The Journal of Asia Entrepreneurship and Sustainability RESEARCHARTICLE

Global Trend in Cybercrime and Internet Users' Security: A Bibliometric and VOSviewer Analysis (2017–2026)

Ms. Sweeti[1], Dr. Himanshu Mathur[2], Dr. Sunita Verma[3]

[1]Research Scholar, School of Business, Mody University of Science and Technology, Lakshmangarh, Sikar, Rajasthan.
[2]Assistant Professor, School of Business, Mody University of Science and Technology, Lakshmangarh, Sikar, Rajasthan.
[3]Professor, School of Business, Mody University of Science and Technology, Lakshmangarh, Sikar, Rajasthan.

Abstract
This study offers a comprehensive systematic literature review of cybercrime and user security awareness from 2017 to 2026. From the Dimensions database, 517 open-access research articles were collected using keywords such as "cyber security", "cybercrime," and "internet users". Using Microsoft Excel and VOSviewer, we performed Bibliometric analysis to examine citation patterns, publication trends, thematic clusters, countries, and publication output. The results show a significant rise in cyber security research, particularly after 2020, due to growing cyber threats and digital transformation. Most studies focus only on technology-related aspects. However, significant gaps remain in user awareness, behavioural cyber security, and data availability. The study proposes a conceptual framework linking cyber threats, user awareness, and security mechanisms. The finding offers discernment for policymakers, practitioners and researchers to strengthen cyber security awareness and governance.

Keywords: Cyber security, Cybercrime, User Awareness, Internet Users, Phishing, Data Security, Digital Risk.

1. Introduction

Over the last few years, the rapid growth of digitalization has completely changed how we connect socially, operate businesses, and manage institutions globally. Increased digitalization has improved efficiency and accessibility through the use of internet-based systems in these sectors for example, healthcare, banking, governance, and education. At the same time, it has increased cyber risk for internet users. The wider adoption of digital technology has turned cyber-attacks into a pressing global issue, increasing the risk to the safety of personal data, corporate networks, and national security systems (Alkhalil et al., 2021)

By the term Cyber-crime, it refers how criminal use the computer either as a tool or as a target to harm user's data and information. Examples of cybercrime are phishing, identity theft, ransomware attacks, and unauthorized access to confidential information. Over time, these crimes are increasing rapidly and affect human life. They use social engineering methods to exploit human vulnerabilities instead of technical issues.

Cybersecurity has become a multidisciplinary field that aims to protect digital assets through technical, organizational, and behavioural measures. Cybersecurity includes intrusion detection, spam detection, and malware detection on computer and mobile networks.

Evidence indicates that human factors continue to be a critical point of failure even if much progress has been achieved in the development of cutting-edge cybersecurity technology, particularly through the use of AI and machine learning.

No matter how advanced a cybersecurity system people use, if they use it carelessly, it will fail, and hackers exploit this vulnerability. That's why attacks like phishing and social engineering are so successful because ordinary internet users lack awareness and habits.

The reality is now forcing us to change the way we view digital security, where user behaviour is being considered as a core component of the modern security model. However, if we look at the research and studies done so far, we see a significant gap. First, most research focuses solely on technical fixes and completely ignores the human behavioural aspects. Furthermore, gathering data on this topic is extremely difficult because companies do not openly disclose information about cyber-attacks, leading to a significant lack of reliable and accurate data for research (Cremer et al., 2022). New threats have added to the woes; ransomware and AI attacks are evolving so rapidly that our old security strategies are quickly rendered useless (Beaman et al., 2021). We cannot address these gaps unless we review what has already been done. To address this need, this study presents A Bibliometric Analysis to understand internet users' awareness and the evolving nature of cybercrime. Analysing the period from 2017 to 2026, we extracted 620 research papers from the Dimensions database.

2. Literature Review

The domain of cyber security and cybercrime has witnessed substantial scholarly attention because of the rapid growth of digitalization and the rise of cyber threats in the last decade. The literature currently in publication can be generally classified into four major thematic sections.

(1) Technological advancements in cyber security
(2) Social engineering and phishing attacks.
(3) Artificial Intelligence (AI) in cyber security.
(4) Cyber risk and data availability challenges

2.1 Technological advancements in cyber security

A major portion of the literature focuses on technological solutions designed to prevent, detect, and mitigate cyber threats. For example, machine learning and data-driven methods have gained significant popularity because they have the ability to process large volumes of data and identify anomalous patterns. Machine learning techniques have enhanced capabilities for intrusion detection, malware classification, and threat prediction, enabling more effective identification of constantly evolving and complex threats (Shaukat et al., 2020). Compared to traditional rule-based systems, these approaches foster automation and improve detection accuracy.

While these technology advancements significantly help strengthen cybersecurity infrastructure, they primarily focus on system-level vulnerabilities and often overlook the human element, a crucial factor in cybersecurity.

2.2 Social engineering, ransomware and phishing attacks

Phishing is currently one of the most prevalent forms of cyber fraud on the internet, enabling criminals to deceive users and steal their sensitive data. Phishing attacks primarily target human vulnerabilities rather than technical flaws (Alkhalil et al., 2021). These threats are becoming increasingly sophisticated, with criminals employing psychological manipulation and social engineering strategies to induce people to share sensitive information.

Phishing detection has become progressively complex due to the dynamic nature of attack strategies and the use of personalised targeting (Basit et al., 2020).

These studies highlight that even the most advanced security technology can be rendered ineffective if deceptive communication goes undetected. These reinforce the argument that both user education and awareness are essential for cybersecurity.

An analysis of the evolution of ransomware reveals that modern attacks are highly organized and targeted; hackers frequently employ a “double extortion” strategy, wherein they not only encrypt data but also threaten to leak sensitive information. Such fraudulent activities are rapidly increasing, resulting in massive financial losses.

2.3 Artificial Intelligence (AI) in cybersecurity

AI has significantly improved cybersecurity’s ability to identify and address cyber threats in real time. AI-based systems are more effective at analysing large datasets, identifying trends, and predicting potential attacks with greater efficiency. To improve transparency and interpretability in automated decision systems, the concept of “Explainable artificial intelligence” has been brought into cybersecurity. This is especially critical in cybersecurity contexts because grasping the reasons behind threat detection is fundamental for maintaining trust and accountability (Zhang et al., 2022)

Despite these improvements, AI-driven cybersecurity measures have certain limitations. Model bias, a lack of transparency, and overreliance on automation can reduce their effectiveness, particularly when human understanding is required.

2.4 Cyber risk and data availability challenges

Another important direction of research focuses on challenges related to cyber risk assessment and data availability. The major obstacle in cyber security research is the lack of reliable and comprehensive datasets. This issue arises primarily due to the underreporting of cyber incidents by organisations, often driven by reputational concerns and regulatory implications (Cremer et al. 2022). The evolving nature of cyber risks limits the availability of historical data, making it difficult to develop predictive models and risk assessment frameworks (Biener et al., 2015; Eling et al., 2016).

The paper makes three contributions to the cyber security literature by addressing these questions. First, it provides an extensive Bibliometric and thematic overview of research on cybercrime and user awareness. Second, it identifies underexplored areas, particularly in relation to behavioural cyber security. Third, it presents a theoretical framework for future research integrating technological and human-centric perspectives. The scarcity of reliable data continues to constrain testing. At the last mostly research is heavily focused on developed economics with relatively fewer studies focusing on developing countries. Where digital literacy levels may be lower, and the risk of cyber fraud is high. However, a critical examination reveals that user awareness and behavioural aspects remain underexplored.

2.5 Research Gap

Based on the previous study, we found the following research gaps.

Most studies focus only on technology-related aspects; they ignore human behavior and user awareness.

There are no integrated frameworks that combine all factors, such as behavioral, technological, and police aspects.

Given these gaps, we clearly need a systematic literature review that maps out current research but

also identifies underexplored areas. It provides a foundation for future research.

3. Research methodology

This study conducts a systematic literature review of cybercrime and cybersecurity awareness of internet users from 2017 to 2026. For this study, 620 research articles were collected from the Dimensions database. The following research questions are the focus of the study.

1. What are the key trends in cyber security research publications from 2017 to 2026?
2. What thematic clusters and research streams have emerged in the field of cybercrime and cyber security?
3. What are the dominant areas of focus in highly cited studies?
4. What critical research gaps exist in the current literature?

3.1 Review Design and Approach

This study follows a structured protocol based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. The objective of this study is to provide a comprehensive and unbiased overview of the existing literature on cybercrime and cybersecurity, identify research trends, and highlight knowledge gaps. To achieve this, a PRISMA chart was adopted, which involves clearly defined stages of data identification, screening, eligibility assessment, and inclusion.

3.2 Data Source and Search Strategy

This dataset was collected from the Dimensions database, which provides broad coverage of research papers from 2017 to 2026. This database is chosen because of its open access publications, extensive coverage and free access. The following search terms were used.

- "Cyber security"
- "Cybercrime"
- "Internet users"

These keywords were selected to capture the intersection of technological and user-centric aspects of cyber security. The search was carried out without limiting subject categories to ensure broad coverage of the literature.

3.3 Exclusion and Inclusion Criteria

To ensure relevance and quality, the following exclusion and inclusion criteria were applied to the dataset using Microsoft Excel.

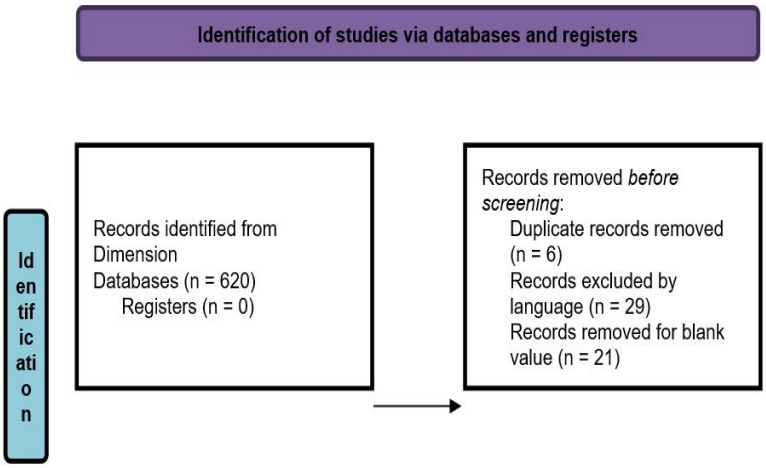
Inclusion Criteria

1. Articles published between 2017 and 2026
2. Open-access research articles
3. Studies related to "Cybercrime, Cybersecurity and Internet users"

Exclusion Criteria

1. Blank values in DOI, title, abstracts, etc.
2. Publications not in English language
3. Articles not directly related to cybersecurity for internet users
4. Duplicate records
5.

3.4 PRISMA-Based Screening Process



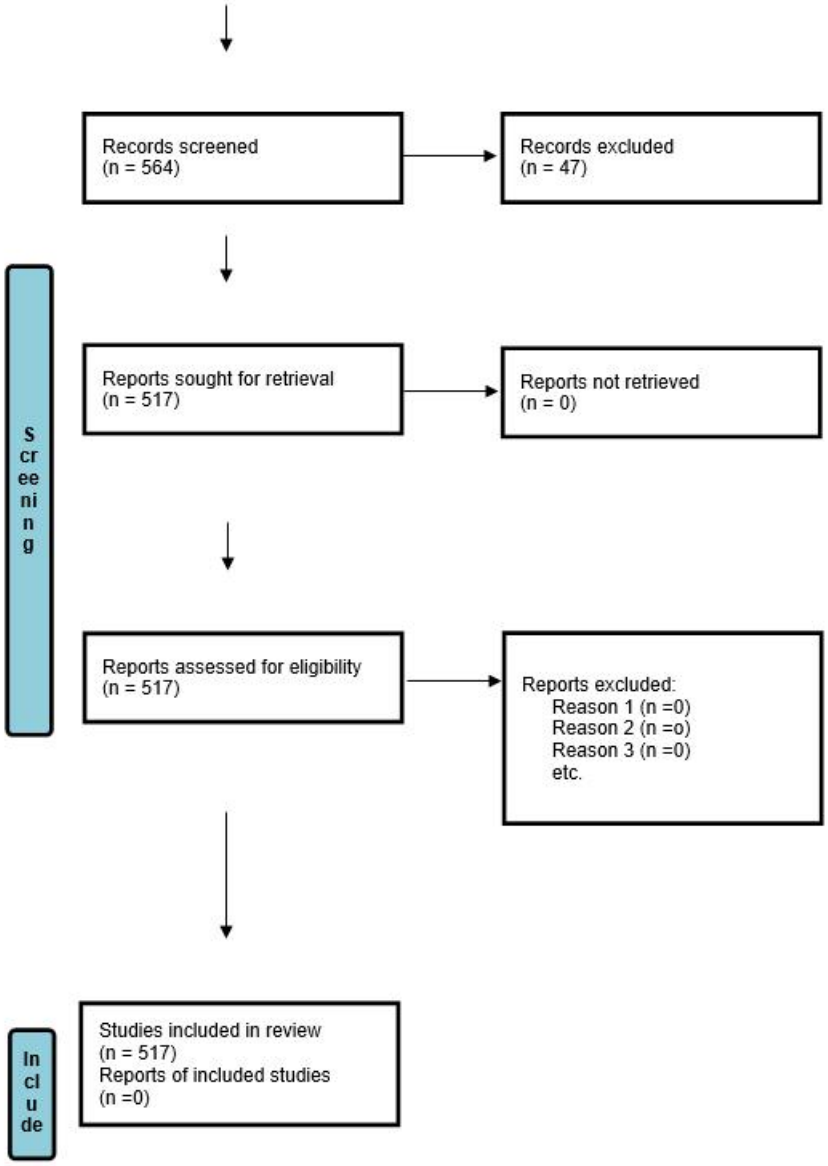


Figure 1 Prisma Diagram

3.5 Data Preparation and Extraction

The selected articles were exported in CSV format from the Dimensions database. The dataset included information such as author names, publication year, article title, abstract, Citation count, etc.

The data were filtered using Microsoft Excel to remove irrelevant data and prepared for analysis.

4. Data Analysis and Interpretation

Descriptive and Bibliometric analyses were used in this study.

Descriptive analysis

Microsoft Excel was used to analyze

- Yearly Publication trend
- Citation analysis
- Country and its publications
- Source of publication and its documents

Bibliometric analysis

VOSviewer software was used to perform Co-occurrence analysis of keywords.

- Network visualization
- Overlay visualization
- Density visualization

VOSviewer is widely used in Bibliometric studies for mapping scientific knowledge and identifying relationships among research variables.

The analysis of the systematic literature review was based on Bibliometric and descriptive analysis of 517research articles.

The analysis is divided into two major parts.

- Descriptive analysis
- Bibliometric analysis by VOSviewer

4.1 Descriptive analysis

The findings reveal four distinct phases of research evolution.

4.1.1 Yearly Publication Trends

Table1. Publication – Year-wise

Publication Year	Number of publication
2017	16
2018	24
2019	16
2020	41
2021	60
2022	80
2023	85
2024	88
2025	74
2026	33

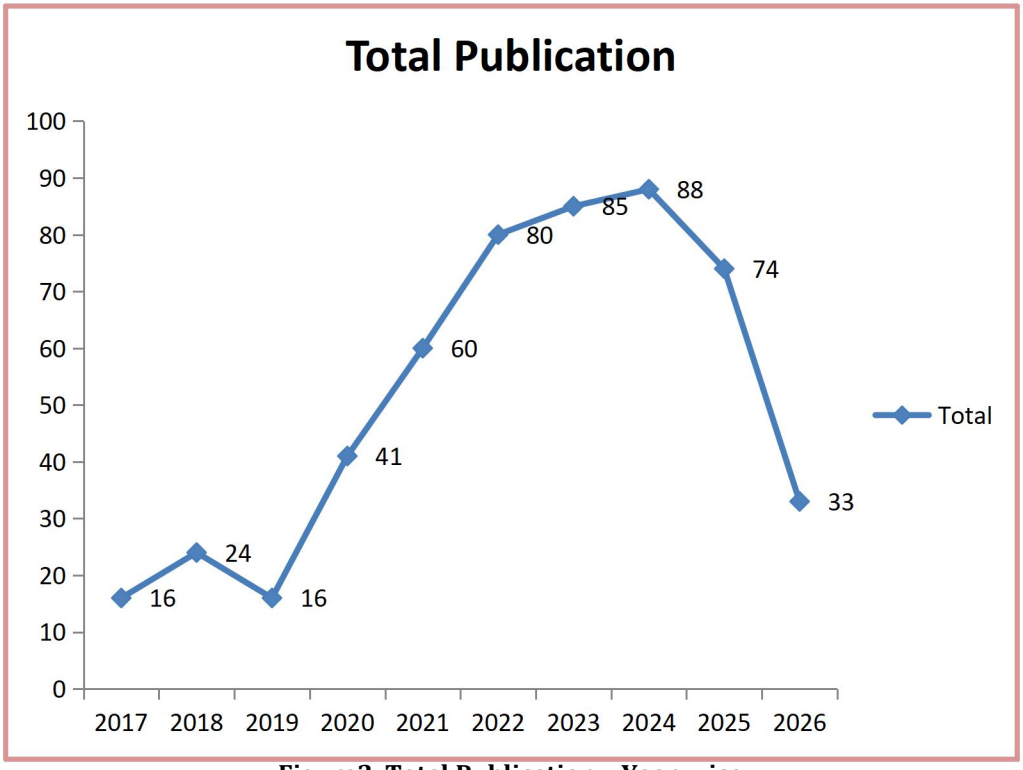


Figure2. Total Publication – Year-wise

1. Initial Phase (2017 to 2019) -Research output remained relatively low and unstable, indicating that cybersecurity awareness was still an emerging area of academic interest.
2. Growth Phase (2020 to 2023) - Publications have increased since 2020 due to increased digitalisation during the COVID-19 pandemic. Digitalisation has led to increased cyber threats, and there has been an increase in work related to cybersecurity and the development of tools to mitigate these threats.
3. Maturity Phase (2024) –The highest number of articles (88) were published in 2024. Indicating that this field receives the most research attention during this period. This reflects its establishment as an important research domain.
4. Decline Phase (2025-2026) - Declines were recorded in 2025 and 2026. The decline in 2026 was not due to reduced researchers' interest.

Overall, this shows a growing trend, confirming that researchers' interest in cybersecurity is increasing day by day.

4.1.2 Citation Analysis

This citation table shows that technology-related studies dominate the research. Most papers are based on machine

learning and artificial intelligence. The paper "A Survey in Machine Learning Techniques for Cyber Security in the Last Decade" (citation-509) is based on machine learning and is highly cited. Phishing and ransomware remain major research topics, which appear to be a growing threat in cybersecurity.

Table2. Citation analysis

Author	Title	Citation
Shaukat et al., 2020	A Survey on Machine Learning Techniques for Cyber Security in the Last Decade	509
Alkhalil et al., 2021	Phishing Attacks: A Recent Comprehensive Study and a New Anatomy	496
Basit et al., 2020	A comprehensive survey of AI-enabled phishing attacks detection techniques	411
Zhang et al., 2022	Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research	405
Cremer et al., 2022	Cyber risk and cybersecurity: a systematic review of data availability	345
Shaukat et al., 2020	Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cyber security	302
Beaman et al., 2021	Ransomware: Recent advances, analysis, challenges and future research directions	260
Alabdan et al., 2020	Phishing Attacks Survey: Types, Vectors, and Technical Approaches	218
Alawida et al., 2022	A deeper look into cyber security issues in the wake of Covid-19: A survey	155
Perwej et al., 2021	A Systematic Literature Review on the Cyber Security	149

4.1.3 Country and its publications

The top 10 countries and their documents are presented in this table. It represents the number of publications by each country and their citation and total link strength. Indonesia published the highest number of papers in cybersecurity field. The articles from Australia were highly cited. This means other researchers used these findings in their studies. Meanwhile, the United States shows the highest total link strength. This indicates that it acts as the main collaborative engine for the study, preferring cross-border joint ventures over single-nation outputs.

Table3. Country and its publication

S. No.	Name of country	Number of document	Citation	Total link strength
1.	Indonesia	78(Highest)	255	18
2.	United States	57	1089	29(Highest)
3.	United kingdom	47	1804	27
4.	India	32	465	13
5.	Australia	31	1824(Highest)	27
6.	Malaysia	26	381	21
7.	Saudi Arabia	22	905	16
8.	China	21	772	8
9.	South Africa	18	321	11
10.	Canada	15	739	12

4.1.4 Source of publication and its document

IEEE is the main journal that published the most papers in the database. The citation count of IEEE Access is 1580, and the link strength of these documents is 516.

Table4. Source of Publication and its document

S. No.	Source	Documents	Citation	Link strength
1.	IEEE access	24	1580	516
2.	Computer & security	15	957	424
3.	Humanities and social science communications	9	133	384
4.	Security journals	8	194	254
5.	Journal of cyber security	7	230	130

4.2 Bibliometric analysis

4.2.1 Network Visualisation (Thematic Clusters)

Network visualisation creates a network of important keywords used in this literature review. This shows which subtopics have been trending in previous studies.

This network visualisation was created with VOSviewer. It provides a comprehensive overview of the intellectual structure of previous research on cybercrime and cybersecurity. Figure 2 shows a co-occurrence analysis based on 517 articles. This visualization reveals a total of 42 interconnected terms grouped into five distinct clusters, reflecting the field's multidimensional nature. The central nodes of this cluster are policy, behaviour, cyber attack, and education; the size of each term represents the link strength and occurrence of each term.

Cluster1. Human behaviour and digital literacy (Red)

This cluster has the highest 11 key terms, such as social media platforms, cybersecurity awareness, cybersecurity education and questionnaires. This cluster is focused on user-centric aspects because most of the terms are related to the human factor. The importance of this cluster shows that scholars are focusing more on individual contribution to mitigate cyber risk. The strong links behaviour and education indicate researcher focused on human factor.

Cluster2. Technology and cyber crime (Green)

This cluster shows 10 items. These terms are related to cybercrime, like phishing, hacker, hacking and some terms are related to technology, like IoT, machine learning, website, algorithm, and computer. It represents the technological aspect of how it helps to detect cybercrime.

Cluster3. Digitalisation and legal framework (Blue)

This cluster shows terms like digital era, digitalisation, ICT and communication technology. They represent an increase in the use of the internet and the growing use of digital things. Some terms include legal framework, law enforcement, personal data protection and law enforcement agency. They indicate that a legal framework is necessary to protect personal data in this digital era because cybercrime is rapidly growing.

Cluster4. Cyber attack and governance (Yellow)

This cluster shows 8 items such as cyber attack, defense, governance, policy, national security and information security. This cluster represents the importance of institutional mechanisms in solving cyber security challenges. The highest link strength of policy and cyber attack terms indicates a better connection between cyber attack study and policy research. The integration of terminology such as national security and governance indicates that cyber security is progressively analysed from a national perspective.

Cluster5. Cyber crime and COVID-19 (Purple)

This cluster is relatively small and includes terms like COVID, cyber criminal, data breach, identification and stakeholder. It reflects the situation-specific escalation in cybercrimes during COVID- 19. When multiplied, online activity generated new vulnerabilities.

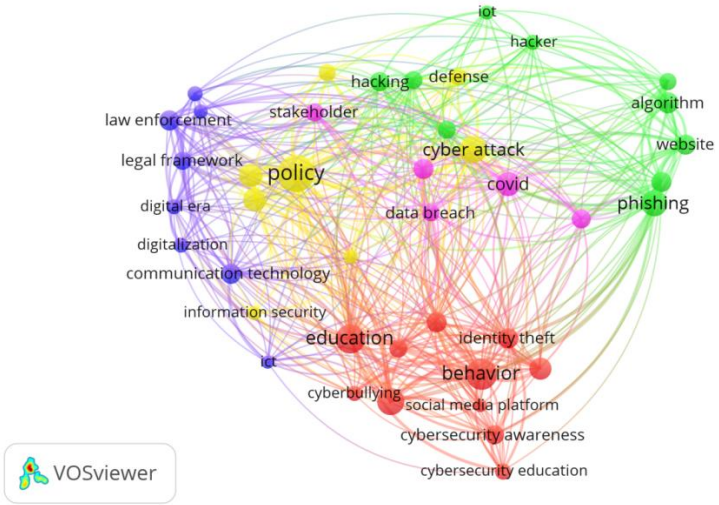


Figure3. Network visualisation based on co-occurrence of terms

4.2.2 Overlay visualisation

The overlay visualisation represents insights into the time-dependent progression of these terms by mapping their occurrence over different time periods. The yellow colour is represent these terms is newer than dark colours term in this map.

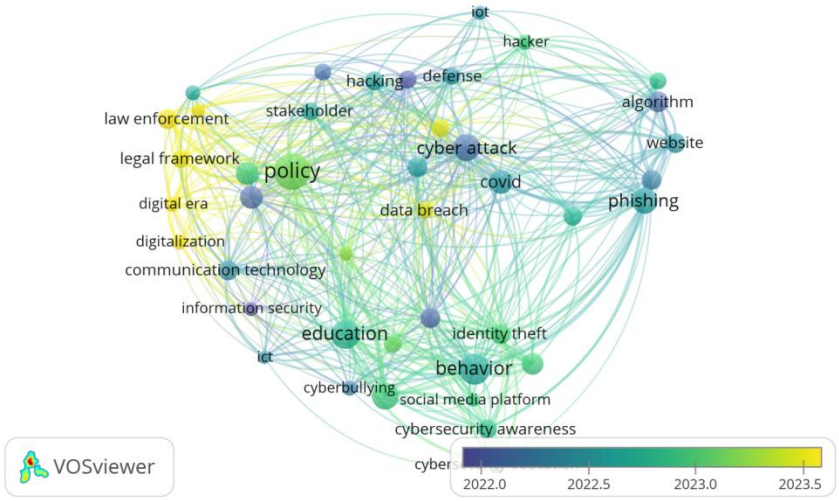


Figure 4. Overlay visualisation based on the co-occurrence of terms

4.2.3 Density Visualisation

The density visualisation (Figure 4) illustrates the frequency and concentration of keywords within the dataset by using colour gradients. Areas with brighter colours represent higher keyword occurrence and consequently, greater research attention, while darker areas indicate less frequently studied topics.

The analysis shows that terms such as cyber-attacks, Policy, phishing and behaviour occupy the most prominent positions in the density map, indicating that these are the core focal points of the literature.

Despite the rapid growth in research, this visualisation reveals significant gaps, while policy, cyber attack and phishing-related aspects have received significant study. Cybersecurity and cyber education fall into less dense regions. This suggests that despite the growing recognition of cybercrime, there remains little research on the human behaviour of cybersecurity.

Currently, some developed areas related to cybersecurity are showing considerable density, such as legal frameworks and information security. These represent a growing but still developing area of research. This finding points to the field gradually expanding into interdisciplinary domains such as governance and education.

From a critical perspective, this density reflects an imbalance in the concentration of visualisation literature. While technical research has dominated, studies of users' digital literacy and cyber awareness have received comparatively less attention. This study points to the need for a more balanced and comprehensive research approach that integrates technical, behavioural and institutional aspects.

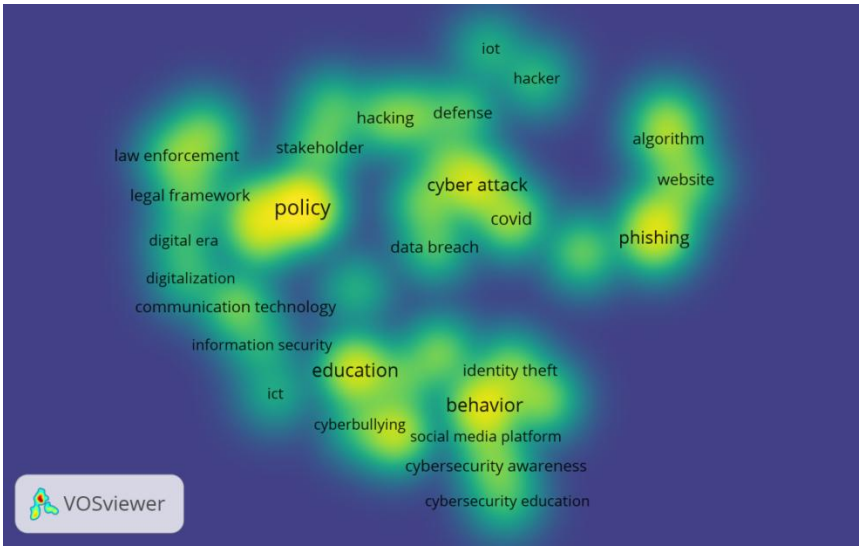


Figure5. Density visualisation based on co-occurrence of terms

5. Result and Discussion

The results of this comprehensive literature review provide valuable insights into how user security awareness and cybercrime are changing.

This research paper presents both the limitations and strengths of existing literature. A positive conclusion is the rapid growth of cybersecurity research, especially after 2020. This growing trend shows that the use of digital technology is increasing day by day and the related increase in cybercrimes. The increase in publications shows that most studies are related to academic and practical interest in addressing cybersecurity challenges. Despite this increase, the findings are limited to technology-oriented research. Highly cited studies are focused on machine learning, AI and automated threat detection systems (Shaukat et al., 2020). Although these technological developments have improved the capability to detect and mitigate cyber threat patterns, they mostly address system-level vulnerabilities rather than human-related risks. While the role of user awareness and behavioural factor increase but it has still developed less the comparision. The network and density visualisation highlight that terms such as cybersecurity and cybersecurity education are present. They are not as strongly linked with other research clusters as technological themes. This supports past studies that indicate human error is still a significant factor in cybersecurity breaches (Alkhalil et al., 2021).

Furthermore, overlay visualisation indicates that researchers' interest is gradually shifting from basic cybercrime concepts to more advanced and interdisciplinary topics. This includes terms such as cyber awareness, cyber education and legal frameworks. Therefore, we can say that the field of cybersecurity is moving toward a more comprehensive and integrated understanding.

The weak connection between clusters related to behavioural technology and policy suggests that research in this field remains fragmented. The lack of reliable and comprehensive data on cyber incidents also remains a significant problem (Cermer et al. 2022).

Underreporting of cybercrime also reduces the availability of data sets needed for empirical analysis. This not only impacts academic research but also hinders the development of effective policy and risk management frameworks.

Overall, these findings highlight a fundamental imbalance in the literature where technological solutions are being extensively studied, while human behaviour and institutional dimensions, which are critical aspects of cybersecurity, are relatively neglected. This imbalance highlights the need for a more holistic and interdisciplinary approach to this aspect of cybersecurity.

6. Recommendation and Implications

6.1 Theoretical Implications

This research paper presents a synthesis of existing cybersecurity literature through a systematic and Bibliometric analysis, thereby contributing to the current body of knowledge. Unlike earlier studies that emphasised technical aspects, this study integrates technical, behavioural, and policy perspectives, offering a more comprehensive understanding of cybersecurity research.

Identifying the distinct thematic groups and their interrelationships in this study helps establish a conceptual foundation for future research. The study emphasises that user awareness should be treated as a key factor in cybersecurity models rather than a secondary aspect.

This opens up new avenues for interdisciplinary research for the researcher, integrating information systems, psychology and sociology.

6.2 Practical Implications

The findings have significant implications for practitioners, organisations and cyber security professionals. Technical literature indicates that organisations often prioritise technical solutions while underestimating the impact of users' cybersecurity behaviour.

A human behaviour-centric approach should be adopted in cybersecurity, as human behaviour currently represents the most vulnerable factor in this field.

They should now invest more in these cybersecurity awareness and training programs and periodically assess their effectiveness.

Given the rising threat of cyber attacks, particularly phishing and social engineering, it has become essential for organisations to adopt a multi-layered security strategy. This strategy should combine technical security measures with users' education in cyber security.

6.3 Policy Prescriptions

Policymakers should focus on implementing a standard reporting framework for cyber incidents. Promoting digital literacy and awareness programs at the national level and encouraging collaboration between government, industry, and academia.

The study highlights limited coordination between policy research and cybersecurity awareness and cybersecurity education. This means the current policies and regulations are not sufficiently addressing the behavioural aspects of cybersecurity. Therefore, a more user-centric policy approach is required.

6.4 Directions for future Research

There are some suggestions for future research in the cybersecurity field.

- Study about the cybersecurity awareness level of digital banking users.
- Study about the cybersecurity challenges in developing countries.
- Develop an integrated model combing these factors behaviour, technology and policy.

- Enhancing the availability and transparency of data related to cybercrime reporting.
- Investigating the importance of AI in behavioural cybersecurity.

References

1. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.https://doi.org/10.3389/fcomp.2021.563060
2. Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., &Kifayat, K. (2020). A comprehensive survey of AI-enabled phishing attack detection techniques. Telecommunication Systems, 76(1), 139–154. https://doi.org/10.1007/s11235-020-00733-2
3. Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. Computers & Security, 111, 102490.https://doi.org/10.1016/j.cose.2021.102490
4. Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance – Issues and Practice, 40(1), 131–158. https://doi.org/10.1057/gpp.2014.19
5. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., &Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance – Issues and Practice, 47, 698–736. https://doi.org/10.1057/s41288-022-00266-6
6. Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 17(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122
7. Li, K., Kim, D. J., Lang, K. R., Kauffman, R. J., &Naldi, M. (2020). How should we understand the digital economy in Asia? A critical assessment and research agenda. Electronic Commerce Research and Applications, 44, 101004.https://doi.org/10.1016/j.elerap.2020.101004
8. Parewa, D. K., & Mordia, D. (2024). Comparative analysis of registered cyber-crimes among Rajasthan and its neighbouring states. International Journal of Scientific Research in Mathematical and Statistical Sciences, 11(6), 17–22.
9. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020a). A survey on machine learning techniques for cybersecurity in the last decade.IEEE Access, 8, 222310–222354.https://doi.org/10.1109/ACCESS.2020.3041951
10. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020b). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13(10), 2509.https://doi.org/10.3390/en13102509
11. Tranfield, D., Denyer, D., & Smart, P. (2003).Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British Journal of Management, 14(3), 207–222. https://doi.org/10.1111/1467-8551.00375
12. Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., &Taher, F. (2022). Explainable artificial intelligence applications in cybersecurity: State-of-the-art in research. IEEE Access, 10, 93104–93139. https://doi.org/10.1109/ACCESS.2022.3204051
13. Mohamed, N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. KnowlInfSyst 67, 6969–7055 (2025). https://doi.org/10.1007/s10115-025-02429-y
14. RatneshKushwaha, Dr.SharadPatil. (2025). AI-Driven Threat Intelligence: A Predictive Analytics Framework for Enhancing Cyber Défense Capabilities. International Journal of Research & Technology, 13(2), 270–284. Retrieved from https://ijrt.org/j/article/view/557
15. Source:Page MJ, et al. BMJ 2021;372:n71. doi: 10.1136/bmj.n71.
16. This work is licensed under CC BY 4.0. To view a copy of this license,
17. Visit https://creativecommons.org/licenses/by/4.0/