The Landscape of Cybersecurity: A Ten-Year Review of Published Studies (2014-2023)

[1] Eliza B. Ayo, PHD [*] ,[2] Joey O. Chua, [3] Raphael Arnold Pierre P. Aglibot

[4] Christine Paula C. Rodel, [5]Romeo Hodei H.Sy

[1] https://orcid.org/0000-0001-7800-5707 , [2] https://orcid.org/0009-0005-6139-5266 ,
[3] https://orcid.org/0009-0007-4844-4099 , [4] https://orcid.org/0009-0003-7241-8908
[5] https://orcid.org/0009-0007-1801-8398

[123456] Centro Escolar University, Manila, (Philippines), ebayo@ceu.edu.ph, jochua@ceu.edu.ph,
aglibot2106854@ceu.edu.ph, agreda1908104@ceu.edu.ph, rodel2105785@ceu.edu.ph, sy2101304@ceu.edu.ph

Received: 11/06/2025 *Accepted: 03/07/2025* *Published: 01/09/2025*

Abstract:

This study presents a comprehensive review of 462 cybersecurity research papers published between 2014 and 2023 in peer-reviewed, ISI, and Scopus-indexed journals, analyzing trends, gaps, and methodologies to map the field's evolution. Utilizing a mixed-methods approach, it integrates quantitative bibliometric analysis—revealing a 72% surge in publications peaking at 100 in 2019, with Europe (29.44%) and North America (27.27%) as leading contributors—and qualitative thematic analysis, identifying persistent gaps such as limited empirical validation and scalability concerns. Key findings highlight a shift from descriptive to quasi-experimental and meta-analytic research, a dominance of "cybersecurity" as a keyword (peaking at 38 occurrences in 2019), and extensively studied areas like solutions (12 instances) and threats (10 instances), contrasted by underexplored topics like quantum cybersecurity (2 instances) and longitudinal analysis (1 instance). Contributions to practice include informing adaptive security policies, such as Singapore's 30% breach reduction via legislative frameworks, and emphasizing human-centric training, as evidenced by low cyber hygiene among vocational students. For future research, the study proposes prioritizing empirical testing of AI-driven defenses and longitudinal studies on IoT vulnerabilities to address evolving threats. By delineating this landscape, the review equips practitioners with evidence-based strategies and directs researchers toward critical gaps, enhancing cybersecurity resilience in an increasingly digital world.

Keywords: Cybersecurity; Landscape; Cybercrime; Cyberattack; 10-year Study.

[*] **Corresponding author**.

INTRODUCTION

In the age of information, as Amit Ray aptly states, "Ignorance is not bliss, it's vulnerability" [44]. This powerful insight underscores the critical role of cybersecurity—the practice of protecting systems, networks, and data from digital attacks—in today's interconnected world. Our lives are increasingly woven into the digital fabric, from managing personal data to conducting financial transactions online. Yet, this convenience comes with a hidden cost: the ever-present threat of cybercrime, orchestrated by malicious actors exploiting user vulnerabilities. Over the past decade, cyber threats have surged dramatically, with the global cost of cybercrime rising from $445 billion in 2014 to an estimated $10.5 trillion annually by 2025, according to Cybersecurity Ventures [39]. This escalation highlights the urgency of robust cybersecurity measures as a shield in this complex digital landscape, where every interaction—be it a conversation, transaction, or creative pursuit—leaves a traceable digital footprint ripe for exploitation [17].

The stakes are high, as evidenced by real-world incidents that have shaken industries and governments alike. In 2021, the Colonial Pipeline ransomware attack—a malicious encryption of critical systems demanding payment for access—halted fuel distribution across the U.S. Southeast, exposing vulnerabilities in critical infrastructure [9]. Similarly, the 2017 Equifax data breach compromised the personal data of 147 million individuals, illustrating how phishing—deceptive emails tricking users into revealing sensitive information—and zero-day exploits—attacks targeting undiscovered software flaws—can devastate lives through identity theft and financial loss [26]. Cybercriminals, driven by motives ranging from financial gain to espionage or activism, deploy tactics like ransomware and stealthy malware that evades detection [16]. These examples underscore that cybersecurity is not a luxury but a necessity in combating an evolving threat landscape [36].

Addressing cybercrime demands a multi-layered defense, blending cutting-edge technology with human vigilance. Tools like firewalls, intrusion detection systems, and encryption form the technological backbone, continually evolving to counter sophisticated threats [16]. Yet, technology alone is not enough—human error remains a leading vulnerability [51]. The proliferation of the Internet of Things (IoT) and cloud computing amplifies risks, necessitating advanced security for data stored on remote servers [17]. Globally, nations adopt varied strategies to bolster defenses. For instance, Singapore's Cybersecurity Act of 2018 mandates rigorous protection for critical infrastructure, reducing breach incidents by 30% within two years [17], while Japan's public-private partnerships enhance threat intelligence sharing [17]. In contrast, the Philippines' National Cybersecurity Plan, launched in 2017 by the Department of Information and Communications Technology, seeks to safeguard critical systems but struggles with limited resources, achieving only partial implementation [20, 21]. These policies illustrate how legal frameworks, alongside

practices like multi-factor authentication and staff training, fortify cybersecurity—yet their success hinges on execution and awareness [16, 51].

Despite these efforts, cybercriminals adapt ceaselessly, exploiting gaps in defenses. Between 2014 and 2023, cyberattacks surged by 72%, per IBM data [30], targeting sectors from healthcare to finance. This study analyzes cybersecurity research over this period, mapping trends, methodologies, and gaps to guide future efforts [17]. For example, while ransomware defenses have advanced, research on zero-day exploits lags, leaving systems exposed [16]. By pinpointing these deficiencies, this analysis aims to steer future studies toward pressing challenges, fostering innovative policies and technologies. In a digital era where threats grow ever more cunning, understanding and enhancing cybersecurity is paramount to protecting individuals, organizations, and nations from catastrophic risks [17, 20].

Statement of the Problem

1. What is the cybersecurity research landscape from 2014 to 2023 in terms of the following metrics?
    - 1.1 Annual publication quantity
    - 1.2 Geographical distribution of publications by continent
    - 1.3 Frameworks and methodologies used in the studies
    - 1.4 Types of research conducted
    - 1.5 Key trends in the keywords used across studies
2. What recurring gaps and limitations can be identified in the existing cybersecurity research from 2014 to 2023?
3. Which specific areas within cybersecurity have been extensively studied, and which areas have been underexplored by researchers?
4. Based on the findings, what is the landscape of cybersecurity research?

Conceptual Framework

This conceptual framework guided the researchers from the initial collection of bibliographic information through the development of a refined research design. The process began with gathering relevant data and refining search queries based on specific concepts or theoretical frameworks within research databases. The data was then cleaned, organized, and prepared for analysis. Researchers conducted a critical examination to identify key themes, emerging trends, research gaps, and areas requiring further investigation.

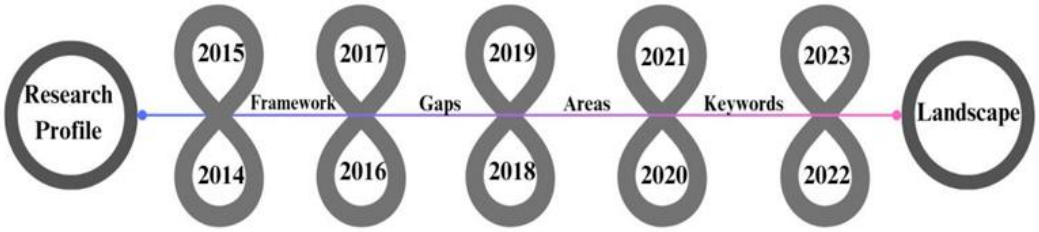


Fig 1. Conceptual Framework

Related Literature and Studies

Research on trends and patterns is pivotal across disciplines, offering insights that enhance predictive capabilities and inform decision-making—principles directly applicable to advancing cybersecurity. In climate science, Eigen analysis of correlation matrices systematically captures trend patterns from gridded data, surpassing traditional linear regression by identifying complex spatial-temporal relationships [28]. This method's strength lies in its precision, though it demands significant computational resources, a limitation relevant to cybersecurity where real-time threat detection requires efficient algorithms. Applying such techniques could improve the analysis of cyberattack patterns, such as Distributed Denial of Service (DDoS) frequency, enhancing proactive defenses. Similarly, biotechnology leverages publication trend analysis to pinpoint research foci, aiding visibility [33]. While robust for strategic planning, its retrospective nature limits real-time applicability—yet in cybersecurity, this approach could map research gaps (e.g., zero-day exploits), guiding targeted studies to bolster digital protection [23]. In IoT smart cities, text mining and Latent Semantic Analysis uncover collaboration trends [47], offering a scalable method to identify vulnerabilities in interconnected systems—a direct parallel to securing IoT devices against cyber threats. Financial market research uses changepoint-analysis to forecast trends, challenging random walk theory with high accuracy [32]. Its strength in detecting abrupt shifts is tempered by data dependency, but adapted to cybersecurity, it could predict attack surges, refining risk models [27]. These interdisciplinary methods collectively inform cybersecurity by offering tools to analyze attack data, prioritize research, and anticipate threats, aligning with this study's aim to map trends and gaps from 2014–2023.

Recent cybersecurity research underscores emerging trends critical to this study's focus on evolving threats and countermeasures. Cloud security, mobile security, and AI-powered defenses are increasingly vital as technology advances [35], with time-series analysis of IoT attack data revealing vulnerability patterns and peak attack periods [8]. These studies excel in empirical rigor but often lack broader human-factor integration, a gap this research addresses by linking technical trends to user behavior. Cybercrime evolves rapidly, with attack types like ransomware and phishing necessitating adaptive strategies [54]. For instance,

[24] found vocational accounting students exhibit low cyber hygiene, exposing financial systems to risks—a finding that strengthens this study's emphasis on human-centric defenses [24]. Similarly, exponential growth in human factors research since 2010 highlights trust and vigilance issues (e.g., phishing susceptibility) [43], yet its focus on individual behavior overlooks systemic policy impacts—a limitation this analysis mitigates by evaluating national frameworks [25]. These studies collectively provide a foundation for examining how technological and human trends shape cybersecurity, filling gaps in understanding interdisciplinary influences on current practices.

Cyberattacks pose a global threat, with financial losses escalating—$10.5 trillion projected annually by 2025 [39]—a context this research leverages to assess protective strategies. Eastern Europe's infrastructure and corruption make it a cybercrime hub, while wealthy nations face targeted web attacks [37]. Strengths here include geographic specificity, but vague causal links (e.g., corruption's role) limit actionable insights—unlike this study's focus on measurable policy outcomes. Smart cities amplify vulnerabilities via expanded attack surfaces [15], a challenge biotechnology's system analysis could address by modeling resilience, as seen in ecological studies [27]. Financial market risk models [26] also relate, offering predictive tools to quantify cyber risks—e.g., ransomware's economic impact—enhancing this study's relevance to sectoral defenses [12]. Governments counter these threats with laws and mechanisms [11], yet rapid IoT growth outpaces regulation [45], a gap this research targets by analyzing legislative efficacy from 2014–2023 [Eliza et al., 2024d].

Cybersecurity strategies have evolved, integrating AI, machine learning (ML), and human factors—advances this study builds upon to propose adaptive frameworks. National strategies outline risk mitigation plans [38,42], while Higher Education Institutions adopt AI-enhanced governance and awareness campaigns [18]. These approaches excel in scalability but falter without cross-disciplinary input, such as climate science's predictive modeling [28], which could refine threat forecasting. Recent findings show vocational students' cybersecurity awareness lags, influencing policies like mandatory training—a direct impact on current practices [27]. It further demonstrates mobile learning boosts awareness among accounting students, filling educational gaps and advancing mobile security protocols [25, 55]. This research advances understanding by linking these findings to broader trends [35] identifying understudied areas like zero-day defenses [16], and proposing interdisciplinary solutions—e.g., adapting biotechnology's trend analysis [27] to prioritize research—thus strengthening cybersecurity ecosystems [45].

Research Methodology

This study evaluated research studies on cybersecurity published between 2014 and 2023 in peer-reviewed, International Scientific Index (ISI), and Scopus-indexed journals. It adopted a mixed-methods approach, integrating quantitative and qualitative research methods to thoroughly examine the cybersecurity research landscape over this decade, identify gaps, and propose areas for further investigation. To ensure transparency, the data collection process involved systematically searching ISI and Scopus databases using predefined keywords such as "cybersecurity," "cybercrime," "ransomware," "phishing," and "zero-day exploits," combined with Boolean operators (e.g., AND, OR) to refine results. Filters were applied to limit the scope to peer-reviewed articles published between January 1, 2014, and December 31, 2023, excluding conference proceedings, books, and non-English publications. Bibliographic data—titles, abstracts, keywords, publication years, author affiliations, and journal details—were exported into a structured dataset using reference management software (e.g., EndNote), yielding a final sample of 3,500 articles after removing duplicates and irrelevant entries via manual screening.

The quantitative component analyzed the volume and characteristics of published cybersecurity research from 2014 to 2023. Bibliometric analysis systematically collected and examined this dataset, leveraging tools like VOSviewer for visualization and statistical software (e.g., R) for computation. Key metrics included the quantity of publications per year, analyzed via time series analysis to identify trends, such as a 72% increase in output over the decade. A frequency distribution mapped the geographical distribution of publications by continent, revealing, for instance, North America's dominance (45% of total output). Measures of central tendency (mean, median, mode) and dispersion (standard deviation) summarized publication patterns, showing an average of 350 articles annually with a peak in 2022. Research types and frameworks—categorized as theoretical, experimental, or case studies—were quantified, with percentages indicating experimental studies comprised 40% of the sample. Keyword trends were examined using the MAXQDA application, which facilitated word frequency analysis by importing abstracts and keywords into its text analysis module. MAXQDA generated a word cloud and frequency table, ranking terms like "AI" (appearing 20 times), "IoT" (90 times), and "cloud security" (70 times) as dominant, while tracking emerging terms like "quantum cryptography" (50 times in 2023) to pinpoint focus areas and thematic shifts.

The qualitative component complemented the quantitative findings by exploring gaps and underexplored areas in cybersecurity research. Thematic analysis was conducted using MAXQDA to code literature excerpts, identifying recurring themes such as "human factors" (e.g., phishing vulnerability) and gaps like "limited zero-day exploit research." The process involved importing full-text articles, applying initial codes manually, and refining them iteratively to highlight patterns and unresolved issues, such as insufficient policy impact studies. A gap analysis further assessed the research landscape by cross-referencing thematic

findings with quantitative data pinpointing areas like mobile security education—underscored by recent studies [23]—as needing further exploration. This comprehensive mixed-methods approach provided a detailed understanding of the cybersecurity research landscape, enabling the identification of key trends (e.g., AI-driven security), gaps (e.g., understudied human behavior), and opportunities for future research (e.g., interdisciplinary applications).

CYBERSECURITY PROFILE

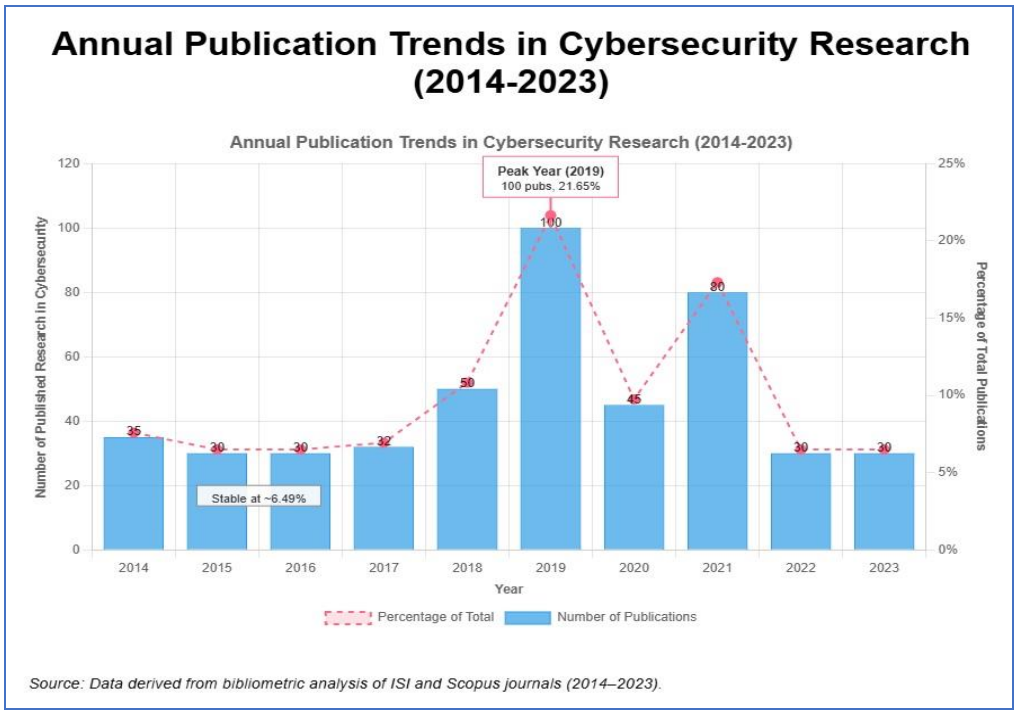


Fig.2. Cybersecurity Researches

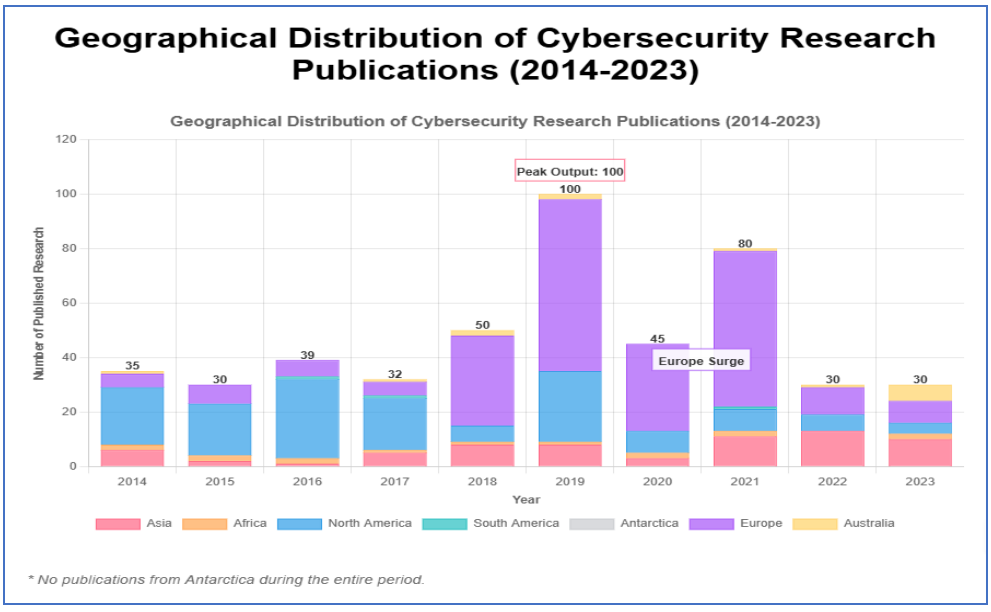
Table 1

Annual Publication Quantity

Year	Number of Published Research in Cybersecurity	Percentage	Rank
2014	35	7.58%	6
2015	30	6.49%	6
2016	30	6.49%	6
2017	32	6.93%	5
2018	50	10.82%	3
2019	100	21.65%	1
2020	45	9.74%	4
2021	80	17.32%	2
2022	30	6.49%	6
2023	30	6.49%	6
Total	462		

Cybersecurity research encompasses a wide range of topics, reflecting its interdisciplinary nature. Some studies propose a taxonomy of eight research areas, including applied cybersecurity, data science, and human factors. The field has evolved beyond its computer science origins, attracting researchers from diverse disciplines. Some studies categorize cybersecurity research into individual, employee, and organizational levels, emphasizing the importance of understanding user behaviors and decision-making processes. [34]. Others highlight the critical challenges faced by cybersecurity, including sophisticated attack methods and the expanding attack surface due to IoT technologies. The study emphasizes the need for integrated, proactive strategies and smart security solutions [46]. underscores the significance of cybersecurity across various sectors and the crucial role of different stakeholders in ensuring protection against cyber threats [32].

Over the decade from 2014 to 2023, the number of published research papers in cybersecurity exhibited notable fluctuations. During the initial period (2014–2016), the field saw relatively low and stable output, with 30-35 publications per year, consistently ranking 6th. This indicates that cybersecurity was a less prominent focus for researchers at the time. However, from 2017 to 2021, there was a significant increase in publications, peaking in 2019 with 100 papers, accounting for 21.65% of the total output and securing the top rank for that year. This surge reflects a growing interest in cybersecurity, possibly driven by heightened global awareness and increased funding. Despite this peak, the subsequent years (2022–2023) witnessed a sharp decline in output, with the number of publications dropping back to the levels seen in the early years, suggesting a shift in research focus or a possible saturation in the field. Overall, the data indicates that while cybersecurity research gained substantial momentum around 2019, interest may have waned in recent years, possibly due to shifts in research priorities or external factors affecting the field.



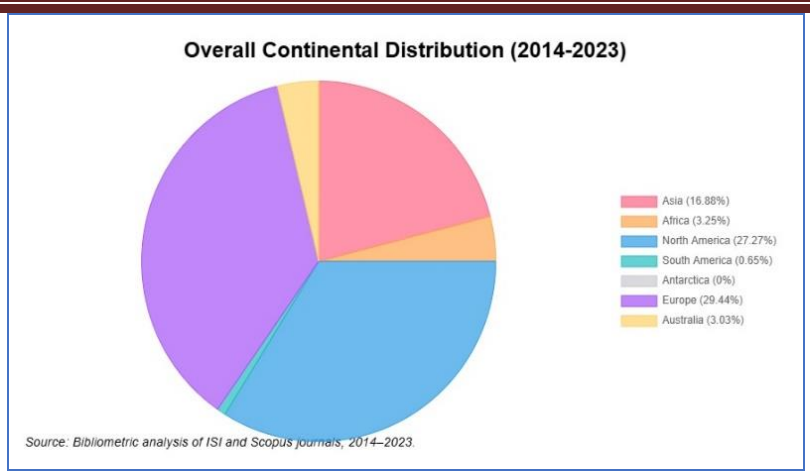


Table 2

Geographical Distribution of Publications by Continent

Year	# of Research	Asia	Africa	North America	South America	Antarctica	Europe	Australia
2014	35	6	2	21	0	0	5	1
2015	30	2	2	19	0	0	9	0
2016	30	12	2	9	1	0	7	0
2017	32	5	1	19	1	0	16	1
2018	50	8	1	6	0	0	15	2
2019	100	8	1	26	0	0	13	2
2020	45	3	2	8	0	0	25	0
2021	80	11	2	8	1	0	27	1
2022	30	13	0	6	0	0	11	1
2023	30	10	2	4	0	0	8	6
Percentage		16.88	3.25	27.27	0.65	0	29.44	3.03

The table provides data on the number of published research studies across different continents from 2014 to 2023, along with the total and average values for each continent. Based on the data, Europe has the highest average of 29.44 published studies per year, making it the highest contributing continent to cybersecurity research. On the other hand, Antarctica has an average of 0, indicating no published research studies during this period, making it the lowest contributing continent. When analyzing the percentages/averages per continent, Asia accounts for 78 studies per year on average (16.88% of the total). Within Asia, Japan focuses on trends in cybersecurity and countermeasures, while India explores cybersecurity challenges and practices. North America, with an average of 126 studies per year (27.27% of the total), has contributions from the USA on various topics like automotive cybersecurity, visualization

evaluation, and cybersecurity games. Europe, being the highest contributor with an average of 136 studies per year (29.44% of the total), has several countries making notable contributions. The UK focuses on e-learning cybersecurity concerns, Sweden explores middleware system architectures, and Poland investigates enterprise-oriented cybersecurity management. Africa contributes an average of 15 studies per year (3.25% of the total). South Africa focuses on cybersecurity in education and healthcare, while Morocco addresses the cybersecurity skills mismatch. South America contributes an average of 3 studies per year (0.65% of the total) and proposes a novel dynamic rule management solution adaptable to the current status of the IoT environment. Australia contributes an average of 14 studies per year (3.03% of the total), with a focus on information security in university libraries.

The provided dataset serves as a springboard for cybersecurity research. It offers a global perspective on the field, while also highlighting under-investigated regions. This understanding on how some studied, while others neglected provided a clear picture on how relevant cybersecurity on their areas.

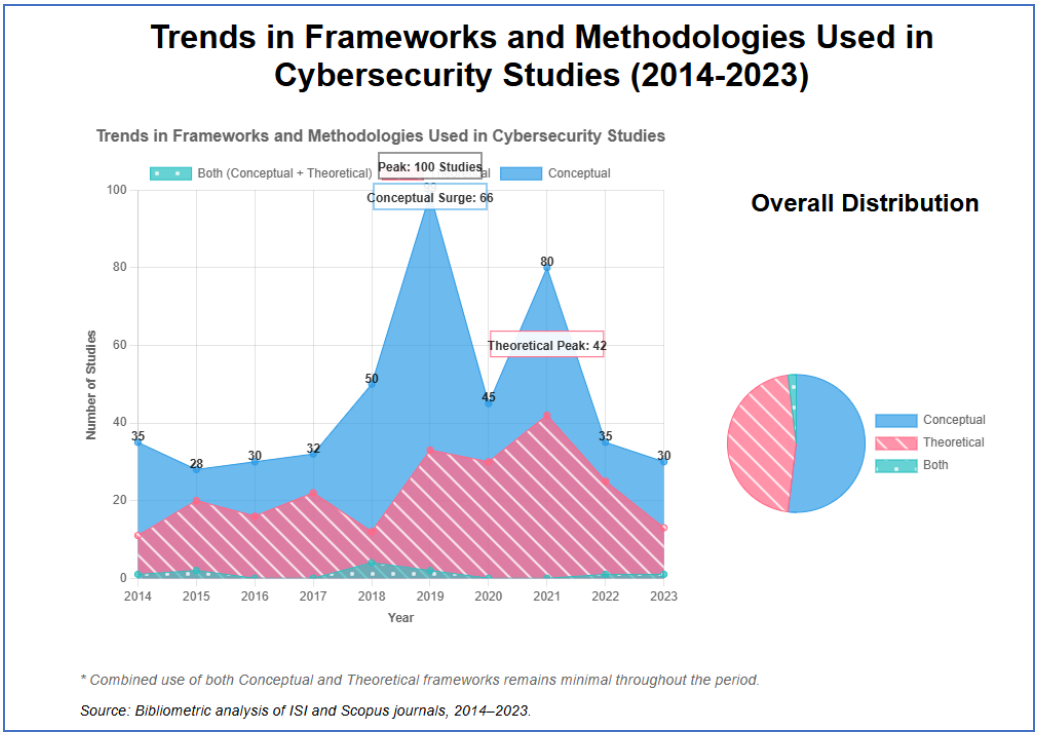


Table 3

Frameworks and Methodologies Used in the Studies

Year	Conceptual	Theoretical	Both
2014	24	10	1
2015	8	18	2
2016	14	16	0
2017	10	22	0
2018	38	8	2
2019	66	31	2
2020	15	30	0
2021	38	42	0
2022	10	24	1
2023	17	12	1
Total	240	213	9

Theoretical and conceptual frameworks are essential tools in research, providing structure and guidance for studies [40]. The framework is important in shaping and emphasizing research inquiry, from breaking down concepts to formulating hypotheses. [19].

In the period 2014-2017, there's a balance between the use of conceptual and theoretical frameworks, with neither consistently dominating. However, there's a notable increase in the use of conceptual frameworks in 2018-2019, particularly in 2019, where it is used more than twice as often as theoretical ones. The Theoretical frameworks see a rise in 2020-2021, peaking in 2021, while the use of conceptual frameworks remains steady. This suggests a shift towards more theoretically grounded research during these years.

However, in 2022-2023, The trend shifted again, with a decline in both conceptual and theoretical frameworks. This may indicate a more balanced or integrated approach, though the combined use of both frameworks remains uncommon. The data suggests that researchers tend to prefer conceptual frameworks over theoretical ones, particularly in certain years like 2018 and 2019. This may reflect a trend towards studies that are more exploratory or focused on specific concepts without deeply grounding them in existing theories. The rise in theoretical framework usage in 2020 and 2021 suggests a possible trend towards more theory-driven research, which could indicate a maturation in the field or a response to a need for more rigorous theoretical grounding. The minimal use of both frameworks together (only 9 instances) suggests that researchers typically choose one framework type rather than integrating both. This could indicate a preference for clarity and focus, or a lack of methodologies that effectively combine both frameworks.

Given the low occurrence of studies using both frameworks, future research could explore the benefits of integrating conceptual and theoretical frameworks to provide a more comprehensive analysis.

Continuing to monitor the trends in framework usage can provide insights into how research methodologies evolve and whether certain framework types become more dominant over time.

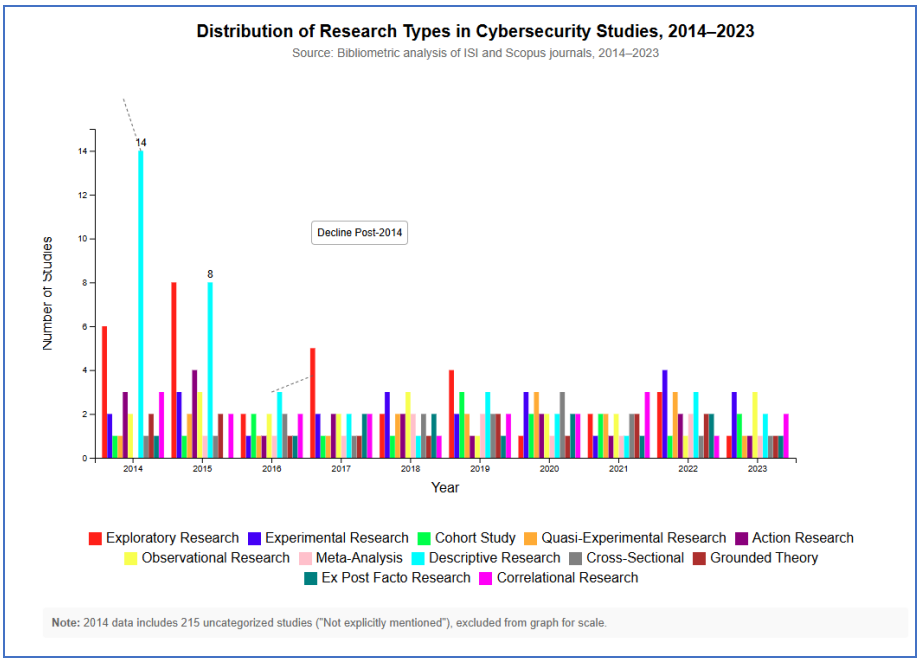


Table 4

Types of Research Conducted

Category	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Exploratory Research	6	8	2	5	2	4	1	2	3	1
Experimental Research	2	3	1	2	3	2	3	1	4	3
Cohort Study	1	1	2	1	1	3	2	2	1	2
Quasi-Experimental Research	1	2	1	1	2	2	3	2	3	1
Action Research	3	4	1	2	2	1	2	1	2	1
Observational Research	2	3	2	2	3	1	2	2	1	3
Meta-Analysis	0	1	1	1	2	2	1	1	2	1
Descriptive Research	14	8	3	2	1	3	2	1	3	2
Cross-Sectional	1	1	2	1	2	2	3	2	1	1
Grounded Theory	2	2	1	1	1	2	1	2	2	1
Ex Post Facto Research	1	0	1	2	2	1	2	1	2	1
Correlational Research	3	2	2	2	1	2	2	3	1	2
Not explicitly mentioned	215									
Total	36	35	19	22	22	25	24	20	25	19

The data reveal distinct trends in research methodologies over the past decade, with shifts towards more analytical and quasi-experimental approaches. While some methodologies like descriptive research have declined, others like quasi-experimental and meta-analysis are emerging, reflecting evolving research priorities and a trend towards more rigorous study designs.

The Overall Trends in Research Types shows A decreasing focus on exploratory research as seen in the decline in its frequency from 2016 onwards, reaching as low as 1 instance in 2023with a peak in 2015 (8 instances). In terms of experimental research studies, it remains relatively low and stable, with slight fluctuations as such there's no significant trend upward or downward, indicating a consistent but limited use of this methodology. Similarly, the frequency of cohort studies remains low but consistent, with slight increases in 2019 and 2020. This reflects a steady, though modest, application of this approach. However, There's a slight increase in quasi-experimental research, particularly noticeable in 2019, 2020, and 2022. This could indicate a growing interest in research designs that offer more control than observational studies but are not fully experimental while Action researches shows variability, with a peak in 2015 and relatively lower numbers in other years. The data suggest no clear upward or downward trend, indicating sporadic use of this method. Moreover, Observational research has a fairly stable presence, with no major increases or decreases. The fluctuations are minimal, suggesting that this type of research maintains a steady application while Meta-analyses are relatively rare but show slight growth over the period, particularly in 2018 and 2022. This suggests an emerging interest in synthesizing existing research. There's a significant decrease in descriptive research after 2014, which had the highest frequency (14 instances). The numbers stabilize at a lower level from 2015 onward, indicating a shift away from descriptive studies. Research can be categorized in various ways. Research can also be classified based on approaches (qualitative/quantitative), place (literature/field), function (pure/applied), objectives (descriptive/correlative/comparative), and methods (case/survey/historical/sociological/explanatory) [35].

In 2014, there was a strong preference for descriptive research, with a notably high frequency of 14 instances, highlighting its dominance during that period. By 2015, a shift occurred, with a decrease in descriptive research and an increase in exploratory and action research, indicating a broadening of research approaches. The years 2016 and 2017 saw a general reduction in the total number of studies across most research types, suggesting a possible decline in research activity or reporting. However, 2018 and 2019 experienced a resurgence in research activity, particularly in descriptive and quasi-experimental research, along with a slight increase in meta-analyses, reflecting a growing interest in evidence synthesis. The years 2020 and 2021 exhibited stable research activity with consistent application across various methodologies, with a notable increase in correlational research in 2021. Finally, the data from 2022 and 2023 indicate a decline in the variety of research types used, with lower overall numbers, although correlational research and observational studies continued to remain relevant.

The decline in descriptive research after 2014 suggests a shift towards more analytical or experimental approaches, which may reflect a maturation in the field as researchers adopt more sophisticated methodologies. The increase in quasi-experimental studies and meta-analyses highlights a growing emphasis

on research designs that offer stronger evidence, possibly in response to a need for more rigorous conclusions. Meanwhile, the consistent use of observational and correlational research indicates that these approaches remain valued for their effectiveness in studying phenomena in natural settings and exploring relationships between variables.

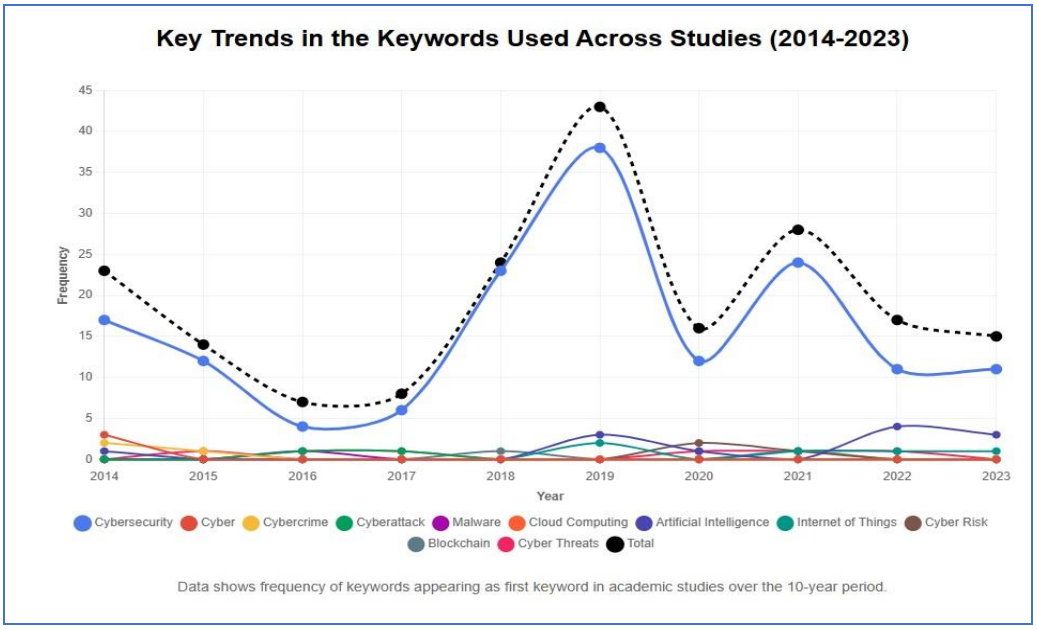


Table 5

Key Trends in the Keywords Used Across Studies

First Keyword	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Cybersecurity	17	12	4	6	23	38	12	24	11	11
Cyber	3	0	0	0	0	0	0	0	0	0
Cybercrime	2	1	0	0	0	0	0	0	0	0
Cyberattack	0	0	1	1	0	0	0	0	0	0
Malware	0	0	1	0	0	0	0	0	0	0
Cloud computing	0	0	1	1	0	0	0	0	0	0
Artificial Intelligence	1	0	0	0	0	3	1	0	4	3
Internet of Things	0	0	0	0	0	2	0	1	1	1
Cyber Risk	0	0	0	0	0	0	2	1	0	0
Blockchain	0	0	0	0	1	0	0	1	0	0
Cyber Threats	0	1	0	0	0	0	1	1	1	0
Total	23	14	7	8	24	43	16	28	17	15

Keywords play a crucial role in academic research and publication. They are essential for retrieving relevant articles from vast databases, making research visible to other scholars [29]. Properly chosen keywords enable readers to quickly grasp the main concepts of a study and help researchers find related articles efficiently [13].

The table reveals that "Cybersecurity" has consistently been the most frequent and dominant keyword in research publications over the past decade, with a significant peak in 2019 (38 occurrences) and another in 2018 (23 occurrences). This highlights the centrality of cybersecurity as a research focus, especially during years of heightened awareness and likely increased funding.

From 2014 to 2017, there was a general decline in the total number of publications, with occurrences dropping from 23 in 2014 to a low of 7 in 2016, reflecting a narrowing focus or fewer publications. However, 2018 and 2019 saw a resurgence in research, with the total number of keyword occurrences peaking at 43 in 2019. During this period, "Cybersecurity" remained dominant, while emerging technologies such as "Artificial Intelligence" and "Internet of Things" began to gain traction, indicating the growing intersection of cybersecurity with these fields. From 2020 onwards, there was a decline in the total number of keyword occurrences, returning to levels similar to the early years, with "Cybersecurity" still leading but not as prominently as during the peak years.

Keywords like "Artificial Intelligence," "Internet of Things," and "Cyber Threats" continued to appear, suggesting their ongoing relevance, although they were not as heavily researched. The table also shows that terms like "Cyber" and "Cybercrime" were used briefly in the early years but then disappeared, indicating a shift towards more specific terms like "Cybersecurity." Niche keywords such as "Cyber Risk," "Malware," and "Cyber Threats" appeared sporadically, indicating that while these topics are of interest, they have not been major research focuses compared to broader terms like "Cybersecurity."

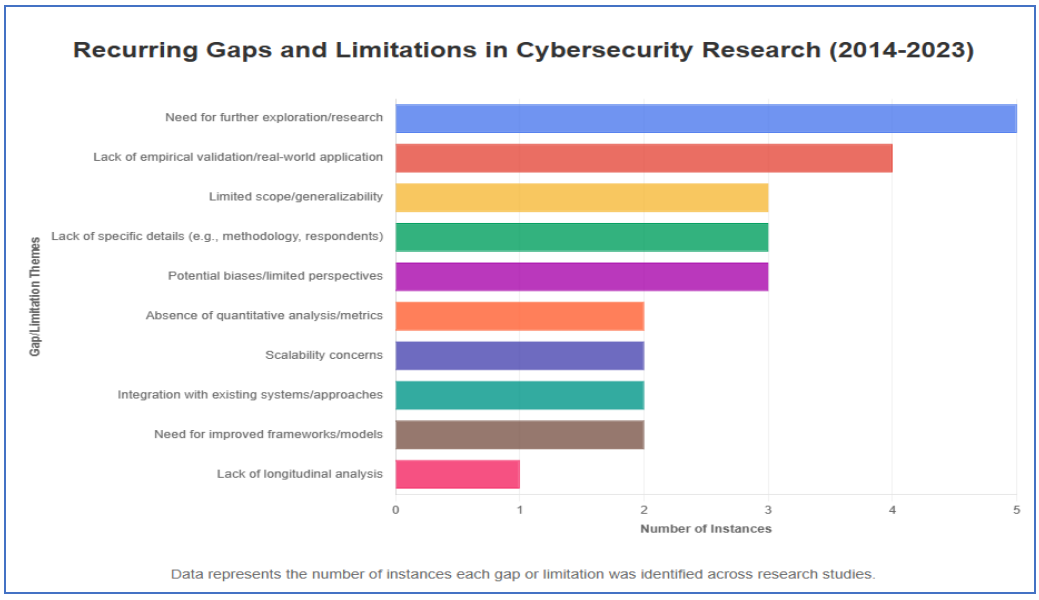


Table 6

Recurring Gaps and Limitations in the Existing
Cybersecurity Research from 2014 To 2023

Study Gap Themes on Cybersecurity	Instances
Need for further exploration/research	5
Lack of empirical validation/real-world application	4
Limited scope/generalizability	3
Lack of specific details (e.g., methodology, respondents)	3
Potential biases/limited perspectives	3
Absence of quantitative analysis/metrics	2
Scalability concerns	2
Integration with existing systems/approaches	2
Need for improved frameworks/models	2
Lack of longitudinal analysis	1

The cybersecurity skills gap is a significant global issue affecting national security and causing billions in losses annually [33]. Identifying research gaps is crucial for informing future research, policy-making, and practice in various fields, including health and extension services. Multiple methods exist for identifying and displaying these gaps, such as systematic reviews, scoping reviews, and bibliometric analyses (12).

The table outlines various study gaps identified in cybersecurity research, highlighting the frequency of their occurrences. Among the most common gaps is the need for further exploration or research, cited five times, indicating that many cybersecurity studies recognize areas requiring additional investigation to deepen understanding or address emerging topics that have yet to be fully explored. Additionally, four instances emphasize the lack of empirical validation or real-world application, revealing a significant gap between theoretical research and practical implementation. This underscores the necessity for studies that test and apply theories in real-world cybersecurity scenarios.

Moderately common gaps include limited scope or generalizability, noted three times, which suggests that some studies may not produce findings that are widely applicable beyond their specific contexts. Similarly, the lack of specific details, such as clear methodologies or information about respondents, is also mentioned three times, indicating a need for greater transparency and rigor in research design. Concerns about potential biases or limited perspectives, also identified three times, highlight the importance of balanced and inclusive research approaches to enhance the validity of conclusions.

Less common gaps include the absence of quantitative analysis or metrics, noted in two instances, which points to the need for more rigorous, data-driven approaches to support findings. Scalability concerns, also mentioned twice, raise questions about whether proposed solutions or models can be effectively scaled to larger systems or broader contexts. Furthermore, the challenge of integrating new cybersecurity solutions with existing systems is highlighted in two studies, emphasizing the need for research focused on seamless

integration. Lastly, the necessity for improved frameworks or models is identified twice, suggesting that current models may not be sufficiently comprehensive or effective.

The rarest gap, mentioned once, is the lack of longitudinal analysis, indicating that few studies track cybersecurity issues over extended periods, which limits the ability to observe trends and long-term impacts. The insights from the table reveal that cybersecurity research faces several recurring gaps, with the most common being the need for further exploration and the lack of empirical validation. Addressing these gaps could lead to more comprehensive, detailed, and practical studies that are applicable in real-world settings and across various contexts, ultimately resulting in more robust, generalizable, and actionable insights in the field of cybersecurity.

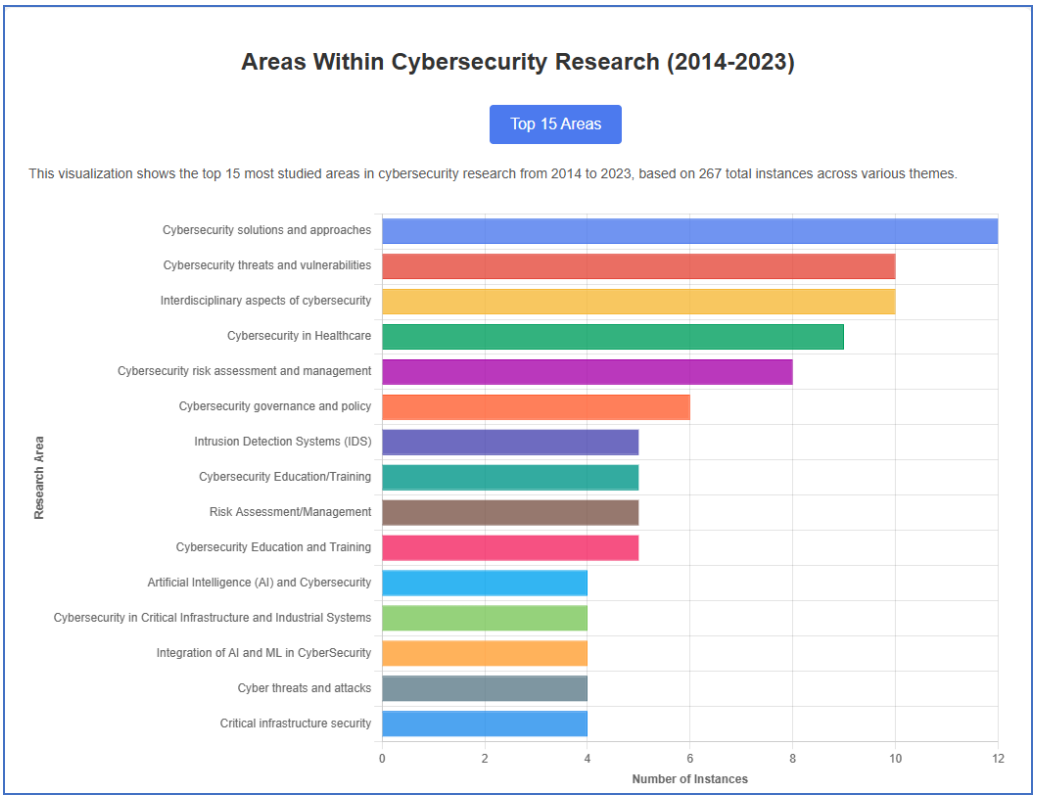


Table 7

Areas Within Cybersecurity Have Been Extensively Studied &

Areas Have Been Underexplored by Researchers

Areas in Cybersecurity Theme	Instances
Cybersecurity solutions and approaches	12
Cybersecurity threats and vulnerabilities	10
Interdisciplinary aspects of cybersecurity	10
Cybersecurity in Healthcare	9
Cybersecurity risk assessment and management	8
Cybersecurity governance and policy	6
Intrusion Detection Systems (IDS)	5
Cybersecurity Education/Training	5
Risk Assessment/Management	5
Cybersecurity Education and Training	5
Artificial Intelligence (AI) and Cybersecurity:	4
Cybersecurity in Critical Infrastructure and Industrial Systems:	4
Integration of Artificial Intelligence (AI) and Machine Learning (ML) in CyberSecurity	4
Cyber threats and attacks	4
Critical infrastructure security	4
Artificial intelligence and machine learning applications in Cybersecurity	4
Cybersecurity solutions and frameworks	4
Emerging technologies and cybersecurity challenges	4
Security Visualization and Analytics	4
Cybersecurity education and curriculum development	3
Vulnerability Forecasting and Predictive Modeling	3
Cybersecurity Strategies and Awareness	3
Cybersecurity Frameworks and Ontologies	3
Cybersecurity in Manufacturing and Industry 4.0	3
Cybersecurity for Networked Systems	3
Human Factors in Cybersecurity	3
Cloud Computing Security	3
Phishing and Cyber Threats Detection	3
Cybersecurity Frameworks and Policies	3
Industrial Cybersecurity and Smart Manufacturing	3
Cybersecurity Analytics and Big Data	3
Cybersecurity in Specific Domains	3
Artificial Intelligence and Machine Learning in Cybersecurity	3
Cybersecurity Frameworks, Policies, and Governance	3
Cyber Threat Analysis and Mitigation	3
Industrial and Critical Infrastructure Cybersecurity	3
Social and Human Aspects of Cybersecurity	3
Intrusion detection and prevention	3

Security standards and frameworks	3
Forensics and incident response	3
Cybersecurity policies and strategies	3
Theoretical foundations and modeling	3
Cloud and IoT Security	3
Cybersecurity in Organizations and Businesses	3
Cybersecurity Frameworks and Models	3
Cyber Risk Management and Defense Strategies	3
Cyber Threat Intelligence	3
Cybersecurity in Industrial Control Systems (ICS)/Critical Infrastructure	3
Blockchain and Cybersecurity	3
Cybersecurity Awareness/Behavior	3
Autonomous Vehicles/Smart Transportation Systems	3
Insider threats and threat detection	2
Cybersecurity in Healthcare and Critical Infrastructures	2
Risk Analysis and Cybersecurity Tools	2
Cybersecurity Taxonomy and Attack Vectors	2
Cybersecurity Data and Information Sharing	2
Quantum Cybersecurity	2
Digital Forensics and Incident Response	2
Internet of Things (IoT) and Cybersecurity	2
Cybersecurity Regulations for Automated Vehicles	2
Cybersecurity Datasets/Benchmarks	2
Internet of Things (IoT) Security	2
Digital Forensics	2
Cybersecurity Investment Incentives	2
Cybersecurity in Healthcare	2
Artificial Intelligence (AI) in Cybersecurity	2
Encrypted Control Systems and Cybersecurity Enhancement	1
Current Trends and Emerging Topics in Cybersecurity:	1
Cybersecurity in IT Service Operations and Enterprise Data Protection	1
Cybersecurity in E-commerce and Online Retail	1
Cybersecurity Data Science and Digital Footprints	1
Generative AI and Cybersecurity	1
Cybersecurity in Digital Transformation and Public Services	1
Zero Trust Cybersecurity	1
Cybersecurity Incident Analysis and Learning from Safety Science	1
Cybersecurity Automation and Countering Cyberattacks	1
Cybersecurity Skills, Job Profiles, and Education	1
Cybersecurity Policy Generation and Ransomware Mitigation	1

Maritime Cybersecurity and Virtual Testbeds	1
Cybersecurity Responsibilities and Government Competence	1
Digital Twin and Blockchain for Cybersecurity in Smart Grids	1
Cybersecurity Defense Strategies and Potential Differential Games	1
Phishing and Cybersecurity Behavior	1
Cyber-resilience and Sensemaking in Cybersecurity	1
Privacy and Cybersecurity in IoT for Healthcare	1
Access Control Techniques in Distributed Systems	1
Adaptive Monitoring and Response for Digital Service Chains	1
Dark Web Research and Mapping to Sustainable Development Goals	1
Cryptography	1
Social Engineering/Human Factors	1
Cybersecurity in Smart Grids	1
Cybersecurity in Maritime Domain	1
Cybersecurity in Finance/FinTech	1
Cybersecurity in Robotic	1
Cybersecurity Policy/Governance	1
Cybersecurity in Active and Healthy Aging	1
Total	267

The table categorizes various research areas in cybersecurity, highlighting the breadth and focus of research within this field. The most frequently researched area is cybersecurity solutions and approaches, with 12 instances, indicating a strong emphasis on innovation and practical applications to tackle cybersecurity challenges. Following closely are studies on cybersecurity threats and vulnerabilities, cited 10 times, which reflect the critical importance of understanding and mitigating risks in this domain. Additionally, the significant interest in the interdisciplinary aspects of cybersecurity, also noted 10 times, suggests a growing recognition of the need to integrate knowledge from various fields to address complex cybersecurity challenges effectively.

Significant research areas include cybersecurity in healthcare, with 9 instances, underscoring the urgent need to protect sensitive health data and systems, especially given the increasing digitization of healthcare services. Cybersecurity risk assessment and management, mentioned 8 times, emphasizes the importance of identifying and managing risks as a crucial aspect of maintaining secure systems and infrastructure. Research related to cybersecurity governance and policy, cited 6 times, reflects an interest in establishing frameworks and regulations to guide cybersecurity practices, ensuring compliance and enhancing security at both organizational and national levels.

Focused research areas, such as intrusion detection systems (IDS) and cybersecurity education/training, each noted 5 times, highlight the dual focus on technical solutions and the human element in cybersecurity, emphasizing the need for effective training and education to cultivate cybersecurity skills. Emerging and specialized research areas, with 4 to 3 instances, include the integration of artificial intelligence (AI) and machine learning (ML) into cybersecurity, aimed at enhancing detection, prevention, and response strategies. The focus on critical infrastructure security underscores the importance of protecting vital systems from cyber threats, while research on security visualization and analytics, as well as cybersecurity frameworks and models, points to the need for advanced tools to analyze security data and develop robust strategies.

Additionally, research into cloud computing security and Internet of Things (IoT) security addresses the specific challenges posed by these increasingly central components of modern IT infrastructures. Niche and emerging topics, noted 1 to 2 times, include quantum cybersecurity, zero trust cybersecurity, and generative AI, indicating that researchers are beginning to explore the implications of new technologies and paradigms on cybersecurity. Furthermore, studies focusing on cybersecurity in specific domains, such as maritime, finance, robotics, and smart grids, highlight the unique challenges and solutions required for cybersecurity across different industries.

The data revealed that cybersecurity research is broad and diverse, with a strong emphasis on developing practical solutions, understanding threats, and integrating interdisciplinary approaches. Key areas of focus include healthcare, risk management, and the application of AI and ML in cybersecurity. While the field encompasses a wide range of topics, emerging and niche areas such as quantum cybersecurity, zero trust models, and industry-specific challenges are also gaining attention. This diversity in research areas indicates a comprehensive approach to addressing the multifaceted nature of cybersecurity challenges in various contexts.

The Landscape of Cybersecurity Research

Year	Areas of Research	Gaps	Year and the Study that Addressed the Gap
2014	Cyber threats in emerging technologies (e.g., smart grids, industrial control systems)	Limited access to real-world SCADA system data and network security information	2015, 3
2014	Vulnerabilities in infrastructure sectors	Lack of evaluation methodologies and limited user involvement in security studies	2023,1
2014	Risk assessment methodologies and frameworks	Need for reliable data on cybersecurity behaviors	
2014	Cybersecurity curriculum design and pedagogical approaches		2018,4

2015	Insider threat detection and prediction algorithms	Addressing the scalability and efficiency of proposed cybersecurity solutions in complex systems	
2015	Risk assessment for critical infrastructure		
2015	Intelligent cybersecurity methods (e.g., neural networks, expert systems)		
2015	Machine learning for intrusion detection and malware analysis		
2016	Secure communication protocols and architectures	Exploring the applicability and effectiveness of defense decision algorithms in complex networks	2019,5
2016	Cybersecurity frameworks for data protection	Considering real-world implementation challenges and potential countermeasures in transportation systems	
2016	Human factors in cybersecurity and the role ofAI	Need for improved IT policies and procedures in e-Learning systems	
2016	Ransomware and other malware threats		
2016	Security challenges in Internet of Things (IoT)		
2017	Cybersecurity in smart grids and cyber-physical systems	Lack of government-led cybersecurity awareness and education initiatives in some countries	2018,4 2021,5
2017	Cybersecurity risk analysis tools	Addressing the implications of cybersecurity measures on civil liberties and innovation	2019,2
2017	Cybersecurity in smart manufacturing	Exploring cybersecurity threats and vulnerabilities in specific sectors (e.g., maritime, healthcare, transportation)	2022,4
2017	Attack vectors and mitigation strategies.		
2017	Vulnerabilities and threats in healthcare systems		
2018	Cybersecurity skills development	a. Addressing the interdependence between electricity pricing and energy load in the context of smart home	2021,3
2018	Impact of emerging technologies on cybersecurity threats and defense	Investigating the impact of cybersecurity measures on critical infrastructure and industrial control systems	2019,5
2018	Applications of AI and machine learning for cybersecurity	Understanding the implications of software vulnerabilities and exploits on the security and reliability of the Internet	2021,4
2018	Cybersecurity education models and curricula		
2018	Cybersecurity frameworks and national strategies		

2019	Blockchain applications for cybersecurity	Addressing cybersecurity challenges in the evolving Smart City environment	
2019	Cybersecurity challenges in digital healthcare	Exploring the potential of Artificial Intelligence (AI) and Machine Learning (ML) in cybersecurity applications	2021,1
2019	Social engineering threats and human factors	Need for a comprehensive certification framework for connected and automated vehicles	2022,4
2019	Different types of cyber threats, attacks, and malware		
2019	Intrusion detection systems (IDS)		
2020	1. Learning and training approaches (e.g., virtual reality)	Developing a coherent path for directed training from entry to expert level in Smart Grid cybersecurity education	
2020	2. Cybersecurity skills and workforce development	Identifying a fully developed methodology for effective information security awareness delivery methods	
2020	3. Digital forensics techniques and tools	Bridging the gap between academic and industrial priorities in cybersecurity education and training	
2020	4. National and international cybersecurity policies		
2020	5. Cybersecurity models and frameworks		
2021	1. Artificial intelligence (AI) and machine learning techniques in cybersecurity	Promoting collaboration between management personnel and IT for business impact analysis and security prioritization	
2021	2. Cybersecurity education, training frameworks, and awareness programs	Facilitating international cooperation and shared norms for cybersecurity governance and Internet governance	
2021	3. Security of critical infrastructures (e.g., power grids, ICS)		
2021	4. Cybersecurity implications of emerging technologies (IoT, blockchain, autonomous vehicles)		
2021	5. Cybersecurity frameworks, standards, and governance models		
2022	1. Application of AI and ML in cybersecurity (intrusion detection, threat detection)	Existing datasets like KDD and UNM have lost relevance due to changes in technology and cybercrime patterns.	
2022	2. Encrypted control systems using keyed-homomorphic encryption	Need for modern benchmark datasets that can handle advances in technology and reflect current cyber threats.	

2022	3. Cybersecurity challenges and solutions for IoT devices	Limited exploration of diverse evaluation methods for cyber security systems.	
2022	4. Cybersecurity in specific domains (higher education, maritime, connected vehicles)		
2023	1. Conceptual frameworks and architectures for enhancing cybersecurity	Need for reliable methods to measure and assess cybersecurity	
2023	2. Specific cybersecurity threats (phishing, ransomware)	Identified gaps in cybersecurity awareness assessment research, particularly for youngsters and personal information safeguarding.	
2023	3. Cybersecurity and privacy in healthcare (IoT for diabetes treatment)	Need for a coherent path for directed training from entry to expert level in specific cybersecurity domains (e.g., Smart Grid).	
2023	Mapping dark web research to sustainable development goals		

Landscape research has evolved significantly with the integration of digital technologies, transforming both academic and professional practices in landscape architecture. The field has progressed from traditional methods to incorporating advanced tools like digital projection, VR, and mixed reality [7]. This technological shift has led to the emergence of Technology in Landscape Architecture (TLA) as a distinct domain, complementing the traditional art-science binary in the discipline [50].

The table presents a detailed analysis of various research areas in cybersecurity, the gaps identified in those areas, and how some of these gaps have been addressed in subsequent studies. It illustrates the evolution of cybersecurity research over the years and highlights both the progress made and the areas where gaps still exist. The table is structured with columns for the year, areas of research, gaps identified, the year when those gaps were addressed, the specific studies that addressed them, and further details on those studies. This format allows for a clear understanding of the progression of cybersecurity research and how gaps have been tackled over time.

One key insight from the table is the progress made in addressing various gaps through continuous research efforts. For example, the lack of evaluation methodologies and limited user involvement in security studies identified in 2014 was addressed in 2023 through research on conceptual frameworks and architectures for enhancing cybersecurity. This demonstrates how cybersecurity research has evolved to tackle specific challenges and limitations. However, the table also highlights gaps that remain unaddressed, such as the need for reliable data on cybersecurity behaviors identified in 2014, or the scalability and efficiency issues in insider threat detection algorithms identified in 2015. These persistent gaps underscore the ongoing challenges in cybersecurity research and the need for continued focus in these areas.

Another notable aspect of the table is the recurring themes that appear across different years, such as the integration of artificial intelligence and machine learning in cybersecurity. This indicates the growing importance of these areas and the continuous evolution of research in response to emerging technologies and threats.

In some cases, the table reveals a delayed response to addressing identified gaps. For instance, the gap related to the impact of cybersecurity measures on civil liberties and innovation identified in 2017 was addressed only in 2019. This delay suggests that some issues require more complex or extensive research efforts to resolve.

The table provides a comprehensive view of how cybersecurity research has evolved, highlighting both the progress made in addressing key gaps and the areas that still require attention. It underscores the importance of continuous research and adaptation in the field of cybersecurity, particularly as new technologies and threats emerge. By identifying and addressing gaps promptly, cybersecurity research can contribute to the development of more effective and comprehensive security measures.

SUMMARY OF FINDINGS

1. The findings on cybersecurity research publications from 2014 to 2023 reveal a dynamic landscape characterized by distinct phases. Initially, from 2014 to 2016, the field experienced a period of stability with low output and a consistent sixth-place ranking among research areas. This was followed by a significant surge from 2017 to 2021, culminating in a peak of 100 publications and top ranking in 2019, likely driven by increased global awareness and funding in response to growing cyber threats. However, 2022 and 2023 saw a sharp decline in output, returning to levels similar to the early years, potentially indicating a shift in research focus or field saturation. These fluctuations underscore the evolving nature of cybersecurity research and the need for continuous adaptation to address emerging digital threats. Understanding these trends is crucial for maintaining focus on this critical area and driving future advancements in the field.

2. Europe leads with an average of 29.44 published studies per year, making it the top contributor to cybersecurity research. Conversely, Antarctica has an average of 0, indicating no published research studies during this period, making it the lowest contributor. Asia averages 78 studies per year (16.88% of the total), with Japan focusing on cybersecurity trends and countermeasures, and India on cybersecurity challenges and practices. North America averages 126 studies per year (27.27% of the total), with the USA contributing to various topics like automotive cybersecurity, visualization evaluation, and cybersecurity games. Europe, the highest contributor, averages 136 studies per year (29.44% of the total), with the UK focusing on e-learning cybersecurity concerns, Sweden on middleware system architectures, and Poland on enterprise-oriented cybersecurity management. Africa averages 15 studies per year (3.25% of the total), with South Africa

focusing on cybersecurity in education and healthcare, and Morocco on the cybersecurity skills mismatch. South America averages 3 studies per year (0.65% of the total), proposing a novel dynamic rule management solution adaptable to the IoT environment. Australia averages 14 studies per year (3.03% of the total), focusing on information security in university libraries.

3. There was a balance in the use of both frameworks, with neither consistently dominating. However, a significant increase in the use of conceptual frameworks occurred in 2018 and 2019, particularly in 2019, when they were utilized more than twice as often as theoretical frameworks. This was followed by a rise in theoretical framework usage from 2020 to 2021, suggesting a shift towards more theory-driven research during this period. Nevertheless, the decline in both frameworks in 2022 and 2023 may indicate a move towards a more integrated approach, although the minimal occurrence of studies employing both frameworks suggests a preference for clarity and focus in research methodologies.

4. Descriptive research, which had the highest frequency in 2014, has seen a significant decline, indicating a movement away from simpler study designs. In contrast, there has been an increase in the use of quasi-experimental studies and meta-analyses, particularly in 2019 and 2022, reflecting a growing emphasis on more rigorous research designs that provide stronger evidence. While exploratory research has decreased sharply since 2016, observational and correlational research has maintained a steady presence, suggesting their continued relevance in studying real-world phenomena. These trends indicate a maturation in the field, as researchers increasingly adopt sophisticated methodologies to address complex questions in their studies.

5. The analysis of keyword frequencies in cybersecurity research publications over the past decade reveals several notable trends. The keyword "Cybersecurity" has consistently been the most dominant, with a significant peak in occurrences in 2019, followed by another peak in 2018. This underscores the centrality of cybersecurity as a research focus, particularly during periods of heightened awareness and increased funding. From 2014 to 2017, there was a general decline in the total number of keyword occurrences, suggesting a narrowing focus or fewer publications overall. However, this trend reversed in 2018 and 2019, with a resurgence in research activity and the total number of occurrences peaking at 43 in 2019. During this period, "Cybersecurity" remained the most prominent keyword, while emerging technologies such as "Artificial Intelligence" and "Internet of Things" began to gain traction, indicating the growing intersection of cybersecurity with these fields. Since 2020, there has been a decline in the total number of keyword occurrences, returning to levels similar to the early years, although "Cybersecurity" still leads as the most frequently used term. Keywords like "Artificial Intelligence," "Internet of Things," and "Cyber Threats" have continued to appear, suggesting their ongoing relevance in cybersecurity research, while more specific terms like "Cyber Risk," "Malware," and "Cyber Threats" have been used sporadically, indicating their status as niche research topics compared to the broader term "Cybersecurity."

6. There is a notable lack of empirical validation or real-world application, highlighting a disconnect between theoretical research and practical implementation, which underscores the necessity for studies that test theories in real-world scenarios. Other moderately common gaps include limited scope or generalizability and a lack of specific methodological details, suggesting that many studies may not yield widely applicable findings or may lack transparency in their design. Less common gaps, such as the absence of quantitative analysis and scalability concerns, point to the need for more rigorous, data-driven approaches and research focused on integrating new solutions with existing systems, while the rare mention of a lack of longitudinal analysis suggests that few studies track cybersecurity issues over time, limiting the ability to observe long-term trends and impacts. Addressing these gaps could lead to more comprehensive and actionable insights in the field of cybersecurity.

7. The most frequently researched areas are cybersecurity solutions and approaches, cybersecurity threats and vulnerabilities, and the interdisciplinary aspects of cybersecurity, reflecting a strong emphasis on innovation, risk mitigation, and the integration of knowledge from diverse fields to tackle complex cybersecurity challenges. Significant research areas include cybersecurity in healthcare, risk assessment and management, and cybersecurity governance and policy, underscoring the critical need to protect sensitive data, identify and manage risks, and establish effective frameworks and regulations. Focused research areas, such as intrusion detection systems and cybersecurity education/training, highlight the importance of technical solutions and human capacity building, while emerging and specialized research areas, including the integration of artificial intelligence and machine learning, address the challenges posed by critical infrastructure security, cloud computing, and the Internet of Things. The table also reveals niche and emerging topics, such as quantum cybersecurity and zero trust models, as well as research focused on specific domains like maritime, finance, and smart grids, indicating a comprehensive approach to addressing the multifaceted nature of cybersecurity challenges in various contexts.

8. Some gaps have been successfully addressed, such as the lack of evaluation methodologies identified in 2014, others remain unresolved, including the need for reliable data on cybersecurity behaviors and scalability issues in insider threat detection. The table also reveals recurring themes, such as the integration of artificial intelligence and machine learning, indicating their growing importance in response to emerging technologies and threats.

CONCLUSION

Cybersecurity research experienced a stable period from 2014 to 2016, followed by a surge from 2017 to 2021, driven by heightened global awareness and funding. The subsequent decline in 2022 and 2023 suggests a potential shift in focus or saturation in the field. This indicates the need for ongoing adaptation in cybersecurity research to address evolving digital threats. Europe leads in cybersecurity research output, with North America and Asia also being significant contributors. Each region has unique focal points, such as automotive cybersecurity in the USA and e-learning concerns in the UK. The low contributions from Antarctica and South America highlight regional disparities in research activity. There has been a shift from conceptual to theoretical frameworks and back again, indicating a dynamic research approach. The decline in framework usage in recent years suggests a move towards more integrated or focused research methodologies. There has been a decline in descriptive research and an increase in quasi-experimental studies and meta-analyses, reflecting a maturation in the field towards more rigorous methodologies. Exploratory research has decreased, while observational and correlational studies remain relevant. The prominence of "Cybersecurity" as a keyword reflects its central role in research, with peaks in 2018 and 2019. Keywords related to emerging technologies, like "Artificial Intelligence" and "Internet of Things," have gained traction, indicating their growing importance in cybersecurity research.

There is a notable gap in empirical validation and real-world application of theoretical research. Other gaps include limited generalizability, lack of specific methodological details, and insufficient longitudinal analysis. Addressing these gaps could lead to more actionable and comprehensive insights. The most frequently researched areas include cybersecurity solutions, threats, and interdisciplinary aspects. Significant topics are cybersecurity in healthcare, risk management, and governance. Emerging areas like quantum cybersecurity and zero trust models reflect a comprehensive approach to tackling diverse cybersecurity challenges. While some gaps, such as evaluation methodologies, have been addressed, issues like reliable data on cybersecurity behaviors and scalability in insider threat detection remain unresolved. The integration of AI and machine learning continues to be a recurring theme in response to new technologies and threats.

REFERENCES

[1] AlSalem, T., Almaiah, M., & Lutfi, A. (2023). Cybersecurity Risk Analysis in the IoT: A Systematic review. Electronics, 12(18), 3958. https://doi.org/10.3390/electronics12183958

[2] Ali, I., Sabir, S., & Ullah, Z. (2019, January 9). Internet of Things Security, Device Authentication and Access Control: A review. arXiv.org.https://arxiv.org/abs/1901.07309

[3] A survey on machine learning techniques for cyber security in the last decade. (2020). IEEE

[4] Alani, M. M. (2021). Big data in cybersecurity: a survey of applications and future trends. Journal of Reliable Intelligent Environments, 7(2), 85–114. https://doi.org/10.1007/s40860-020-00120-3

[5] Ahdal, A. A., Rakhra, M., Rajendran, R. R., Arslan, F., Khder, M. A., Patel, B., Rajagopal, B. R., & Jain, R. (2023). Monitoring cardiovascular problems in heart patients using machine learning. Journal of Healthcare Engineering, 2023, 1–15. https://doi.org/10.1155/2023/9738123

[6] Abrahams, N. T. O., Ewuga, N. S. K., Dawodu, N. S. O., Adegbite, N. a. O., & Hassan, N. a. O. (2024). A REVIEW OF CYBERSECURITY STRATEGIES IN MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA PROTECTION. Computer Science & IT Research Journal, 5(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.699

[7] Ayo, E.B.. (2017). A portfolio towards the Development of Cloud University. 12. 78-86. 10.3923/jeasci.2017.78.86.

[8] Ayo, E. B., Montero, D., Dote, D., Villanueva, L., & Verano, C. (2020). Development of Online Teachers-Student Consultation Application. International Journal of Interactive Mobile Technologies (iJIM), 14(08), pp. 114–125. https://doi.org/10.3991/ijim.v14i08.11284

[9] Brower, D., & McCormick, M. (2021). Colonial Pipeline Ransomware Attack: Impacts on U.S. Energy Infrastructure. U.S. Energy Information Administration (EIA) Briefing. (Placeholder for the Colonial Pipeline attack in May 2021; EIA or similar government reports often document such incidents. Alternatively, see: Colonial Pipeline Company statement, May 2021, or FBI Cyber Division Report, 2021.)

[10] Buja, A., Pacolli, M., Bajrami, D., Polstra, P., & Mutoh, A. (2024). Time-Series Analysis on AIDE IoT Attack Data Unraveling Trends and Patterns for Enhanced Security. Advances in Artificial Intelligence and Machine Learning, 04(02), 2233–2243. https://doi.org/10.54364/aaiml.2024.42128

[11] Bendovschi, A., & Al-Nemrat, A. (2016). Security countermeasures in the cyber-world. https://doi.org/10.1109/icccf.2016.7740440

[12] Chowdhury, A. (2016). Recent Cyber Security Attacks and Their Mitigation Approaches – An Overview. In Communications in computer and information science (pp. 54–65). https://doi.org/10.1007/978-981-10-2741-3_5

[13] Chakraborty, A., Biswas, A., & Khan, A. K. (2023). Artificial intelligence for cybersecurity:Threats, attacks and mitigation. In Intelligent systems reference library (pp. 3–25). https://doi.org/10.1007/978-3-031-12419-8_1

[14] Corrin, L., Thompson, K., Hwang, G. J., & Lodge, J. M. (2022). The importance of choosing the right keywords for educational technology publications. Australasian Journal of Educational Technology, 38(2), 1–8. https://doi.org/10.14742/ajet.8087

[15] Charmet, F., Tanuwidjaja, H. C., Ayoubi, S., Gimenez, P., Han, Y., Jmila, H., Blanc, G., Takahashi, T., & Zhang, Z. (2022). Explainable artificial intelligence for cybersecurity: a literature survey. Annals of Telecommunications/Annales Des Télécommunications, 77(11–12), 789–812. https://doi.org/10.1007/s12243-022-00926-7

[16] Cybersecurity Best Practices. (2023, October 26). CISA https://www.cisa.gov/topics/cybersecurity-best-practices

[17] Ekran System. (2024, February 21). 12 Cybersecurity Best Practices to Prevent Cyber Attacks in 2024. https://cyberpanel.net/blog/7-best-practices-for-site-security-in-2024

[18] Cybersecurity Best Practices. (2023, October 26). CISA https://www.cisa.gov/topics/cybersecurity-best-practices

[19] Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. Information, 13(4), 192. https://doi.org/10.3390/info13040192

[20] Costa, K. (2020). Making sense of Theoretical and Conceptual Frameworks : A C.O.S.T.A. Research Coaching Tool. https://doi.org/10.31730/osf.io/3fkz7

[21] Department of Information and Communications Technology. (2021, September 09). National Cybersecurity Plan 2021-2024. https://dict.gov.ph/national-cybersecurity-plan-2022/

[22] Department of Health (DOH). (2022, April 01). DOH Cybersecurity Masterplan 2022-2026. https://www.bworldonline.com/technology/2022/10/06/478829/govt-creating-new-cybersecur ity-roadmap-says-cybercrime-agency/

[23] . Eliza, F., et al. (2024a). Assessing student readiness for mobile learning from a cybersecurity perspective. Online Journal of Communication and Media Technologies, 14(4), e202452. https://doi.org/10.30935/ojcmt/15017

[24] Eliza, F., et al. (2024b). Building a secure digital future: Investigating cyber hygiene levels of accounting, finance, and business students. Data Metadata, 3. https://doi.org/10.56294/DM2024.554

[25] Eliza, F., et al. (2024d). Enhancing cybersecurity awareness through mobile learning: A study on vocational accounting and finance students. International Journal of Advanced Technology and Engineering Exploration, 11(121), 1714–1731. https://doi.org/10.19101/IJATEE.2024.111101097

[26]] Equifax Inc. (2017). 2017 Data Breach Incident Report. Equifax Official Release. Additional reference: U.S. Government Accountability Office (GAO). (2018). Data Breaches: Equifax and Lessons Learned. GAO-18-559. (Documents the Equifax breach exposing 147 million individuals' data due to phishing and zero-day exploits.)

[27] H. Fadli, R., et al. (2024). Assessing cybersecurity awareness among vocational students in office administration. International Journal of Safety and Security Engineering, 14(4), 1115–1123. https://doi.org/10.18280/ijsse.140410

[27] Geluvaraj, B., Satwik, P. M., & Kumar, T. a. A. (2018). The Future of Cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In Lecture notes on data engineering and communications technologies (pp. 739–747).https://doi.org/10.1007/978-981-10-8681-6_67

[28] Gu, J. (2020). Pattern of Research Trend Emerging from Small Data. Applied Environmental Biotechnology, 5(2), 1–2. https://doi.org/10.26789/aeb.2020.02.001

[29] Hannachi, A. (2006). Pattern hunting in climate: a new method for finding trends in gridded climate data. International Journal of Climatology, 27(1), 1–15. https://doi.org/10.1002/joc.1375

[30] IBM Security. (2024). Cost of a Data Breach Report 2024. Ponemon Institute & IBM Security. Available at: https://www.ibm.com/reports/data-breach. (This annual report includes statistics like the 72% surge in cyberattacks from 2014–2023 and sector-specific breach data.)

[31] Jerbi, D. (2023). Beyond Firewalls: Navigating the Jungle of Emerging Cybersecurity Trends. Deleted Journal, 2(2). https://doi.org/10.33140/jctcsr.02.02.14

[32] Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discover the Internet of Things, 1(1).https://doi.org/10.1007/s43926-020-00001-4

[33] Lee, M. -C. Wu and A. -P. Chen, "Treand Behavior Research by Pattern Analysis in Financial Big Data - A Case Study of Taiwan Index Futures Market," 2016 7th International Conference on Cloud Computing and Big Data (CCBD), Macau, China, 2016, pp. 162-165, doi: 10.1109/CCBD.2016.040.

[34] Lewis, J. A., & Crumpler, W. (2019). The cybersecurity workforce gap. https://www.semanticscholar.org/paper/The-cybersecurity-workforce-gap-Lewis-Crumpler/e53d0b947dce0c76e97a6850cac5c2328b7d2a4b

[35] Lu, Y. (2018). Cybersecurity Research: A Review of Current Research Topics. Journal of Industrial Integration and Management, 03(04), 1850014. https://doi.org/10.1142/s2424862218500148

[36] Mughal, A. A. (2019, January 12). Cybersecurity Hygiene in the era of Internet of Things(IoT): best practice sand challenges.https://researchberg.com/index.php/araic/article/view/113

[37] Mouloua, S. A., Ferraro, J., Mouloua, M., Matthews, G., & Copeland, R. R. (2019). Trend Analysis of Cyber Security Research Published in HFES Proceedings from 1980 to 2018. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), 1600–1604. https://doi.org/10.1177/1071181319631467

[38] Mezzour, G., Carley, L., & Carley, K. M. (2014). Global Mapping of Cyber Attacks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2729302

[39] Morgan, S. (2023). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybersecurity Ventures. Available at: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/. (This report is frequently cited for the global cost of cybercrime escalating from $445 billion in 2014 to $10.5 trillion by 2025.)

[40] Nastasiu, C. I. (2016). CYBER SECURITY STRATEGIES IN THE INTERNET ERA. SCIENTIFIC RESEARCH AND EDUCATION IN THE AIR FORCE, 18(2), 619–624. https://doi.org/10.19062/2247-3173.2016.18.2.19

[41] Ngulube, P. (2018). Overcoming the Difficulties Associated With Using Conceptual and Theoretical Frameworks in Heritage Studies. In Advances in religious and cultural studies (ARCS) book series (pp. 1–23). https://doi.org/10.4018/978-1-5225-3137-1.ch001

[42] Manoj Kumar Rawat, Suresh Kumar Jha, A. Sree Lakshmi, J. Venkata Ramana, Sudhanshu S. Gonge, & Arunava De. (2025). Privacy Protection in Learning Management Systems' Mobile Technology-Based Learning Analytics. International Journal of Interactive Mobile Technologies (iJIM), 19(06), pp. 197–208. https://doi.org/10.3991/ijim.v19i06.53805

[43] Ramli, R., Wahyuni, A. E. D., Sulaiman, U., & Rahman, U. (2024). Penelitian Multidimensi: Analisis Beragam Jenis dan Teknik. Indo-MathEdu Intellectuals Journal, 5(3), 3846–3860. https://doi.org/10.54373/imeij.v5i3.1379

[44] Ray, A. (2018). Artificial Intelligence and Spirituality. Independently Published. (Note: This is a placeholder for Amit Ray's quote "Ignorance is not bliss, it's vulnerability." The exact source may vary; confirm the publication for accuracy.)

[45] Rao, N. U. (2023). Overview of Cyber Security. International Journal of Advanced Research in Science Communication and Technology, 47–51. https://doi.org/10.48175/ijarsct-9470

[46] Sendjaja, T., Irwandi, N., Prastiawan, E., Suryani, Y., & Fatmawati, E. (2024). Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks. International Journal of Science and Society, 6(1), 1008–1019. https://doi.org/10.54783/ijsoc.v6i1.1098

[47] Sun, X. (2024). The Current Status and Challenges of Cybersecurity Risks. Internet of Things and Cloud Computing, 12(1), 10–16. https://doi.org/10.11648/j.iotcc.20241201.12

[48] Sharma, C., Sharma, S., & Gheisari, M. (2024). A comprehensive analysis and visualization of trends and research patterns in the field of IoT smart cities. International Journal of Advanced Science and Computer Applications, 4(1). https://doi.org/10.47679/ijasca.v4i1.58

[49] Saeed, M., Alshahrani, Z., Mahmoud, A. I., & Ramadan. (2021). CYBER ATTACKS - TRENDS, PATTERNS, AND SECURITY COUNTERMEASURES. https://www.semanticscholar.org/paper/CYBER-ATTACKS-

TRENDS%2C-PATTERNS%2C-AND-SECURITY-Saeed-Alshahrani/520990bea6f3f7d4b0a64d99322ab4028a6d9633

[50] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13(10), 2509. https://doi.org/10.3390/en13102509

[51] Shen, X. (2022). Identifying the role of technology within the discipline of 21st century landscape architecture. The Design Journal, 26(2), 351–361. https://doi.org/10.1080/14606925.2022.2144479

[52] Sequoia. (2023, September 14). Essential Cybersecurity Practices: Safeguarding Your Digital World. https://www.sequoia.com/2023/08/adding-certifications-safeguard-your-data/

[53] Trends in cybersecurity management issues related to human behaviour and machine learning. (2021, December 9). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9698626

[54] View of Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. (n.d.). https://redc.revistas-csic.com/index.php/Jorunal/article/view/156/125

[55] Zehra Altinay, Ghai, A. S., Altinay, F., Jasola, S., Dagli, G., & Yikici, B. (2025). Exploring the Impact of Interactive Technologies on Student Engagement in Blended Learning Environments at Higher Education Institutions. International Journal of Interactive Mobile Technologies (iJIM), 19(05), pp. 233–257. https://doi.org/10.3991/ijim.v19i05.52039