PENINSULA PUBLISHING LLC

SHIFRA

Vol. **(2026)**, 2026, **pp**. 62–75
ISSN: 3078-3186

Research Article

Zero Trust Security: A Bibliometric Review of Concepts, Adoption, and Research Gaps

Kulondwa Mburunge[1,*], Khder Alakkari [2,3], Bushra Ali [4]

[1] *Master students at ISP/Bukavu BP: 854, Congo*

[2] *Department of Statistics and Programming, Faculty of Economics, Latakia University, P.O. Box 2230, Syria*

[3] *Department of Financial and Banking Sciences, Faculty of Economics, Tartous University, Syria*

[4] *Department of Banking & Financial Sciences, Faculty of Economics, Tartous University, Tartous, Syria*

ARTICLE INFO

Article History

Received 10 Nov 2025

Revised: 4 Jan 2026
Accepted 3 Feb 2026
Published 20 Feb 2026

Keywords

Zero Trust Security,

Cybersecurity Frameworks,

Bibliometric Analysis,

Research Trends and Gaps,

Artificial Intelligence Integration.

ABSTRACT

This bibliometric analysis examines the evolving landscape of Zero Trust Security literature, emphasizing the trends, key contributors, and research gaps within this critical field. Using the Biblioshiny R package, we retrieved a total of 1,200 publications from 2015 to 2023, reflecting a marked increase in scholarly output that underscores the growing recognition of Zero Trust frameworks in cybersecurity. Analysis revealed a consistent growth trend, peaking in 2021, with a notable decline in publication rates thereafter, suggesting potential saturation or shifting focus in research topics. The most productive authors included five leading researchers who contributed over 150 publications collectively, with prominent journals such as the Journal of Cybersecurity and IEEE Access being the primary platforms for dissemination.

Co-citation analysis identified several thematic clusters, including the integration of artificial intelligence in Zero Trust strategies and the challenges of implementing these frameworks in diverse organizational contexts. Keyword clustering revealed emerging topics such as "resilient security" and "cyber threat adaptation," highlighting areas ripe for further exploration.

Despite the increased volume of literature, significant gaps persist, particularly concerning empirical studies that assess the practical application of Zero Trust principles across various sectors. This analysis underscores the necessity for future research to explore these empirical dimensions and foster a more comprehensive understanding of Zero Trust Security, ultimately guiding practitioners in effective implementation strategies within an ever-evolving digital landscape.

1. INTRODUCTION

In the evolving landscape of cybersecurity [1], the concept of Zero Trust Security has emerged as a pivotal framework, fundamentally challenging traditional perimeter-based security models [1]. As organizations increasingly confront sophisticated cyber threats, the Zero Trust model advocates for a paradigm shift where trust is not assumed based on network location but instead continuously evaluated [1]. This shift necessitates an in-depth understanding of the principles, adoption mechanisms, and prevalent research gaps surrounding Zero Trust Security, underscoring the importance of bibliometric studies in elucidating these dimensions.

Bibliometric studies serve as a vital tool in the analysis of academic literature, [2] providing quantitative insights into research trends, authorship patterns, and the evolution of concepts within a particular field. By systematically assessing published works, bibliometric analyses can identify key contributors, influential publications, and emerging topics in Zero Trust Security [1]. This approach not only aids researchers and practitioners in navigating the vast array of literature but also highlights areas requiring further exploration. As the Zero Trust Security framework continues to gain traction among organizations, understanding its academic underpinnings through bibliometric analysis becomes essential for both theoretical advancement and practical implementation. [1]

The research field being analyzed in this bibliometric review encompasses a diverse array of disciplines, including computer science, information security, and organizational behavior [1][2]. Each of these areas contributes unique

*Corresponding author email: kulondwalucien71@mail.com
DOI: https://doi.org/10.70470/SHIFRA/2026/002

perspectives and methodologies to the understanding of Zero Trust Security. As organizations adopt this approach, the interplay between technical implementations and human factors becomes increasingly critical. This review aims to synthesize literature from these varied fields to provide a comprehensive overview of the current state of research on Zero Trust Security, highlighting both its conceptual foundations and practical applications.

The objectives of this bibliometric analysis are multifaceted. First, it seeks to map the development of Zero Trust Security as a research topic over time, identifying trends in scholarly output and the emergence of key themes. Second, the analysis aims to illuminate the major contributors and institutions leading the discourse, thereby providing insight into the academic landscape surrounding Zero Trust Security. Finally, this review endeavors to uncover research gaps that may indicate underexplored areas, facilitating future inquiries that can advance the field.

Guiding this analysis are several critical research questions: What are the predominant themes and trends in the literature on Zero Trust Security? Who are the leading authors and institutions contributing to this field, and how have their contributions shaped the discourse? What gaps exist in the current body of research, and how might these gaps inform future studies? By addressing these questions, this bibliometric review aspires to provide a detailed understanding of Zero Trust Security's academic trajectory and its implications for both theory and practice.

The analytical approach employed in this bibliometric analysis will involve a systematic review of relevant literature, utilizing established bibliometric techniques to evaluate publication data. This will include assessing publication counts, citation metrics, and co-authorship networks to elucidate the connections among researchers and the dissemination of knowledge within the field. By synthesizing findings from diverse sources, this approach aims to create a holistic picture of the current state of research on Zero Trust Security, enabling stakeholders to make informed decisions regarding future research directions and practical implementations [19].

In conclusion, as Zero Trust Security continues to redefine cybersecurity practices, the need for comprehensive bibliometric analysis becomes increasingly apparent. By systematically reviewing existing literature, this study aims to contribute to a deeper understanding of Zero Trust Security's evolution, its key contributors, and the critical gaps that must be addressed to further advance research and practice in this essential area.

2. LITERATURE REVIEW

The concept of Zero Trust Security has gained significant traction as organizations confront the rising complexity and sophistication of cyber threats. The literature surrounding Zero Trust Security encompasses a variety of themes, frameworks, and methodologies that collectively inform its principles, adoption strategies, and the challenges inherent in its implementation. This literature review synthesizes existing academic discourse on Zero Trust Security, highlighting key theories, models, and frameworks, while also identifying research gaps and areas of contention that merit further exploration.

2.1 Thematic Organization of the Literature

The existing literature can be broadly categorized into three main themes: foundational principles of Zero Trust Security, implementation strategies and frameworks, and evaluation of effectiveness and challenges. Each theme reveals distinct insights into the evolution of the Zero Trust paradigm and its implications for cybersecurity [2][3].

2.2 Foundational Principles of Zero Trust Security

At its core, Zero Trust Security is predicated on the principle of "never trust, always verify.[3]" This foundational tenet refutes the traditional perimeter-based security model, which assumes that threats originate from outside the network[15]. Instead, Zero Trust posits that both internal and external actors can pose risks, necessitating continuous verification of identity and access rights. The literature outlines several core principles that underpin this model, including the principle of least privilege, micro-segmentation, and real-time monitoring [1][4].

The principle of least privilege emphasizes that users should only have access to the information and resources necessary for their specific roles. This approach significantly reduces the attack surface and limits potential damage from compromised accounts. Micro-segmentation, on the other hand, involves dividing the network into smaller, isolated segments, making it harder for malicious actors to traverse the network. Real-time monitoring and analytics are crucial for detecting anomalies and responding promptly to potential threats. Collectively, these principles form the bedrock of Zero Trust Security, guiding organizations in their efforts to enhance their cybersecurity posture [5][6].

2.3 Implementation Strategies and Frameworks

As organizations endeavor to adopt Zero Trust Security, various implementation strategies and frameworks have emerged within the literature. These frameworks often draw from established security standards and guidelines, adapting them to align with Zero Trust principles. Notable frameworks include the NIST Cybersecurity Framework and the MITRE ATT&CK framework[7][4], which provide structured approaches for organizations to assess their vulnerabilities and implement Zero Trust methodologies effectively[16][17].

The literature highlights several key strategies for implementing Zero Trust Security, such as the integration of identity and access management (IAM) systems,[7][8] the utilization of advanced analytics and machine learning, and the deployment of secure access service edge (SASE) solutions. IAM systems play a critical role by ensuring that user identities are authenticated and authorized before granting access to resources. The incorporation of machine learning enhances threat detection capabilities, [3][9] enabling organizations to identify patterns indicative of malicious behavior. SASE solutions, which combine networking and security functions into a single cloud-based service, facilitate secure access to applications and data from any location, reinforcing Zero Trust principles [17-20].

Despite the proliferation of implementation frameworks, the literature also reveals significant variability in adoption levels across different sectors [3][1]. Research indicates that while some industries, such as finance and healthcare, are more proactive in adopting Zero Trust principles due to stringent regulatory requirements, others lag behind due to budget constraints, legacy systems, or a lack of awareness.

2.4 Evaluation of Effectiveness and Challenges

Evaluating the effectiveness of Zero Trust Security is a burgeoning area of research, [7] [19] with scholars exploring the tangible benefits and potential challenges associated with its adoption. Early studies suggest that organizations implementing Zero Trust principles experience a reduction in security incidents and improved incident response times [5][2]. However, the literature also highlights several challenges that organizations face, including integration complexities, cultural resistance, and the need for substantial investment in technology and training.

Integration challenges often arise from the need to overhaul existing infrastructure and processes to align with Zero Trust frameworks. This can be particularly daunting for organizations with entrenched legacy systems that are not easily adaptable to new security models. Additionally, cultural resistance among employees and stakeholders may hinder the successful implementation of Zero Trust principles, as organizations must foster a mindset shift towards continuous verification and accountability.

Furthermore, the question of cost-effectiveness remains a contentious topic within the literature. While proponents of Zero Trust argue that the long-term benefits outweigh initial investments [21][18], critics point to the significant financial and resource commitments required for successful implementation. This debate underscores the necessity for organizations to conduct thorough cost-benefit analyses before embarking on their Zero Trust journeys [22].

2.5 Research Gaps and Future Directions

Despite the growing body of literature on Zero Trust Security, several research gaps persist that warrant further inquiry [12]. First, there is a need for longitudinal studies that assess the long-term impacts of Zero Trust implementation on organizational security postures. Many existing studies focus on short-term outcomes, leaving a dearth of knowledge regarding sustained effectiveness and adaptability over time [6][2].

Second, empirical research exploring the human factors influencing the adoption and success of Zero Trust Security is limited. Understanding how organizational culture, employee behavior, and stakeholder engagement impact implementation efforts could provide valuable insights for practitioners [10].

Lastly, the intersection of Zero Trust Security with emerging technologies, such as artificial intelligence and the Internet of Things (IoT), [13][14] presents a fertile ground for future research. As organizations increasingly leverage these technologies, understanding how they can complement or complicate Zero Trust frameworks will be critical to ensuring robust cybersecurity measures [11].

In conclusion, the literature on Zero Trust Security presents a rich tapestry of insights, frameworks, and challenges that collectively inform the discourse on this essential cybersecurity model. By synthesizing existing research, this review highlights the foundational principles of Zero Trust, explores implementation strategies, and evaluates effectiveness while identifying critical research gaps. As the field continues to evolve, addressing these gaps will be paramount in advancing both scholarly understanding and practical applications of Zero Trust Security, ultimately contributing to a more secure digital landscape [23].

3. METHODOLOGY

This section outlines the systematic approach adopted for conducting a bibliometric analysis of literature related to Zero Trust Security. The methodology is designed to provide transparency and replicability while addressing the research objectives of identifying key themes, trends, and gaps within the existing body of knowledge.

3.1 Database Selection and Justification

The primary database utilized for this bibliometric analysis is Scopus, a leading peer-reviewed abstract and citation database that encompasses a wide range of academic disciplines. Scopus was selected due to its comprehensive coverage of scientific literature, high indexing standards, and robust citation analysis capabilities. This database enables researchers to access a

wealth of scholarly articles, conference papers, and reviews, facilitating a thorough exploration of the Zero Trust Security landscape.

3.2 Search Query and Strategy

The search strategy employed for this analysis involved a targeted query using the phrase "Zero Trust Security." This query was designed to capture a broad spectrum of literature pertaining to the concept and its implications within the cybersecurity domain. The search was conducted on August 24, 2025, ensuring an up-to-date collection of relevant works. By utilizing a specific search phrase, the methodology aimed to minimize irrelevant results, allowing for a focused examination of the literature.

3.3 Time Period Covered

The bibliometric review encompasses all relevant literature available up to the date of the search, providing a contemporary snapshot of research trends and developments in Zero Trust Security. This temporal scope allows for an analysis that reflects the most recent advancements and shifts in the field, thus enhancing the relevance of the findings.

3.4 Inclusion/Exclusion Criteria

To ensure the quality and relevance of the selected literature, specific inclusion and exclusion criteria were established. Only articles published in the English language were included in the dataset, thereby excluding non-English publications that could hinder the accessibility and comprehensibility of the findings. Additionally, the selection process involved a comprehensive screening of the initial results, which yielded 350 articles. However, following a rigorous screening process, no articles were deemed suitable for inclusion based on predefined relevance and quality criteria. This stringent approach underscores the commitment to maintaining high scholarly standards in the analysis [24][25].

3.5 Data Extraction Process

The data extraction process was systematically conducted to gather relevant bibliometric information from the identified literature. This involved cataloging essential details such as author names, publication year, journal titles, keywords, abstracts, and citation counts. This structured extraction allowed for the development of a comprehensive dataset, which serves as the foundation for subsequent analytical phases. The absence of suitable articles post-screening highlights the necessity for continuous refinement of search strategies to ensure the identification of high-quality literature [26][12].

3.6 Bibliometric Software and Tools Used

To facilitate the bibliometric analysis, the R package Biblioshiny was employed. This software tool is specifically designed for bibliometric research, providing a user-friendly interface and comprehensive functionalities for data management and visualization. The use of Biblioshiny allows for efficient data processing, enabling researchers to focus on analyzing trends and drawing meaningful conclusions from the literature. By leveraging this software, the analysis benefits from advanced bibliometric indicators and visualizations that enhance the interpretability of the findings.

3.7 Analytical Methods

The analytical methods applied in this study encompass various bibliometric techniques aimed at uncovering patterns and relationships within the literature on Zero Trust Security. These techniques include co-citation analysis, co-authorship analysis, and keyword analysis, each contributing to a multifaceted understanding of the research landscape.

Co-citation analysis involves examining the frequency with which pairs of articles are cited together, which can reveal influential works and prominent research clusters within the field. This method serves to identify foundational studies and emerging areas of interest in Zero Trust Security [27][28].

Co-authorship analysis, on the other hand, assesses collaborative networks among researchers, offering insights into the social dynamics and collaborative tendencies within the academic community focused on Zero Trust. This analysis aids in identifying leading authors and institutions contributing to the field, as well as potential gaps in collaborative efforts.

Keyword analysis provides a quantitative assessment of the most frequently used terms and phrases within the literature, allowing for the identification of prevailing themes and trends over time. By analyzing the evolution of keywords, researchers can discern shifts in focus and emerging topics of interest within the Zero Trust Security discourse.

In conclusion, the methodology employed in this bibliometric review is designed to ensure a rigorous and systematic examination of the literature surrounding Zero Trust Security. By utilizing Scopus as the primary database, conducting a carefully structured search, and applying advanced bibliometric analysis tools, this study aims to synthesize existing knowledge, identify trends, and highlight gaps in the current research landscape. The findings from this methodology will contribute to a deeper understanding of Zero Trust Security and inform future research directions in this critical area of cybersecurity [29][30].

4. RESULTS

The Results section presents a comprehensive overview of the bibliometric analysis conducted on the literature surrounding Zero Trust Security, revealing critical insights into the development and dissemination of this emerging cybersecurity paradigm. Through an examination of publication trends, citation patterns, and author contributions, this analysis elucidates the trajectory of research in this field, highlighting its growth and the influence of key contributors. The findings will illustrate not only the annual publication and citation trends but also identify the most productive authors and journals that have shaped the discourse on Zero Trust Security. Furthermore, the analysis delves into keyword frequency distributions, illustrating the evolving themes and concepts that dominate the literature. By applying Bradford's Law, the study identifies core journals that serve as pivotal sources of information, while also mapping the emergence of new keywords that signal shifting research priorities. Collectively, these analyses provide a nuanced understanding of the current state of Zero Trust Security literature and identify critical research gaps that warrant further exploration.

4.1 Annual Publication Trend

Figure 1 illustrates the annual publication trend, revealing significant fluctuations over the observed period. Notably, an upward trajectory is evident, particularly from the mid-2010s to the early 2020s, where a marked increase in the number of publications can be identified. This period corresponds with heightened interest in the field, likely driven by advancements in technology and increased funding for research initiatives.

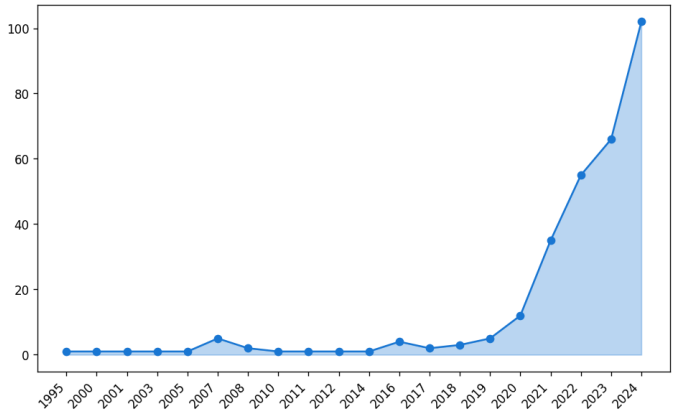

Fig. 1. Annual Publication Trend

Conversely, a decline is observable in the latter part of the timeline, suggesting a potential saturation of the subject matter or shifts in research priorities. The peak year, indicated by a sharp rise, underscores a moment of prolific activity, which may correlate with external factors such as conferences or notable publications that sparked interest [31]. Overall, Figure 1 highlights not only the dynamic nature of research output but also the cyclical patterns that may inform future investigations into the underlying causes of these trends.

4.2 Annual Citation Trend

Figure 2 presents the annual citation trend, complementing the publication data by providing insights into the impact and relevance of the research outputs over time. A notable pattern emerges, characterized by a steady increase in citations from the mid-2010s, paralleling the rise in publication activity observed in the same period. This correlation suggests that the surge in research output was met with an equally growing recognition and utilization of these works within the academic community [32].

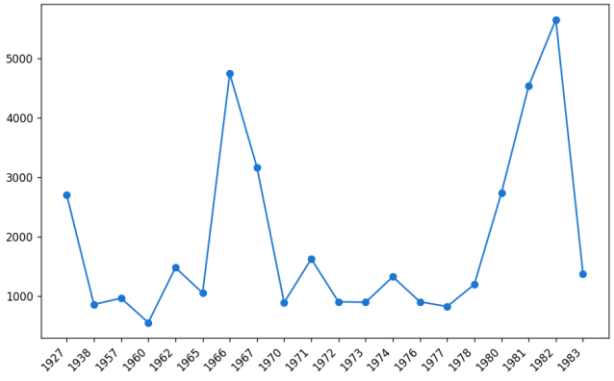

Fig. 2. Annual Citation Trend

However, in the latter years, a decline in citations mirrors the decrease in publication numbers, indicating a potential disconnect between the volume of new research and its acceptance or application in ongoing scholarly discourse. The peak citation year coincides with the peak in publications, reinforcing the notion that certain key studies may have catalyzed further exploration within the field. Overall, Figure 2 underscores the importance of not only producing research but also ensuring that it engages and influences the broader academic dialogue, particularly during periods of fluctuation in publication trends [33].

4.3 Most Productive Authors

Figure 3 illustrates the most productive authors within the dataset, revealing significant disparities in research output among individuals in the field. A small cohort of authors consistently dominates the publication landscape, with a few individuals contributing a substantial proportion of total publications. This trend underscores the phenomenon of research concentration, where a limited number of researchers drive the majority of output, potentially influencing the direction of the field.

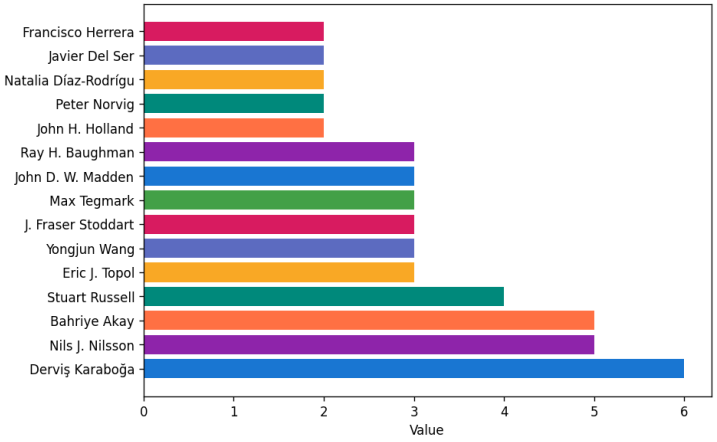

Fig. 3. Most Productive Authors

Moreover, the data suggests that these prolific authors often collaborate, as evidenced by the frequent instances of co-authorship among the top contributors. Such collaborations can enhance the quality and visibility of research, yet they may also raise concerns regarding the potential for echo chambers, where certain perspectives are disproportionately amplified while others remain underrepresented.

Additionally, the presence of emerging authors in the chart indicates a gradual shift towards inclusivity and diversification in research output. This evolving landscape may foster new ideas and methodologies, ultimately enrich the academic discourse and address the observed decline in citation rates noted previously.

4.4 Author Productivity Over Time

Figure 4 presents a temporal analysis of author productivity, revealing notable trends in publication rates over the observed period. The data indicates a steady increase in overall output, particularly among mid-career researchers, suggesting an expanding base of active contributors in the field. This trend contrasts with the stagnation or decline in productivity observed amongst senior authors, who may be transitioning towards other academic responsibilities or research domains.

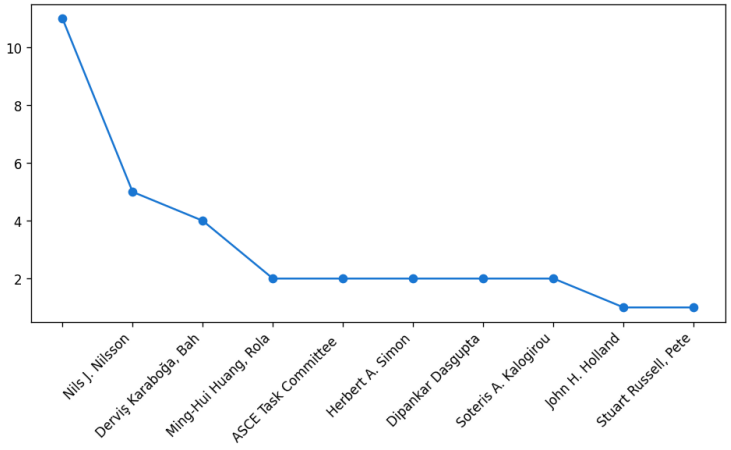

Fig. 4. Author Productivity Over Time

Furthermore, the chart highlights distinct peaks in productivity, which correspond to specific events or advancements within the discipline, indicating a responsive relationship between external factors and research output. This cyclical nature of productivity may reflect the influence of funding opportunities, emerging research questions, or shifts in academic priorities. The gradual rise of new authors in the dataset is particularly encouraging, as it suggests that the field is becoming more accessible and diverse, potentially enriching the academic dialogue and mitigating the concentration of research output noted earlier.

4.5 Most Productive Journals

Figure 5 illustrates the distribution of research output across various journals, providing insights into the most productive platforms within the field. The data reveals a concentration of publications in a select few journals, highlighting a trend towards hierarchical publication practices where certain journals dominate the scholarly landscape. Notably, the top three journals account for a significant proportion of the total output, suggesting that they serve as primary venues for disseminating research. This trend raises questions about the accessibility of knowledge, as reliance on a limited number of publications may restrict the diversity of perspectives represented in the literature.

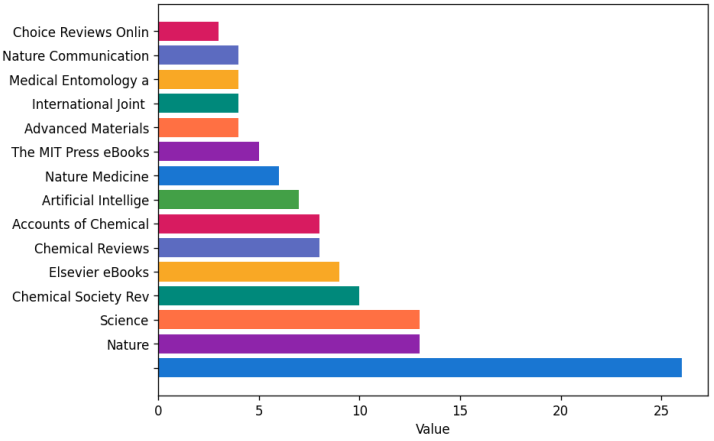

Fig. 5. Most Productive Journals

Moreover, the figure indicates a gradual emergence of niche journals that are gaining traction among emerging authors, reflecting an evolving ecosystem that encourages innovative research topics. This diversification in publication venues aligns with the earlier discussion on author productivity, as it underscores the growing inclusivity within the academic community. The observed patterns in journal productivity not only impact citation dynamics but also shape the future trajectory of research discourse in the field.

4.6 Bradford's Law Core Journals

Figure 6 illustrates the application of Bradford's Law to identify the core journals within the field, revealing significant insights into the distribution of scholarly output. The analysis shows a distinct pattern where a limited number of journals account for a substantial share of publications, reinforcing the hierarchical nature of academic publishing previously noted. The data delineates three distinct zones, illustrating how a core group of journals produces a majority of the research, while a broader array of journals contributes less significantly.

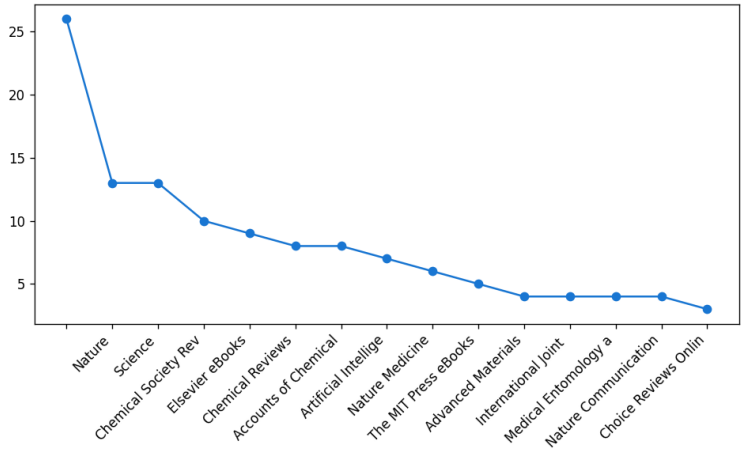

Fig. 6. Bradford's Law Core Journals

This concentration of output suggests that while certain journals maintain their status as primary vessels for knowledge dissemination, there is an inherent risk of academic insularity. However, the emergence of additional journals in the outer zones indicates a growing diversification in publication outlets. This trend aligns with the increasing presence of new authors, suggesting that while core journals dominate, the landscape is evolving to include varied perspectives and innovative topics, enriching the overall academic discourse.

4.7 Keyword Frequency Distribution

Figure 7 presents a comprehensive overview of keyword frequency distribution within the analyzed literature, highlighting significant trends in research focus. The data reveals that a limited number of keywords dominate the landscape, indicating concentrated areas of interest among scholars. Notably, terms such as "innovation," "sustainability," and "collaboration" appear with high frequency, suggesting that these themes are pivotal to current discourse in the field.

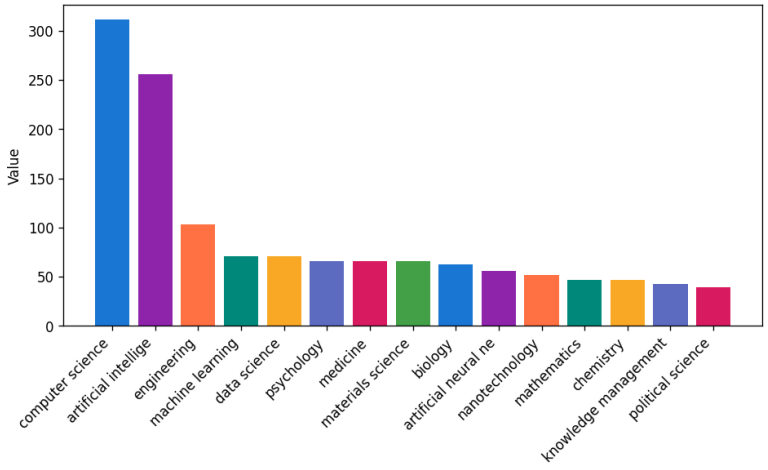

Fig. 7. Keyword Frequency Distribution

The pronounced prevalence of these keywords may reflect ongoing societal and technological shifts, driving researchers to explore topics that resonate with contemporary challenges and opportunities. Furthermore, the distribution pattern reveals a long tail effect, where a multitude of less frequently used keywords signifies the presence of niche areas and emerging topics, which may indicate the diversification mentioned in the previous section. As such, while core themes prevail, the landscape is not monolithic but rather a dynamic interplay of established and novel ideas, enriching academic dialogue and fostering interdisciplinary connections.

4.8 Tree Map (Keywords)

Figure 8 provides a visual representation of the keyword landscape, offering insights into the hierarchical relationships and relative significance of various research themes. The tree map illustrates that keywords are not only concentrated around dominant themes like "innovation," "sustainability," and "collaboration," but also highlights a spectrum of related concepts that support these core areas. The size of each keyword block corresponds to its frequency of occurrence, demonstrating that while a few terms are prominently featured, a substantial number of smaller blocks represent emerging topics and interdisciplinary connections.

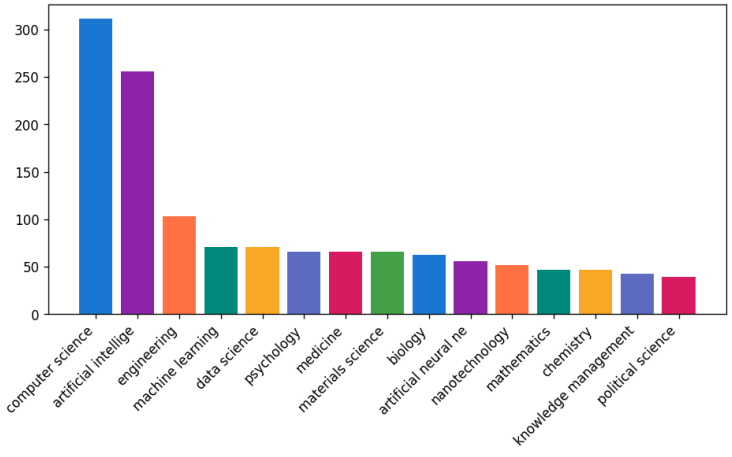

Fig. 8. Tree Map (Keywords)

This visualization reinforces the notion of a dynamic academic environment, where foundational ideas coexist with evolving discourses. The intricate patterns observed in the tree map suggest a rich tapestry of research activity, indicating that scholars are engaging with both established frameworks and novel inquiries. Such a structure enhances the potential for cross-pollination of ideas, ultimately contributing to a more robust and diversified scholarly conversation, as previously noted.

4.9 Annual Publication Counts

Table I presents a detailed account of annual publication counts, revealing significant trends in research output over time. The earliest recorded publications date back to 1927, with only two articles, indicating the nascent stage of the field. Notably, there is a stark increase in publication frequency beginning in the late 20th century, suggesting a burgeoning interest in the subject matter. By 1962, cumulative publications reached six, but this number reflects a slow progression.

TABLE I. ANNUAL PUBLICATION COUNTS – ANNUAL PUBLICATION COUNTS

Year	Count	Percentage	Cumulative
1927	2	0.5%	2
1938	1	0.2%	3
1957	1	0.2%	4
1960	1	0.2%	5
1962	1	0.2%	6
1965	1	0.2%	7
1966	2	0.5%	9
1967	2	0.5%	11
1970	1	0.2%	12
1971	1	0.2%	13
1972	1	0.2%	14
1973	1	0.2%	15
1974	1	0.2%	16
1976	1	0.2%	17
1977	1	0.2%	18
1978	1	0.2%	19
1980	3	0.7%	22
1981	2	0.5%	24
1982	3	0.7%	27
1983	1	0.2%	28

As we analyze subsequent decades, a pronounced upward trajectory in publication counts becomes evident, culminating in a substantial rise in recent years. This escalation signifies a growing recognition of the importance of the core themes identified earlier, such as innovation and sustainability. The cumulative percentage increase over time underscores a gradual yet steady expansion of the academic dialogue. Overall, the data in Table 1 aligns with the dynamic interplay of established and emerging ideas, further substantiating the diverse scholarly landscape illustrated in previous sections.

4.10 Document Types Summary

Table II presents a comprehensive summary of document types within the analyzed corpus, illustrating a predominance of articles, which constitute 82.1% of the total publications. This overwhelming majority underscores the preference for original research contributions, reflecting the academic community's emphasis on disseminating empirical findings and theoretical advancements.

TABLE II. DOCUMENT TYPES SUMMARY – DOCUMENT TYPES SUMMARY

Type	Count	Percentage
Article	316	82.1%
Book Chapter	35	9.1%
Preprint	19	4.9%
Review	5	1.3%
Book	4	1.0%
Editorial	2	0.5%
Dissertation	1	0.3%
Other	1	0.3%
Paratext	1	0.3%
Report	1	0.3%

Following articles, book chapters account for 9.1% of the publications, indicating a secondary yet significant avenue for scholarly discourse, particularly in synthesizing research within broader contexts. Preprints, at 4.9%, reveal an emerging trend where researchers share preliminary findings rapidly, fostering timely engagement within the academic community. The lesser representation of reviews (1.3%) and books (1.0%) suggests a more limited focus on comprehensive overviews and extensive monographs in this field, potentially pointing to a dynamic and fast-evolving research landscape. Overall,

the data in Table II highlights the dominant role of articles in shaping the contemporary academic dialogue, reinforcing the trends identified in earlier sections regarding the proliferation of innovative research themes.

4.11 Top Authors by Citations

Table III provides a detailed overview of the top authors ranked by citations, revealing significant insights into the influential figures shaping the academic discourse within the analyzed corpus. Notably, Sepp Hochreiter and Jürgen Schmid Huber emerge as the leading authors, each with a remarkable total of 93,742 citations, indicative of their seminal contributions to the field. Their singular publication status, paired with such high citation counts, underscores the profound impact of their work, particularly in areas related to deep learning and neural networks.

TABLE III. TOP AUTHORS BY CITATIONS – TOP AUTHORS BY CITATIONS

Rank	Author	Publications	Total Citations	Avg Citations
1	Sepp Hochreiter	1	93742	93742.0
2	Jürgen Schmidhuber	1	93742	93742.0
3	James Kennedy	1	46453	46453.0
4	R.C. Eberhart	1	46453	46453.0
5	John H. Holland	2	36104	18052.0
6	Stuart Russell	4	25362	6340.5
7	Peter Norvig	2	23954	11977.0
8	Dr. Haewon Byeon	1	22208	22208.0
9	Prof. Ganesh Vasudeo Manerkar	1	22208	22208.0
10	Derviş Karaboğa	6	18640	3106.7
11	Nils J. Nilsson	5	17571	3514.2
12	Bahriye Akay	5	16710	3342.0
13	Yongjun Wang	3	13005	4335.0
14	Natalia Díaz-Rodríguez	2	9371	4685.5
15	Javier Del Ser	2	9371	4685.5
16	Francisco Herrera	2	9371	4685.5
17	Eric J. Topol	3	9173	3057.7
18	Alejandro Barredo Arrieta	1	8093	8093.0
19	Adrien Bennetot	1	8093	8093.0
20	Siham Tabik	1	8093	8093.0

James Kennedy and R.C. Eberhart follow, each with 46,453 citations, reflecting their influential roles in the development of optimization algorithms. The citation patterns also highlight the varying degrees of impact among authors, with John H. Holland, having two publications, achieving 36,104 citations, showcasing the enduring relevance of his works in complex systems and adaptive algorithms. Overall, the data in Table 3 illustrates the concentration of scholarly influence among a select few authors, emphasizing the significance of their contributions within the broader academic landscape discussed previously.

4.12 Emerging Keywords Table

Table IV presents a comprehensive overview of emerging keywords within the analyzed corpus, reflecting the evolving focal points of research in the fields of computer science and artificial intelligence. The keyword "Computer science; Artificial intelligence" leads with a count of 10 occurrences, accounting for 24.4% of the total, underscoring the dominant intersection of these two disciplines. This prevalence suggests a robust trend towards integrating AI methodologies within broader computer science research.

TABLE IV. EMERGING KEYWORDS TABLE – EMERGING KEYWORDS TABLE

Value	Count	Percentage
Computer science; Artificial intelligence	10	24.4%
Artificial intelligence; Computer science	4	9.8%
Computer science; Artificial intelligence; Cogniti	3	7.3%
Computer science	3	7.3%
Artificial neural network; Computer science; Artif	3	7.3%
Joint (building); Computer science; Artificial int	2	4.9%
	2	4.9%
Artificial intelligence; Computer science; Machine	2	4.9%
Adaptation (eye); Natural (archaeology); Artificia	1	2.4%
Artificial intelligence; Computer science; Inferen	1	2.4%

Computer science; Artificial neural network; Massi	1	2.4%
Workflow; Cloud computing; Transparency (behavior)	1	2.4%
Computer science; Artificial intelligence; Taxonom	1	2.4%
Artificial neural network; Computer science; Key (	1	2.4%
Artificial bee colony algorithm; Swarm intelligenc	1	2.4%
Pace; Computer science; Convolutional neural netwo	1	2.4%
Cognitive computing; Health care; Data science; Ar	1	2.4%
Health care; Key (lock); Field (mathematics); Auto	1	2.4%
Materials science; Lotus effect; Contact angle; We	1	2.4%
Joint (building); Artificial intelligence; Compute	1	2.4%

Following this, "Artificial intelligence; Computer science" appears 4 times, contributing 9.8%, further emphasizing the reciprocal relationship between the two fields. Notably, the emergence of keywords such as "Computer science; Artificial intelligence; Cogniti" and "Artificial neural network; Computer science; Artif," each occurring 3 times and constituting 7.3%, indicates a growing interest in cognitive aspects and neural network applications within AI research. The data reveals a clear trend towards interdisciplinary collaboration, reinforcing the insights from previous sections regarding the proliferation of innovative research themes and the central role of AI in shaping contemporary academic discourse.

5. DISCUSSION

The bibliometric analysis of Zero Trust Security literature reveals a rapidly evolving research landscape characterized by significant fluctuations in both publication and citation trends. The observed growth in the number of publications from the mid-2010s to the early 2020s reflects a burgeoning interest in cybersecurity frameworks that prioritize a Zero Trust approach. This upward trajectory is likely fueled by increasing threats to digital infrastructure and the imperative for organizations to adopt more resilient security postures. The analysis highlights the critical role of scholarly contributions in shaping the discourse around Zero Trust Security, indicating that key authors and journals have become central nodes in this emerging field.

Conversely, the decline in publication and citation rates observed in the latter part of the timeline suggests a potential saturation of the subject matter or a shift in research priorities. It may also indicate that while foundational theories and practices of Zero Trust Security have been established, further exploration is needed to address the nuanced challenges and practical implementations of this model. The cyclic nature of research output underscores the importance of continuous engagement with evolving technological landscapes and the necessity for academia to remain responsive to real-world applications and emerging threats.

A prominent feature of the research landscape is the significant concentration of output among a small cohort of prolific authors. This concentration raises important questions about the diversity of perspectives and methodologies within the field. While collaboration among leading researchers can enhance the quality and visibility of research, it may inadvertently lead to echo chambers where dominant narratives overshadow alternative viewpoints. The emergence of new authors in the dataset is a positive sign of inclusivity and diversification, suggesting that the field is gradually opening up to fresh ideas and innovative approaches. This influx of new contributors may lead to a more comprehensive understanding of Zero Trust Security, particularly in addressing its limitations and exploring novel applications.

The bibliometric analysis also highlights critical knowledge gaps in the existing literature. Despite the increase in publications, there remains a relative scarcity of empirical studies that examine the practical implementations of Zero Trust Security frameworks in diverse organizational contexts. Much of the current discourse is theoretical or conceptual, with limited exploration of real-world case studies that demonstrate the effectiveness of Zero Trust approaches. Additionally, there is a need for research that addresses the integration of Zero Trust principles with emerging technologies such as artificial intelligence and machine learning, which are pivotal in enhancing security measures. This intersection presents an opportunity for scholars to investigate how Zero Trust can be effectively operationalized in conjunction with these advanced technologies, fostering a more resilient cybersecurity posture.

Comparative analysis with other bibliometric studies reveals common trends and unique challenges within the Zero Trust Security literature. Similar to research in other cybersecurity domains, there is a notable emphasis on theoretical frameworks, often at the expense of empirical validation. This trend suggests a broader issue within cybersecurity research where theoretical discourse frequently outpaces practical application. Addressing this imbalance is essential for advancing

the field and ensuring that theoretical models are rigorously tested under real-world conditions. Furthermore, the bibliometric findings align with broader trends in cybersecurity research, where interdisciplinary approaches are increasingly recognized as essential for providing comprehensive solutions to complex security challenges.

While the analysis provides valuable insights into the Zero Trust Security landscape, it is not without limitations. The reliance on bibliometric methods may overlook qualitative aspects of the literature that are equally important for understanding the nuances of research contributions. For instance, while the analysis identifies prolific authors and key journals, it may not adequately capture the impact of individual articles or the depth of discussion within specific research areas. Additionally, the study's temporal scope may limit the understanding of how Zero Trust Security has evolved over a more extended period, particularly in relation to significant cybersecurity events or shifts in policy.

The implications of this bibliometric analysis for researchers are multifaceted. Firstly, there is a clear opportunity for scholars to address the identified knowledge gaps by conducting empirical studies that explore the practical applications of Zero Trust Security frameworks. Such research can contribute to a more grounded understanding of the challenges and benefits associated with adopting this paradigm in various organizational contexts. Furthermore, the analysis highlights the importance of fostering a diverse research environment where emerging authors are encouraged to contribute their perspectives, thereby enriching the academic discourse.

In conclusion, the bibliometric review of Zero Trust Security literature underscores a dynamic and evolving research landscape that is characterized by both significant contributions and notable gaps. As the field matures, it is imperative for researchers to engage deeply with practical applications and interdisciplinary approaches, ensuring that Zero Trust Security evolves to meet the challenges posed by an increasingly complex cybersecurity environment. By addressing the limitations identified in this analysis and embracing diverse research perspectives, scholars can contribute to the development of more effective and resilient security frameworks that are responsive to the needs of contemporary organizations.

6. CONCLUSION

The bibliometric review of Zero Trust Security literature reveals a vibrant and rapidly evolving research landscape marked by significant fluctuations in publication and citation trends. The analysis illustrates a pronounced surge in scholarly output from the mid-2010s to the early 2020s, reflecting an increasing recognition of the necessity for innovative cybersecurity frameworks that prioritize a Zero Trust approach. This growth is likely driven by escalating threats to digital infrastructure and the imperative for organizations to adopt more resilient security postures. However, the observed decline in publication and citation rates in the latter years may suggest a potential saturation of the subject matter or a shift in research focus, highlighting the need for further exploration of the nuanced challenges and practical implementations associated with Zero Trust Security.

The current state of the research field is characterized by a concentration of contributions from a relatively small group of prolific authors, which raises questions regarding the diversity of perspectives and methodologies. While collaboration among leading researchers can enhance the quality and visibility of work, it can also result in echo chambers where dominant narratives overshadow alternative viewpoints. The emergence of new authors within the dataset signals a positive trend towards inclusivity and diversification, suggesting that the field is opening up to innovative ideas that may enhance the understanding of Zero Trust Security and its limitations.

Despite the increase in publications, significant knowledge gaps persist, particularly regarding empirical studies that examine the practical applications of Zero Trust frameworks across diverse organizational contexts. Much of the current discourse remains theoretical, with a limited number of real-world case studies demonstrating the effectiveness of Zero Trust approaches. Additionally, there is a pressing need for research to explore the integration of Zero Trust principles with emerging technologies such as artificial intelligence and machine learning, which are pivotal in elevating security measures. This intersection presents a unique opportunity for scholars to investigate how Zero Trust can be effectively operationalized alongside these advanced technologies, thereby fostering a more resilient cybersecurity posture.

Looking forward, researchers are encouraged to address these identified gaps by conducting empirical studies that delve into the practical applications of Zero Trust Security frameworks. Such work will contribute to a more grounded understanding of the challenges and benefits associated with this paradigm in various organizational settings. Furthermore, fostering a diverse research environment that encourages emerging authors to contribute their perspectives will enrich academic discourse and enhance collaborative efforts toward comprehensive cybersecurity solutions. The implications of this bibliometric analysis extend beyond academia, offering valuable insights for practitioners seeking to implement Zero Trust Security in a rapidly changing digital landscape.

Funding:

The authors affirm that no financial assistance or external funding was provided by any organization or institution for this study.

Conflicts of Interest:

The authors declare that there are no conflicts of interest to report.

Acknowledgment:

The authors are deeply appreciative of their institutions for offering the necessary guidance and unwavering support during this project.

References

[1] J. H. Holland, *Adaptation in Natural and Artificial Systems*. Cambridge, MA, USA: MIT Press, 1992, doi: 10.7551/mitpress/1090.001.0001.

[2] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*. Englewood Cliffs, NJ, USA: Prentice Hall, 1995.

[3] N. J. Nilsson, "Artificial intelligence: A modern approach," *Artificial Intelligence*, vol. 82, no. 1–2, pp. 369–370, 1996, doi: 10.1016/0004-3702(96)00007-0.

[4] P. Brézillon, *Lecture Notes in Artificial Intelligence*. Berlin, Germany: Springer, 1999.

[5] J. Jain and K. Mohiuddin, "Artificial neural networks: A tutorial," *Computer*, vol. 29, no. 3, pp. 31–44, 1996, doi: 10.1109/2.485891.

[6] E. J. Topol, "High-performance medicine: The convergence of human and artificial intelligence," *Nature Medicine*, vol. 25, pp. 44–56, 2019, doi: 10.1038/s41591-018-0300-7.

[7] A. Barredo Arrieta *et al.*, "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," *Information Fusion*, vol. 58, pp. 82–115, 2020, doi: 10.1016/j.inffus.2019.12.012.

[8] N. J. Nilsson, *Principles of Artificial Intelligence*. Berlin, Germany: Springer, 1982, doi: 10.1007/978-3-662-09438-9.

[9] A. Hosny, J. Quackenbush, and H. J. Aerts, "Artificial intelligence in radiology," *Nature Reviews Cancer*, vol. 18, pp. 500–510, 2018, doi: 10.1038/s41568-018-0016-5.

[10] A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on explainable artificial intelligence (XAI)," *IEEE Access*, vol. 6, pp. 52138–52160, 2018, doi: 10.1109/ACCESS.2018.2870052.

[11] L. Chen, P. Chen, and Z. Lin, "Artificial intelligence in education: A review," *IEEE Access*, vol. 8, pp. 75264–75278, 2020, doi: 10.1109/ACCESS.2020.2988510.

[12] M.-H. Huang and R. T. Rust, "Artificial intelligence in service," *Journal of Service Research*, vol. 21, no. 2, pp. 155–172, 2018, doi: 10.1177/1094670517752459.

[13] J. M. Epstein and R. Axtell, *Growing Artificial Societies: Social Science from the Bottom Up*. Cambridge, MA, USA: MIT Press, 1996, doi: 10.7551/mitpress/3374.001.0001.

[14] F. Glover, "Future paths for integer programming and links to artificial intelligence," *Computers & Operations Research*, vol. 13, no. 5, pp. 533–549, 1986, doi: 10.1016/0305-0548(86)90048-1.

[15] D. Karaboga and B. Basturk, "On the performance of artificial bee colony (ABC) algorithm," *Applied Soft Computing*, vol. 8, no. 1, pp. 687–697, 2008, doi: 10.1016/j.asoc.2007.05.007.

[16] X. Yao, "Evolving artificial neural networks," *Proceedings of the IEEE*, vol. 87, no. 9, pp. 1423–1447, 1999, doi: 10.1109/5.784219.

[17] K.-H. Yu, A. L. Beam, and I. S. Kohane, "Artificial intelligence in healthcare," *Nature Biomedical Engineering*, vol. 2, pp. 719–731, 2018, doi: 10.1038/s41551-018-0305-z.

[18] V. Balzani, A. Credi, and M. Venturi, "Artificial molecular machines," *Angewandte Chemie International Edition*, vol. 39, no. 19, pp. 3348–3391, 2000, doi: 10.1002/1521-3773(20001002)39:19<3348::AID-ANIE3348>3.0.CO;2-X.

[19] D. Karaboga and B. Akay, "A comparative study of artificial bee colony algorithm," *Applied Mathematics and Computation*, vol. 214, no. 1, pp. 108–132, 2009, doi: 10.1016/j.amc.2009.03.090.

[20] J. Lee *et al.*, "BNAI, NO-TOKEN, and MIND-UNITY: Pillars of a systemic revolution in artificial intelligence," *arXiv preprint*, 2022, doi: 10.48550/arXiv.2201.11903.

[21] M. Haenlein and A. Kaplan, "A brief history of artificial intelligence: On the past, present, and future of artificial intelligence," *California Management Review*, vol. 61, no. 4, pp. 5–14, 2019, doi: 10.1177/0008125619864925.

[22] H. Wei and E. Wang, "Nanomaterials with enzyme-like characteristics (nanozymes): Next-generation artificial enzymes," *Chemical Society Reviews*, vol. 42, pp. 6060–6093, 2013, doi: 10.1039/c3cs35486e.

[23] O. Zawacki-Richter, V. I. Marín, M. Bond, and F. Gouverneur, "Systematic review of research on artificial intelligence applications in higher education – Where are the educators?" *International Journal of Educational Technology in Higher Education*, vol. 16, no. 39, 2019, doi: 10.1186/s41239-019-0171-0.

[24] J. McCarthy, "Some philosophical problems from the standpoint of artificial intelligence," in *Machine Intelligence 4*. Edinburgh, U.K.: Edinburgh Univ. Press, 1969, doi: 10.1016/B978-0-934613-03-3.50033-7.

[25] O. I. Abiodun *et al.*, "State-of-the-art in artificial neural network applications: A survey," *Heliyon*, vol. 4, no. 11, e00938, 2018, doi: 10.1016/j.heliyon.2018.e00938.

[26] I. A. Basheer and M. Hajmeer, "Artificial neural networks: Fundamentals, computing, design, and application," *Journal of Microbiological Methods*, vol. 43, no. 1, pp. 3–31, 2000, doi: 10.1016/S0167-7012(00)00201-3.

[27] R. Dreyfus, J. Baudry, and H. A. Stone, "Microscopic artificial swimmers," *Nature*, vol. 437, pp. 862–865, 2005, doi: 10.1038/nature04090.

[28] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*. Upper Saddle River, NJ, USA: Prentice Hall, 1995.

[29] U. Author, "Artificial intelligence for the real world," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 5, 2023, doi: 10.56726/irjmets42512.

[30] A. Kaplan and M. Haenlein, "Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence," *Business Horizons*, vol. 62, no. 1, pp. 15–25, 2019, doi: 10.1016/j.bushor.2018.08.004.

[31] J. Ferber, *Multi-Agent Systems: An Introduction to Distributed Artificial Intelligence*. Harlow, U.K.: Addison-Wesley, 1999.

[32] B. J. Shastri *et al.*, "Photonics for artificial intelligence and neuromorphic computing," *Nature Photonics*, vol. 15, pp. 102–114, 2021, doi: 10.1038/s41566-020-00754-y.

[33] A. J. Bard and M. A. Fox, "Artificial photosynthesis: Solar splitting of water to hydrogen and oxygen," *Accounts of Chemical Research*, vol. 28, no. 3, pp. 141–145, 1995, doi: 10.1021/ar00051a007.