R. Siwakoti, M. Bhurtel, D. B. Rawat, A. Oest, and R. C. Johnson, "Advances in IoT Security: Vulnerabilities, Enabled Criminal Services, Attacks, and Countermeasures," IEEE Internet Things J, vol. 10, no. 13, pp. 11224–11239, Jul. 2023, doi: 10.1109/JIOT.2023.3252594.

[2] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," Electronics (Basel), vol. 12, no. 6, p. 1333, Mar. 2023, doi: 10.3390/electronics12061333.

[3] R. Kumar, B. Kandpal, and V. Ahmad, "Industrial IoT (IIOT): Security Threats and Countermeasures," in 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), IEEE, Mar. 2023, pp. 829–833. doi: 10.1109/ICIDCA56705.2023.10100145.

[4] R. Yousef, M. Jazzar, A. Eleyan, and T. Bejaoui, "A Machine Learning Framework & Development for Insider Cyber-crime Threats Detection," in 2023 International Conference on Smart Applications, Communications and Networking (SmartNets), IEEE, Jul. 2023, pp. 1–6. doi: 10.1109/SmartNets58706.2023.10215718.

[5] O. Darwish, Y. Tashtoush, A. Bashayreh, A. Alomar, S. Alkhaza'leh, and D. Darweesh, "A survey of uncover misleading and cyberbullying on social media for public health," Cluster Comput, vol. 26, no. 3, pp. 1709–1735,

significant risks to the availability, integrity, and confidentiality of critical information stored within large corporations. Besides that, it threatens the privacy of individuals because it relates to many types of sensitive data, including information concerning health, details of the use of accounts of others, bank account details, and social media profiles [6]. The cyberattacks that occurred a couple of decades ago were much less complex than those in the present day, and fewer internet-based products demanded security protection [7]. In contrast, rapid technology growth has made the commission of electronic crimes easier and more sophisticated. Moreover, cybercrime has been exposed to more significant ramifications owing to the increased use of smartphones, IoT, social media, cloud computing, and cryptocurrency mining. Since the aftermath of cybercrime could be much more agonizing and painful to a woman, it is essential to learn more about why women go into all these reasons that provide the way for this kind of exploitation. There should also be an initiation of viable solutions that can stop this considerable problem [8]. Presented a more consolidated and comprehensive understanding of the current circumstances regarding cybercrimes, especially those committed against women, through various statistical tools and methodologies useful in predicting and forecasting emerging trends characterizing cybercrimes against women[9]. High importance is laid on disseminating such vital knowledge through well-designed programmes targeted at individuals and groups. Such structured programs can be repeated in several spheres and directed to a greater cross-section, thus influencing the audience more effectively. Designing such programs can reduce the possibility of people becoming prey to an attack[10]. It is essential for subsidiary preparation and dissemination of training and information to society to prepare them to better detect and respond to attacks. This particular approach shall indeed be sustained and continued into further work that involves collaboration with members of different institutions, including those who may not possess in-depth knowledge of the topic, at least as far as computer science is concerned[11]. Furthermore, comprehensive techniques will also be designed to help learners deal properly and respond appropriately to phishing e-mails they might encounter.

2. Research Questions

This review explores the current status and condition of the ongoing research concerning cybercrimes within our society. To achieve this objective, the study has carefully formulated and articulated the following specific research questions:

RQ1: Identify and critically review the current research trends in cyber-crimes and cyber security.

RQ2: What is this existing research gap in current times, and how would identifying the said gap lead to the development of future courses?

3. METHODOLOGY

One of the most used secondary research methods is the systematic literature review, showing high rigor and scientific integrity. A systematic review is conducted to yield valid and reliable findings by employing a predetermined systematic approach and applying a strict, exact

Jun. 2023, doi: 10.1007/S10586-022-03706-Z/TABLES/6.

[6] S. Duary, P. Choudhury, S. Mishra, V. Sharma, D. D. Rao, and A. Paul Aderemi, "Cybersecurity Threats Detection in Intelligent Networks using Predictive Analytics Approaches," in 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM), IEEE, Feb. 2024, pp. 1–5. doi: 10.1109/ICIPTM59628.2024.10563348.

[7] M. N. Alam and Md. S. Kabir, "Forensics in the Internet of Things: Application Specific Investigation Model, Challenges and Future Directions," in 2023 4th International Conference for Emerging Technology (INCET), IEEE, May 2023, pp. 1–6. doi: 10.1109/INCET57972.2023.10170607.

[8] K. F. Steinmetz, B. P. Schaefer, C. G. Brewer, and D. L. Kurtz, "The Role of Computer Technologies in Structuring Evidence Gathering in Cybercrime Investigations: A Qualitative Analysis," Crim Justice Rev, p. 073401682311610, Mar. 2023, doi: 10.1177/07340168231161091.

[9] Cyber Crime in India: An Analysis of Crime Against Women in Ever Expanding Digital Space by R. Sankhwar, R. Ahuja, T. Choubey, P. Jain, T. Jain, and M. Verma, published in *Security and Privacy*, Vol. 7, No. 1, Jan 2024. https://doi.org/10.1002/spy2.340.

[10] Cybercrime on a Global Scale: Trends, Policies, and Cybersecurity Strategies by V. R. Gajjar and H. Taherdoost was presented at the *2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*. Published by IEEE in January 2024, the paper discusses worldwide cybercrime trends, cybersecurity policies, and strategic measures for strengthening digital security, and appears on pages 668–676. https://doi.org/10.1109/ICMCSI61536.2024.00105.

[11] Cyber Security Challenges in Social Meta-verse and Mitigation Techniques by A. Chaudhari and co-authors.https://doi.org/10.1109/MITADTSoCiCon60330.2024.10575295](https://doi.org/10.1109/MITADTSoCiCon60330.2024.10575295).

methodology. The systematic literature review has transparency to peer review, scientific rigor, and replicability by other researchers with a very high degree of consistency. A systematic literature review on cybercrime and cyber laws was conducted using the Scientific Procedures and Rationales for Systematic Literature Reviews (SPAR-4-SLR) framework. This method has been widely recognized and adopted by researchers in conducting comprehensive and reliable literature review studies across various fields[12], [13]. Figure 1 shows the research methodology using "SPAR-4-SLR".

3.1. Assembling

The identification stage of the SPAR-4-SLR framework involves examining the research domain, framing research questions, determining the type and quality of sources, and collecting relevant articles for review. Since articles form the core of the study, the researcher primarily concentrates on identifying suitable and credible publications. In this systematic literature review on cybercrimes, the "what" aspect of the study is addressed through the formulation of closely connected research questions, namely RQ1, RQ2, and RQ3.

3.2. Arranging

The second stage of the SPAR-4-SLR process, known as arranging, involves the careful application of inclusion and exclusion criteria to select the most relevant and reliable sources for the study.All the items returned from the first search were meticulously organised and cleaned through this essential study component. This critical part of the study employed the category code tool provided by Scopus to systematically classify the substantial corpus of 1461 articles collected during the previous assembling stage of the research process.

3.3. Assessing

In the entire SPAR-4-SLR process, the third phase, comprehensive statistical analysis was conducted concerning parameters such as the year in which they were published, the highest cited ten papers, the ten most contributing leading journals to the field, participating countries, types of studies conducted, and various techniques used to collect data.

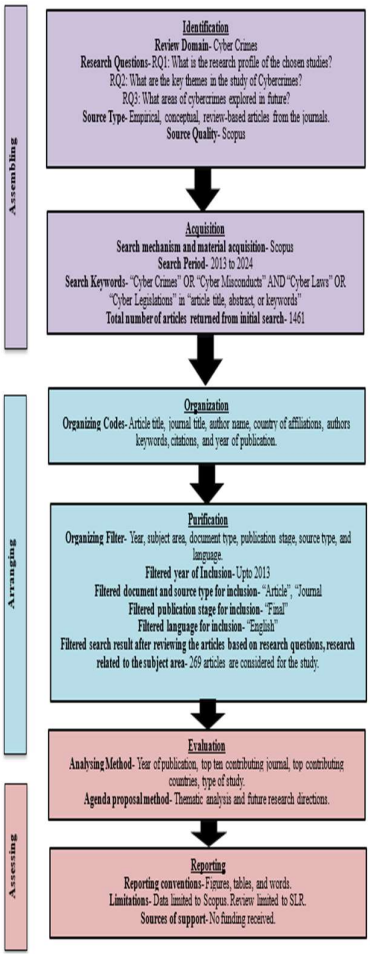

Figure 1: Articles Selection Procedure **Source:** Adapted from [12]

4. FINDINGS

There were 262 papers selected, analyzed in minute detail, and placed in distinct categories; however, these categories were generated based on fundamental characteristics. The primary characteristics encompass essential elements, including publication patterns, types of journals through which the research appeared, citation counts, and various geographic locations through which the study was conducted.

[12] J. Paul, W. M. Lim, A. O'Cass, A. W. Hao, and S. Bresciani, "Scientific procedures and rationales for systematic literature reviews (SPAR-4-SLR)," Int J Consum Stud, vol. 45, no. 4, pp. O1–O16, Jul. 2021, doi: 10.1111/IJCS

[13] The Interplay Between Psychological Empowerment and Employee Engagement: Identifying Research Trends Using SPAR-4-SLR Process by N. Kaul, A. Deshpande, A. Mittal, R. Raut, and H. Bhandari was published in Global Knowledge, Memory and Communication as an ahead-of-print article in 2024. The study explores the relationship between psychological empowerment and employee engagement through a SPAR-4-SLR-based review of emerging research trends. https://doi.org/10.1108/GKMC-09-2023-0322/FULL/XML.

4.1. Publications trends based on year and country

As presented in Figure 2, there is a remarkable rise in publication trends, which was distinguished during this year, along with a particular interest in the most modern subjects of cybercrime and cyber security. Figure 3 depicts in graphic form that the country with the highest percentage trend in publications is the USA.

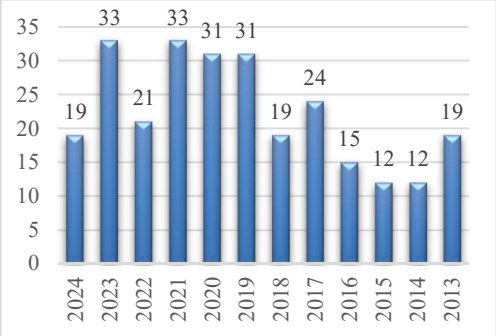

Figure 2: Publications trends year-wise

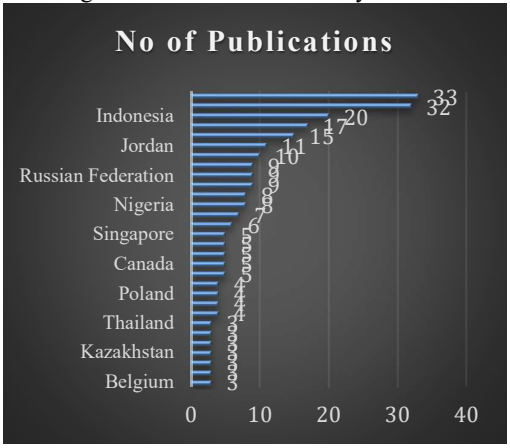

Figure 3: Country-wise publications trends

4.2. Top authors, institutions, and organizations in the research domain

Table 1 summarizes the key authors producing work within the domain of cyber-crimes and securities, specifically including the number of articles published over the last five years. There is a list of the top fifteen authors representing their respective countries with their contributions to this urgently needed field of study. Figure 4 shows the universities with maximum publications in the research domain.

4.3. Top journals and citations of the articles

Table 1 ranked the top fifteen journal publications both by total citations and number of total publications. In the above-classification journals, the International Journal of Cyber Criminology tops the chart by recording the higher number of 29 publications with a total number of 493 citations. Table 2 shows the top cited papers in the research domain.

Fig 4: Top institutions/universities wise publication trends

Table 1: Top authors in the research domain

Author Name	University/Institutes/Departments	Country	No of Publications	Top Journals	Total Citations	Total Publications
Baggili, Ibrahim M	LSU College of Engineering	United States	4	International Journal Of Cyber Criminology	493	29
Hamin, Zaiton	Universiti Technology	Malaysia	3	Computer Law and Security Review	123	18
Wan Rosli, Wan Rosalili	University of Bradford	United Kingdom	3	International Journal of Electronic	39	8

				Security And Digital Forensics		
Manap, Nazura Abdul	Universiti Kebangsaan Malaysia	Malaysia	2	Forensic Science International Digital Investigation	35	8
Apostolopoulos, Theodore K	Athens University of Economics and Business	Greece	2	Journal Of Financial Crime	34	6
Açar, Kemal Veli	Turkish National Police	Turkey	2	Digital Investigation	81	6
Kudrat-E-Khuda, Kudrat E	Department of Law, Dhaka University	Bangladesh	2	Computer Fraud And Se	22	6
				curity		
Cascavilla, Giuseppe	Technische Universiteit Eindhoven	Netherlands	2	Pakistan Journal Of Criminology	19	5
Ganta, Satish Kumar	K L Deemed to be University	India	2	International Journal Of Scientific And Technology Research	19	5
Gritzalis, Dimitris A	Athens University of Economics and Business	Greece	2	Journal Of Money Laundering Control	44	4
Kamaruddin, S	Universiti Pendidikan Sultan Idris	Malaysia	2	International Journal	5	4

				Of Recent Technology And Engineering		
Khan, Shah Khalid	RMIT University	Australia	2	Computers In Human Behavior	74	4
Khan, Abdullah Ayub	Sindh Madressatul Islam University	Pakistan	2	Computers And Security	113	4
laghari, Asif Ali	Sindh Madressatul Islam University	Pakistan	2	Security Journal	14	3
Levi, Michael A	College of Arts, Humanities and Social Sciences	United Kingdom	2	Journal Of Legal Ethical And Regulatory	2	3
				Issues		

Table 2: Most cited papers in the research domain

Authors	Title of the Article	Total Citations
[15]	The Rise in Popularity of Cryptocurrency and Associated Criminal Activity	92
[16]	The Future of Digital Forensics: Challenges and the Road Ahead	82
[17]	Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice	80
[18]	The effect of de-individuation of the internet troller on criminal procedure implementation: An interview with a hater	60
[19]	Assessing the trends, scale and nature of economic cybercrimes: overview and Issues: In Cybercrimes, Cybercriminals and Their Policing, in Crime, Law and Social Change	58
[20]	Fear of cyber-identity theft and related fraudulent activity	57
[21]	Cybercrime threat intelligence: A systematic multi-vocal literature review	53
[22]	Cyberbullying and the law: A review of psychological and legal challenges	43

[23]	Cyberfraud and the implications for effective risk-based responses: themes from UK research	41
[24]	Cyber forensics needs analysis survey: Revisiting the domain's needs a decade later	41
[25]	Public-private cybersecurity	38
[26]	Towards a systemic framework for digital forensic readiness	37
[27]	Regulating cyber-security	34
[28]	Validation of a Cyberbullying Serious Game Using Game Analytics	33
[29]	A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles	30

4.4. Influential keywords in the research domain

Keywords in research articles are critical to the identification of such articles. Table 3 shows the most common keywords in the research area on cybercrimes and cybersecurity based on their frequency in several publications.

4.5. Keyword occurrences and their ranking

All the frequency appearances of each keyword, their description overall strength, and features ranking system based on the number of times these keywords are mentioned in Table 3. It is amusing that the term "cybercrime" was provided in 62 articles, thereby making it the most recurrent keyword in this list, while its total link strength was computed to be 302.

Table 3: Top keyword occurrences and their recent citations

Authors Keywords	**Frequency**	**Recent citations**	**No of occurrences**	**Total Link Strength**	**Ranking for the keywords**
Cybercrime	62	[30], [31]	62	302	R 1
Cyber Security	35	[32], [33]	61	197	R 2
Law Enforcement	24	[34], [35]	28	152	R 3
Digital Forensics	16	[36], [37]	24	80	R 4
Electronic Crime Countermeasures	14	[38], [39]	16	94	R 5
Network Security	12	[40], [41]	12	81	R 6
Cyberbullying	11	[31], [42]	11	30	R 7
Social media	9	[35], [43]	9	32	R 8
Data Privacy	8	[44], [45]	8	51	R 9
Cyber Terrorism	8	[44], [45]	7	32	R 10.5
Cyber Law	7	[34], [35]	7	21	R 10.5
Digital Evidence	5	[46], [47]	6	23	R 12
Dark Web	5	[15], [16]	5	28	R 13
Criminal Law	5	[33], [44]	4	38	R 14.5
Financial Crime	4	[37], [48]	4	23	R 14.5

4.6. Co-occurrence and Bibliographic Coupling

The above analysis, which focuses on the co-occurrence of words used by the author, provides crucial and significant information that

develops a relationship and associates various concepts relating to cybercrimes and aspects of cyber security. To visualize this co-occurrence of authors' keywords, please refer to Figure 5. Moreover, please see Table 3 to view the list of keywords accompanied by the most frequently occurring cybercrime-related keyword.

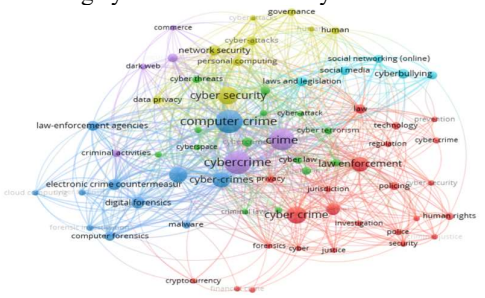

Fig 5: Co-occurrence with authors' keywords

5. Thematic Cluster Analysis

In thematic analysis, six clusters are identified in cyber security and cybercrime research. The themes are discussed as follows:

5.1. Cluster 1- Cybercrime and Cybersecurity

A combination of different forms of cybercrimes has been complied with in the literature review. Cybercrime includes an extended range of activities that encompasses but is not limited to, phishing, fraud from credit cards, Cybercrimes include offences such as bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping of minors through chat rooms, online scams, cyber terrorism, creation and spread of computer viruses, and the circulation of unsolicited commercial messages.In addition, it includes traditional crimes requiring computers or networks to achieve illegal activities[14]. More than 61 per cent of all business and social interactions happen online. Thus, it is imperative to have proper security standards in place further to promote smooth, efficient, and secure interactions, with particular emphasis on areas such as data protection, privacy concerns, reliability and availability of systems, and cybersecurity[15].

5.2. Cluster 2- Cyber Laws

Legal issues about information technology, encompassing computers and the internet, are called cyber law or IT law. The Department of Cyber Law oversees the electronic inflow of information, software, information security, and e-commerce about legal informatics[16]. Consumers depend on cyber laws to protect themselves from fraudulent activities perpetrated by fraudsters online. Modern online currency crimes have been controlled with legislation that helps to reduce identity and credit card theft. Copyright infringement has been made easy with the invention of the internet. Initially, it was easy to misuse intellectual property rights in online communication.

5.3. Cluster 3- Digital Forensics Investigation

It is the systematic process of retrieving and organizing information from electronic devices for investigative purposes. To this end, professionals must be well-trained in the technologies, methodologies, and frameworks. Moreover, the field is divided into four main branches: host forensics, mobile forensics, network forensics, and cloud forensics. Host forensics is often called digital forensics[17]. This is because it encompasses the kind of forensics conducted on standard apparatus, including computers, desktops, servers, and other typical data sources.

5.4. Cluster 4- Cyber Attacks

A cyberattack refers to a deliberate attempt to steal, access, alter, damage, or destroy data, software, or other digital assets through unauthorized access to a computer system, network, or electronic device. Such attacks can seriously disrupt or even completely damage business operations and digital services. The motives behind cyberattacks vary widely, ranging from financial gain and personal revenge to espionage, terrorism, or even acts related to warfare.Various methods of access to the wanted systems include deploying viruses and fraud activities that trick victims into allowing them to lose their passwords. This type of attack produces excessive traffic that overloads the system, rendering it unable to service valid requests and diminishing its overall performance capability[18].

---

[14] New Geographies of Crime? Cybercrime, Southern Criminology and Diversifying Research Agendas by T. Hall and R. Yarwood was published in Progress in Human Geography, Vol. 48, No. 4, in August 2024.

[15] Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach by S. Nazah, S. Huda, J. Abawajy, and M. M. Hassan was published in IEEE Access, Vol. 8, in 2020.

[16] The Rise of Cybercrime and Cyber-Threat Intelligence: Perspectives and Challenges From Law Enforcement by G. Cascavilla was published in IEEE Security & Privacy in June 2024.

[17] C. Grajeda, J. Berrios, S. Benzo, E. Ogunwobi, and I. Baggili, "Expanding digital forensics education with artifact curation and scalable, accessible exercises via the Artifact Genome Project," Forensic Science International: Digital Investigation, vol. 45, p. 301566, Jul. 2023, doi: 10.1016/J.FSIDI.2023.301566.

[18]The Evolution of Ransomware Attacks in Light of Recent Cyber Threats: How Can Geopolitical Conflicts

5.5. Cluster 5- Security of Data

Data security refers to protecting electronic information at every stage of its lifecycle so that no damage, theft, or unauthorized access by parties without rightful authority occurs. It includes factors ranging from hardware, software, storage devices, and end-user devices; access controls and administrative controls; and policies and practices of organizations [19] . In addition, Masking Data helps organizations enable teams to build applications, train end users to interact with the correct data and mask PII when necessary to encourage the development of compliant environments.

5.6. Cluster 6- Cyberbullying using social media

Cyberbullying is defined as any case of bullying behavior that the help of computer technology has performed. Many believe that online platforms such as Facebook, Twitter, and Instagram are vital means of communication and connection. Social media bullying could be agonizing and worse than face-to-face bullying[20].

6. FUTURE RESEARCH AGENDAS/DIRECTIONS

So many themes have developed in cybercrimes and security that have been altered because of keyword pairing methods and research mapping. As discussed earlier, these themes are essential elements that demand more significant attention and research. Utilizing such topics might allow the advancement and development of such work. Such problems can be addressed with more intense study and investigation in this field, resulting in breakthroughs in identifying cyber-crimes and developing a cyber-safe environment.

6.1 Future Theme 1- Exposure of the Cyber Crime Using Machine Learning

Machine learning is the scientific field that predicts the outputs from input data, often called "training data." The machine could learn how to correctly and appropriately predict appropriate outputs for specific inputs using the training data. As far as how one can enter this learning process is concerned, it may be performed either by supervised or unsupervised methods. For instance, machine learning can go through millions of files and find potentially dangerous ones. Because of this, it is being used more to find problems and fix them before they cause much harm[21]. Companies now use machine learning to act before cyber-attacks happen instead of waiting for them. Penetration testing is used to find any weak points in a company's networks, firewalls, and systems by pretending to be an attacker. It, therefore, helps discover the hidden weak spots. This work may also include applying software updates, fixing some code, and using other methods to correct weaknesses in a company's security system using machine learning [22].

6.2 Future Theme 2- Strict cyber laws in the nation

Cyber laws are urgently needed so cybercrimes can be avoided easily. The only legislation in India that discussed cyber-attacks was the Information Technology Act of 2000 and any amendments thereafter. The law has different kinds of crimes. These include breaking someone's privacy, stealing their identity, uploading offensive content, child pornography, and so on. However, some areas are lacking in the law, like cyberbullying, forgery, and piracy [23] . This is because breaking someone's privacy can land somebody in jail and require fines of up to two lakh rupees. If one is found guilty of creating and distributing child pornography, then the punishment will be up to 10 lakh rupees, along with a maximum imprisonment term that would be five years.

6.3 Future Theme 3- Fake profiles and their detections

Social media such as Facebook, Twitter, and Instagram significantly impact life. It is

---

Influence the Cyber Climate? by F. Teichmann, S. R. Boticiu, and B. S. Sergi was published in the International Cybersecurity Law Review, Vol. 4, No. 3, in July 2023.

[19] Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues by M. Levi was published in Crime, Law and Social Change, Vol. 67, No. 1, in February 2017.

[20] Growth of Cyber-crimes in Society 4.0 by V. Sharma, T. Manocha, S. Garg, S. Sharma, A. Garg, and R. Sharma was presented at the 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM 2023).

[21] Indian Government Initiatives on Cyberbullying: A Case Study on Cyberbullying in Indian Higher Education Institutions by M. Kaur and M. Saini was published in Education and Information Technologies, Vol. 28, No. 1, in January 2023.

[22] M. G. Porcedda, "Sentencing data-driven cybercrime. How data crime with cascading effects is tackled by UK courts," Computer Law & Security Review, vol. 48, p. 105793, Apr. 2023, doi: 10.1016/J.CLSR.2023.105793.

[23] I. Arpaci and O. Aslan, "Development of a Scale to Measure Cybercrime-Awareness on Social Media," Journal of Computer Information Systems, vol. 63, no. 3, pp. 695–705, May 2023, doi: 10.1080/08874417.2022.2101160.

something people actively engage in worldwide. There is also an imperative task of identifying bogus profiles. Now, people, software, and even machines mostly create fake accounts. Businesses can now provide services that utilise machine learning and big data analytics to identify any possible fraudulent activity. You can figure this out by checking the user's background information, for example, how often accounts are requested from IP addresses similar to the users or by watching out for weird activity on new or mostly fake accounts[24]. Such acquisitions and usages allow the detection and suspension of fraudulent or bot profiles that may interact with and damage your organization's system or website.

6.4.Future Theme 4- Deep Fakes

Deepfakes are a form of video, audio, or pictorial manipulation involving super-powerful computers and deep learning. It is used for inappropriate aspects, such as fake news and financial scams. Cybercriminals use AI-powered technology to create an image that will be overlaid on an existing video, picture, or sound [25] . Deepfakes technology is being put to many wrong uses, from hoaxes and frauds, fake celebrity pornography, election rigging, social tricks, algorithmic diffusion of falsehoods, identity theft, and money scams, among others. The only way to contain this issue is through a technological solution with AI that can detect and hopefully prevent deep fake situations from occurring.

6.5. Future Theme 5- Supply Chain and Logistics Attacks

A supply chain attack is a specific type of cyberattack conducted against an organisation's suppliers to gain unauthorised access to that organisation's systems or data. In some contexts, attacks involving hostile code penetration into an organisation's systems are called value chain or third-party software attacks [26] . These kinds of attacks require careful planning by the threatening parties involved. A supply chain attack aims to gain access by implanting a backdoor into the products, often software, that the attacked organisations use. This allows malware and other methods of attacks to be introduced into the system through automated patches or software upgrades that have been "trojanized"

6.5. Future Theme 6- Creating the organizations to be Cyber Resilience

Cyber resilience at the organizational level is defined as the ability to achieve the intended outcome in the face of cyberattacks effectively. Hence, the asset pool of information is protected by its ability to defend itself against cyberattacks, such as information technology systems, critical infrastructure, business processes, and organizations' entities in society and nation-states[27]. More importantly, the loss of money and reputational harm are further areas where cyber resilience exercises help. Among several advantages of adopting a cyber-resilience strategy is being able to respond appropriately to any given incident or cyber threat quickly. This strategy generalizes security through methodologies meant to enhance IT governance, expand data protection, reduce the impacts of natural disasters, and curb human error. This gives rise to "cyber resilience" as a marriage of operation resilience with cybersecurity.

7. CONCLUSION

Cybercriminals can utilize computer technology to gain unauthorized entry into confidential information and/or trade secrets owned by business concerns, thus taking such information to their advantage through the Internet. Cybercrime is always capable of causing effects, which can be significantly important. Individuals suffer from financial losses and certain identity thefts. Companies also suffer injuries in terms of reputation, along with punishments in courts of law. Another interesting aspect of cybercrime is that it has the potential to impact society's economy negatively, threaten national security systems, and increase instances of cyberbullying and cyber harassment. This research article discusses cybercrime and its implications for society. Moreover, this paper uses the SPAR-4-SLR approach to analyse the various articles

[24] J. Gruber, L. L. Voigt, Z. Benenson, and F. C. Freiling, "Foundations of cybercriminalistics: From general process models to case-specific concretizations in cybercrime investigations," Forensic Science International: Digital Investigation, vol. 43, p. 301438, Sep. 2022, doi: 10.1016/J.FSIDI.2022.301438.

[25] H. Nobanee, A. Alodat, R. Bajodah, M. Al-Ali, and A. Al Darmaki, "Bibliometric analysis of cybercrime and cybersecurity risks literature," J Financ Crime, vol. 30, no. 6, pp. 1736–1754, Dec. 2023, doi: 10.1108/JFC-11-2022-0287.

[26] A. Despotović, A. Parmaković, and M. Miljković, "Cybercrime and Cyber Security in Fintech," 2023, pp. 255–272. doi: 10.1007/978-3-031-23269-5_15.

[27] Cybercrime on a Global Scale: Trends, Policies, and Cybersecurity Strategies by V. R. Gajjar and H. Taherdoost was presented at the 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI) and published by IEEE in January 2024.

retrieved from the Scopus database. Overall 1464 articles were extracted from the primary search, and finally, 269 articles were studied by applying the inclusion-exclusion criteria. The study's findings have been drawn upon year-wise and country-wise trends followed by top authors and institutions in the research domain of cybercrime. Also, journals publish articles in the research domain and most referred articles. Some of the six identified future research domains include detecting cybercrime through machine learning approaches, enforcing strict cyber laws across the country, identifying spoofed profiles, the issue of deepfakes, supply chain attacks, and cyber resilience. This will go a long way in positively affecting society's perception of cybercrimes, while upcoming research trends will help researchers fetch some insights.

7.1 Study Limitations:

The study has some limitations, and thus these are considered in further studies. The first is that this study accesses articles via the Scopus database only. However, additional studies may embrace other databases besides Scopus, including the Web of Science database. The other limitation of this study is that it is review-based, whereby the empirical research could be done on cybercrime.