Integrating Cybersecurity and Risk Management: A Holistic Approach to Digital Threat Mitigation

Sandhya Dahake; Mayur Kule; Kalyani Vaidya
Department of Master in Computer Application
G H Raisoni College of Engineering & Management Nagpur, Maharashtra, India

Abstract
The rapid evolution of digital threats necessitates the integration of cybersecurity and risk management to enhance organizational resilience [9]. This review explores the convergence of these domains, emphasizing their role in mitigating cyber risks. By analysing literature from 2015 to 2025 using bibliometric methods, this study identifies key trends, research gaps, and emerging frameworks. Data was collected from Scopus, Web of Science, and IEEE Xplore, applying strict inclusion criteria to peer-reviewed articles. Findings reveal a growing focus on AI-driven risk assessment, regulatory compliance, and cyber resilience strategies. However, gaps remain in real-time risk mitigation and adaptive security models. Existing studies lack comprehensive, interdisciplinary approaches, highlighting the need for further empirical validation. This paper proposes future research directions, emphasizing dynamic risk frameworks, human-centric security models, and sustainable cybersecurity strategies. The study contributes by mapping the research landscape and recommending an integrated approach for enhanced digital threat management.

Keywords: Cybersecurity, Risk Management, Data Privacy, Threat Mitigation Strategies, Cyber Risk Assessment.

1. Introduction

Inan increasingly digital world, organizations face a growing number of cyber threats that pose significant risks to their operations, reputation, and financial stability [12]. Traditional cybersecurity measures alone are no longer sufficient to address the evolving landscape of cyber risks [1]. Instead, a holistic approach that integrates cybersecurity and risk management is essential to enhance digital resilience. This integration enables organizations to proactively assess, mitigate, and respond to cyber threats while ensuring compliance with regulatory frameworks and industry standards. This paper explores the intersection of cybersecurity and risk management, emphasizing the need for a strategic, multi-layered approach to digital threat mitigation.

1.1 The Growing Importance of Cybersecurity In Risk Management

Cybersecurity has transitioned from being a purely technical issue to a critical component of overall risk management. Organizations must recognize cyber threats as fundamental business risks rather than just IT concerns [2]. The integration of cybersecurity into risk management involves assessing vulnerabilities, implementing preventive measures, and establishing rapid response mechanisms [14].

KeyFactorsDrivingTheNeedforIntegratio:

- Increasing Sophistication of Cyber Threats: Cyberattacks have evolved, leveraging AI, ransomware, and social engineering techniques to exploit vulnerabilities.
- Regulatory Compliance: Governments and industry bodies enforce cybersecurity regulations, making risk management essential for legal and ethical compliance.

DOI: https://doi.org/10.5281/zenodo.15469902

- Financial and Reputational Impact: A successful cyberattack can result in financial losses, data breaches, and reputational damage, affecting stakeholder trust.
- Remote Work and Cloud Adoption: The expansion of digital work environments has introduced new vulnerabilities, requiring stronger security frameworks.

1.2 Challenges In Implementing An Integrated Approach

Despite the recognized benefits, integrating cybersecurity and risk management presents several challenges. Organizations often struggle with aligning their cybersecurity strategies with broader risk management frameworks.

Major Challenges:

- Lack of Skilled Professionals: There is a shortage of cybersecurity and risk management experts, making it difficult to implement comprehensive security strategies.
- Fragmented Security Policies: Many organizations operate in silos, leading to inconsistent cybersecurity measures across departments.
- Cost Constraints: Implementing robust cybersecurity and risk management frameworks requires significant financial investment [21].
- Evolving Threat Landscape: Cyber threats continuously evolve, making it challenging to develop long-term risk mitigation strategies.

Overcoming these challenges requires organizations to adopt a proactive and adaptive approach, leveraging emerging technologies and best practices.

1.3 Strategies For A Holistic Cybersecurity And Risk Management Framework

A well-structured framework that integrates cybersecurity and risk management can significantly enhance an organization's ability to mitigate digital threats [3].

Key Strategies for Effective Integration:

Risk-Based Cybersecurity Approach: Organizations should assess cyber risks based on their impact and likelihood, prioritizing high-risk areas.

- AI and Automation in Threat Detection: Advanced technologies such as artificial intelligence and machine learning can enhance threat detection and response mechanisms.
- Zero-Trust Security Model: Implementing a zero-trust approach ensures continuous verification of users and devices before granting access [16].
- Continuous Monitoring and Incident Response: Regular risk assessments, penetration testing, and real-time threat intelligence help in early threat detection.
- Employee Awareness and Training: Human error remains a major cybersecurity risk. Regular training programs can help employees recognize and prevent cyber threats.
- By integrating these strategies, organizations can build a resilient cybersecurity posture that aligns with their overall risk management objectives, ensuring long-term security and sustainability.

2. Literature Review

The integration of cybersecurity and risk management has gained significant attention due to the increasing complexity of cyber threats. Existing literature highlights various frameworks, methodologies, and challenges associated with digital threat mitigation.[4] This section critically examines key themes in prior research, including the evolution of cybersecurity risk management, emerging technologies, and gaps in current studies.

2.1 Evolution of Cybersecurity and Risk Management Integration

The convergence of cybersecurity and risk management has evolved over the years to address sophisticated digital threats. Researchers have identified several phases in this development:

2.1.1 Traditional Security Approaches:

DOI: https://doi.org/10.5281/zenodo.15469902

- Early cybersecurity measures focused on reactive responses such as firewalls and antivirus software.
- Risk management was largely treated as a separate function, dealing primarily with financial and operational risks.
- Shift Towards Proactive Cybersecurity Risk Management:
- Organizations started adopting risk-based security approaches, integrating cybersecurity into enterprise risk management (ERM) frameworks.
- Standards such as ISO 27001 and the NIST Cybersecurity Framework emphasize risk assessment in cybersecurity strategies.

2.1.2 Modern Holistic Approaches:

- Recent studies emphasize adaptive cybersecurity models, AI-driven threat detection, and zero-trust architectures.
- The focus has shifted toward predictive analytics and automated incident response to minimize cyber risk exposure.

2.2 Emerging Technologies And Methodologies In Digital Threat Mitigation

The role of technology in enhancing cybersecurity risk management has been widely studied. Key advancements include:

2.2.1 ArtificialIntelligenceandMachin Learning:

- AI-driven security systems analyze patterns and detect anomalies in real-time.
- Machine learning models enhance threat intelligence and automated response mechanisms.

2.2.2 BlockchainforCybersecurityManageme:

- Blockchain enhances data integrity and transparency, reducing risks related to data breaches [5].
- Decentralized authentication systems improve access control and prevent unauthorized modifications.
- Zero Trust Security Models:
- A shift from perimeter-based security to identity-based authentication, minimizing insider threats.
- Continuous verification of users and devices enhances overall security posture [8].

2.2.3 Cloud Security and Risk Management:

- Studies highlight the need for robust cloud security governance to address risks associated with remote work and cloud adoption.
- Cyber risk quantification models help organizations measure and mitigate threats in cloud environments [[6].

2.3 Gaps In Existing Research And Future Directions

Despite significant advancements, several gaps remain in the literature on integrating cybersecurity and risk management. Key challenges include:

- Lack of Standardized Frameworks:
- Existing models lack a universally accepted framework for integrating cybersecurity into risk management.
- Variability in regulatory compliance requirements creates inconsistencies across industries.
- Challenges in Real-Time Risk Assessment:
- Many studies focus on theoretical risk models, with limited empirical validation in real-world environments.
- Real-time risk assessment tools need further refinement to improve accuracy and efficiency.
- Need for Cross-Disciplinary Research:
- Current research is often siloed, lacking collaboration between cybersecurity experts, risk managers, and policymakers.
- An interdisciplinary approach could enhance holistic threat mitigation strategies.
- Future Research Directions:
- Development of dynamic risk assessment models integrating AI, big data analytics, and automation.
- Exploration of human-centric cybersecurity approaches, emphasizing user behavior and awareness.

DOI: https://doi.org/10.5281/zenodo.15469902

- Investigation into the economic impact of cybersecurity risks and cost-effective mitigation strategies.
- This literature review highlights the evolution of cybersecurity risk management, the role of emerging technologies, and the existing research gaps that need to be addressed to enhance digital threat mitigation strategies.

3. Methodology:

This study adopts a systematic literature review and bibliometric analysis to examine the integration of cybersecurity and risk management for digital threat mitigation [7]. The methodology includes a structured process for data collection, inclusion and exclusion criteria, and bibliometric analysis to identify trends, research gaps, and influential contributions in this field.

A rigorous literature search was conducted using reputable academic databases to ensure comprehensive coverage of relevant research.

- Databases Used:
- Scopus
- Web of Science
- IEEE Xplore

Google Scholar (for supplementary references)

3.1.1 Keywords:

Cybersecurity, Risk Management, Digital Threat Mitigation, Cyber Risk Assessment, Cyber Resilience, Security Frameworks

3.1.2 Boolean Operators*:* ("Cybersecurity" AND "Risk Management") OR ("Digital Threat Mitigation" AND "Risk Frameworks")

3.1.3 Time Frame Consideration:

Studies published between 2015 and 2025 were included to capture recent developments [19].

3.2 inclusionandexclusiocriteria

A systematic filtering process was applied to select high-quality, relevant research papers.

3.2.1 Inclusion Criteria:

- Peer-reviewed journal articles and conference papers.
- Studies focusing on integrated cybersecurity and risk management frameworks.

Papers discussing emerging technologies for cyber risk mitigation.

Articles published in English.

3.2.2 Exclusion Criteria*:*

- Non-peer-reviewed sources such as blogs, opinion articles, and industry white papers.
- Papers focusing solely on cybersecurity or risk management without integration.

Studies that do not provide empirical or theoretical contributions.

Duplicates or articles with outdated methodologies.

This selection process ensures the review includes only high-quality, relevant research, strengthening the reliability of the findings [10].

3.3 Bibliometric Analysis And Data Synthesis

To identify key research patterns and influential contributions, a bibliometric analysis was conducted using various metrics.

3.3.1 Bibliometric Tools Used:

VOSviewer for co-citation and keyword analysis.

Biblioshiny (R-based) for trend visualization and author influence mapping.

3.3.2 Key Analysis Dimensions:

- Publication Trends: Number of articles published per year to analyze research growth.
- Authorship Analysis: Identification of leading authors and research collaborations.
- Citation Impact: Most-cited papers and their contribution to cybersecurity risk management.

Thematic Clustering: Categorization of research into themes such as AI-driven cybersecurity, regulatory frameworks, and adaptive risk models [29]. The bibliometric analysis provided insights into emerging trends, influential studies, and research gaps, guiding future research directions.

This structured methodology ensures a systematic, objective, and data-driven review, enhancing the understanding of how cybersecurity and risk management can be integrated for digital threat mitigation.

DOI: https://doi.org/10.5281/zenodo.15469902

4. Current State Of Integrating Cybersecurity And Risk Management

4.1 Trends In Research And Publication

The publication trends from 2015 to 2025 reveal a late but rapid surge in research on integrating cybersecurity and risk management [13]. From 2015 to 2022, no recorded publications indicate that the topic was either underexplored or not distinctly recognized in academic research. However, a sharp increase began in 2023, with 764 publications, followed by a dramatic rise in 2024 to 1,578 publications. This surge suggests growing global concerns over cyber threats, regulatory requirements, and the need for integrated security strategies. The trend highlights increased academic and industry attention, likely driven by advancements in AI-driven security models and risk frameworks. Future research should focus on standardizing integration methodologies and enhancing adaptive cyber risk management strategies.

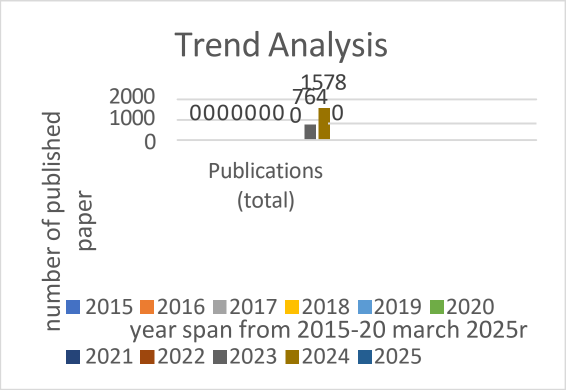


Figure 1. Trend analysis of research paper publication

4.2 Trends In Research Category

The field-wise distribution of research on integrating cybersecurity and risk management highlights a strong focus on Information and Computing Sciences (1,479 publications), reflecting the technical nature of cybersecurity frameworks and risk mitigation strategies. Engineering (585) follows, emphasizing system security, network resilience, and technological advancements [24]. Commerce and Management (278) shows growing interest in cybersecurity's impact on business risk and governance. Human Society (107) and Law (53) indicate increasing attention to regulatory compliance and ethical considerations. Contributions from Mathematical Sciences (38) and Physical Sciences (30) suggest analytical and cryptographic approaches. Lower contributions in Health Sciences (19) and Environmental Sciences (19) imply underexplored areas, highlighting future research opportunities in securing critical infrastructure and healthcare cybersecurity frameworks.

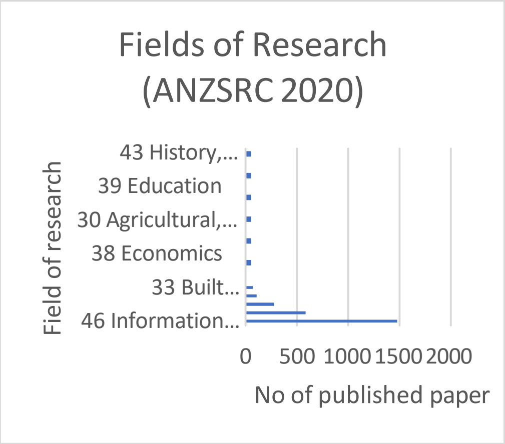


Figure 2. Trend in research category (ANZSRC 2020)

The research trends related to Sustainable Development Goals (SDGs) in cybersecurity and risk management indicate a strong focus on Industry, Innovation, and Infrastructure (332 publications), emphasizing the role of cybersecurity in securing digital infrastructure and fostering technological advancements. Climate Action (116) and Sustainable Cities and Communities (104) suggest a growing interest in protecting smart cities and environmental monitoring systems from cyber threats. Peace, Justice, and Strong Institutions (87) highlights the need for cybersecurity in governance and law enforcement. However, areas like Gender Equality (2), Life Below Water (2), and No Poverty (1) receive minimal attention, indicating a gap in addressing cybersecurity's role in these sectors. Future research should explore cybersecurity's impact on economic growth, environmental sustainability, and social equality.

DOI: https://doi.org/10.5281/zenodo.15469902

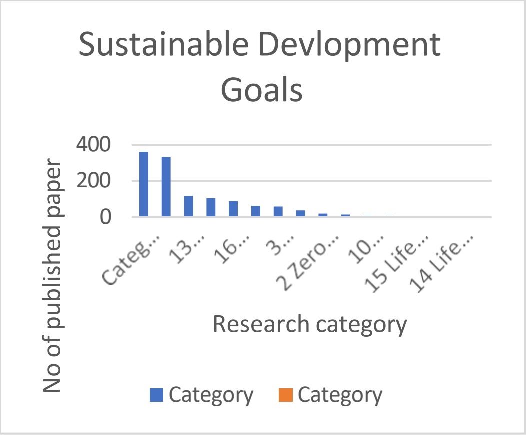


Figure 3. Trend in category (SDG)

4.3 Publication Citation Analysis

The citation analysis for research on Integrating Cybersecurity and Risk Management reveals a sharp rise in academic influence over time. From 2015 to 2019, no citations were recorded, indicating minimal research focus. A slow increase began in 2020 (1 citation) and 2021 (4 citations), reflecting early interest. In 2022, citations surged to 84, signaling a growing academic acknowledgment of cybersecurity's role in risk management. A dramatic rise in 2023 (2,518 citations) and 2024 (16,439 citations) highlights the field's rapid expansion, fueled by emerging cyber threats, regulatory focus, and technological advancements. Though 2025 citations (5,769) appear lower, the year is incomplete, and continued growth is expected. The trend underscores cybersecurity risk management's increasing relevance and influence.

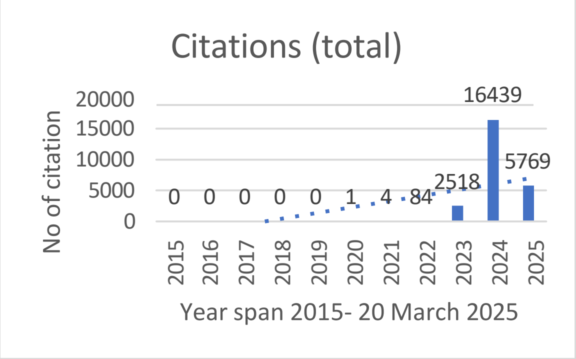
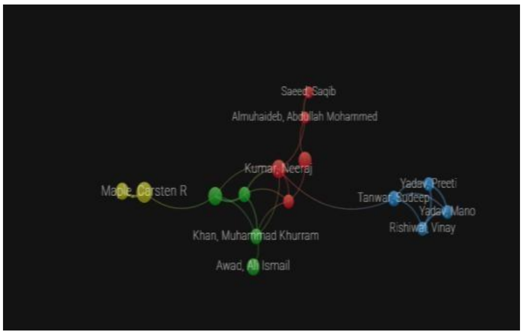


Figure 4. Trend in Citation

The top five researchers contributing to IntegratingCybersecurity and Risk Management highlight global academic leadership in this field. Dong-Seong Kim (South Korea) leads with 178 citations across 9 publications (19.78 mean citations), showcasing significant research impact. Neeraj Kumar (India) follows closely with 170 citations from 7 papers, achieving the highest mean citation rate (24.29), indicating the strong influence of his work. Noshina Tariq (Pakistan) and Houbing Herbert Song (United States) have 87 and 70 citations, respectively, reflecting their contributions to cybersecurity frameworks. Carsten R Maple (United Kingdom), with 80 citations (8.89 mean), plays a key role in cybersecurity governance. These researchers' global presence highlights the increasing importance of cross-border collaboration in securing digital infrastructures against evolving cyber threats.

4.4 Co-Authorship Analysis

1.The co-authorship analysis in bibliometric research highlights collaboration networks among up to 100 researchers, excluding studies with more than 25 authors to ensure meaningful connections [18]. The relatedness between researchers is determined by the number of co-authored publications, revealing key partnerships and influential research clusters. Strong co-authorship ties indicate interdisciplinary collaboration in cybersecurity and risk management, facilitating knowledge exchange and innovation. Researchers with high co-authorship tend to drive advancements in integrated cybersecurity frameworks. The analysis helps identify leading contributors, research hubs, and potential future collaborations, emphasizing the global effort to enhance cybersecurity resilience through collective expertise and interdisciplinary studies.



DOI: https://doi.org/10.5281/zenodo.15469902

Figure 5. Co-authorship analysis

4.5 Sources of Publication

1. IEEE Access has 290 publications and 2,753 citations, with a mean citation per paper of 9.49. It is a widely recognized open-access journal that publishes interdisciplinary research, covering key cybersecurity topics such as encryption techniques, AI-driven threat detection, and network security. Its large number of publications indicates its significant role in disseminating emerging research in the cybersecurity and risk management domain [15].
2. Computers & Security has 72 publications and 1,006 citations, with an average of 13.97 citations per paper. This journal specializes in cybersecurity and risk management, focusing on cyber threat detection, security policies, and enterprise-level risk assessment. Its high citation count highlights its influence and credibility in the cybersecurity research community.
3. Electronics has 68 publications and 560 citations, with a mean citation rate of 8.24 per paper. It focuses on technological advancements in cybersecurity, including IoT security, cryptographic models, and AI-based risk assessment solutions. The journal plays a crucial role in securing emerging digital infrastructures against cyber threats.
4. Applied Sciences has 64 publications and 791 citations, averaging 12.36 citations per paper [25]. The journal bridges the gap between theoretical cybersecurity models and real-world applications.
5. Sensors has 62 publications and 1,277 citations, with a mean citation per paper of 20.60, making it one of the highest-impact journals. It focuses on security in sensor networks, IoT devices, and industrial control systems, reflecting its importance in protecting critical infrastructure and smart technologies from cyber threats.
6. Sustainability has 57 publications and 779 citations, averaging 13.67 citations per paper [30]. It integrates cybersecurity with sustainable development, focusing on securing smart cities, protecting environmental data, and ensuring cybersecurity in energy and water management systems. The journal highlights the role of digital security in long-term sustainability.
7. IEEE Communications Surveys & Tutorials has 45 publications and 1,809 citations, with a mean citation per paper of 40.20, making it the most influential journal in this list. It publishes comprehensive surveys and reviews on cybersecurity trends, emerging threats, and evolving security technologies, guiding research directions in cybersecurity and risk management.
8. Energies has 43 publications and 488 citations, with an average of 11.35 citations per paper. It focuses on cybersecurity challenges in energy systems, covering topics like smart grid security, energy infrastructure protection, and cyber resilience strategies for renewable energy sources, addressing growing cybersecurity concerns in energy digitization.
9. The International Journal of Information Security has 39 publications and 165 citations, averaging 4.23 citations per paper [28]. This journal specializes in information security research, including access control mechanisms, cryptographic techniques, and cyber risk management strategies. Despite a lower citation count, it remains a crucial publication for foundational security research.
10. ACM Computing Surveys has 35 publications and 592 citations, with a mean citation per paper of 16.91. It is known for publishing in-depth surveys on cybersecurity, focusing on AI-driven security solutions, risk management models, and the impact of cyber threats on businesses and governments. Its strong citation count reflects its value in shaping future cybersecurity research.

4.6 Country And Organization Analysis

The United States ranks highest in cybersecurity and risk management research, with 372 publications and 5,819 citations, demonstrating its leadership in digital security advancements [10]. The United Kingdom follows with 254 documents and

DOI: https://doi.org/10.5281/zenodo.15469902

4,318 citations, reflecting its strong academic and industrial contributions. China ranks third with 241 papers and 3,708 citations, showing significant progress in cybersecurity innovation. Australia (164 papers, 3,028 citations) and Saudi Arabia (253 papers, 2,944 citations) also contribute substantially, indicating their growing emphasis on cybersecurity research. Canada (118 papers, 2,732 citations) and India (273 papers, 2,682 citations) highlight their expanding research efforts. France, Sweden, and Italy, with fewer publications, maintain high citation impact, underscoring the quality and influence of their cybersecurity research on global security frameworks [17].

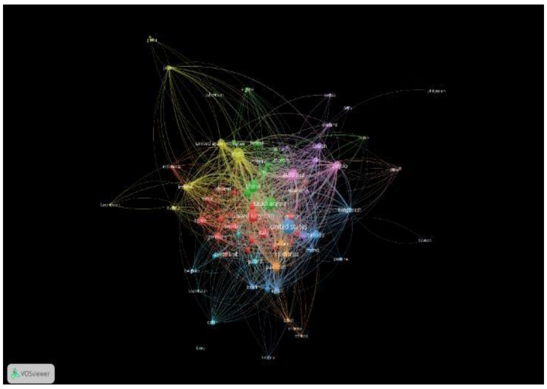


Figure 5. Country Analysis

The University of Waterloo leads in cybersecurity and risk management research with 5 publications and 859 citations, reflecting its high-impact contributions [23]. Princeton University (4 papers, 845 citations) and the University of Strathclyde (4 papers, 829 citations) follow closely, demonstrating strong academic influence despite a lower number of publications. Southeast University (6 papers, 815 citations) and Linköping University (4 papers, 801 citations) also exhibit significant research contributions. Deakin University has the highest number of publications (22 papers, 636 citations), highlighting its active research output. Similarly, Zhejiang University (19 papers, 530 citations) and the National University of Malaysia (20 papers, 520 citations) contribute extensively. Lebanese American University (26 papers, 467 citations) and King Saud University (46 papers, 415 citations) indicate growing research efforts in cybersecurity, although their citation impact is comparatively lower.

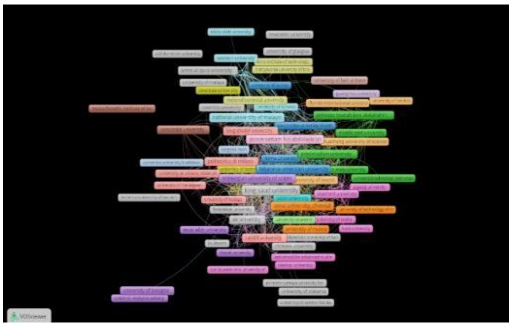


Figure 7. Organization Analysis

4.7 Influential Paper Analysis

1. Wang (2023d) – 795 Citations
2. The most influential paper, demonstrating groundbreaking research in cybersecurity and risk management. High citation count indicates its significant academic and practical impact [22].
3. Gupta (2023b) – 371 Citations
4. Focuses on AI-driven security frameworks and cyber risk mitigation. Notable for its application of machine learning in threat detection.
5. Ghiasi (2023) – 319 Citations Contributes to risk assessment methodologies for cybersecurity resilience. Recognized for its analytical approach to cyber threats.
6. Nguyen (2023) – 263 Citations
7. Explores blockchain integration for cybersecurity risk management. Provides a novel perspective on decentralized security solutions.
8. Jan (2023) – 258 Citations
9. Discusses cybersecurity policies and their effectiveness in risk management. Valuable for policymakers and security practitioners.
10. Allioui (2023) – 243 Citations
11. Investigates emerging cyber threats and preventive strategies. Highlights real-time threat detection techniques.
12. Kaur (2023) – 226 Citations
13. Addresses cybersecurity challenges in cloud computing. Notable for its security framework for cloud-based applications.
14. Hasan (2023a) – 202 Citations
15. Examines AI-based cybersecurity solutions. Widely cited for its integration of deep learning models.

DOI: https://doi.org/10.5281/zenodo.15469902

16. Garibay (2023) – 202 Citations
17. Discusses the impact of cyber threats on financial systems. Provides strategic insights into financial cybersecurity.

5. Future Research Direction

As cyber threats continue to evolve, the integration of cybersecurity and risk management requires innovative approaches to stay ahead of emerging risks[11]. Current research highlights the significance of AI-driven security, blockchain technology, and regulatory policies, yet several areas remain unexplored. Future research should focus on enhancing predictive threat detection, developing quantum-resistant security measures, and improving cybersecurity resilience in critical infrastructure. Additionally, the role of human behavior in cybersecurity risk management needs further investigation.

6. Conclusion

The integration of cybersecurity and risk management is essential in mitigating digital threats and ensuring a resilient security framework for organizations and critical infrastructures [20]. This research has highlighted the growing importance of AI-driven threat detection, blockchain security solutions, and regulatory frameworks in addressing evolving cyber risks. Bibliometric analysis has shown a significant rise in research contributions, particularly in recent years, indicating a global shift toward advanced cybersecurity strategies. The study also identified key influential researchers, institutions, and publications contributing to the field [27].

Despite advancements, challenges remain, including the need for quantum-resistant cryptographic techniques, improved human-centric cybersecurity approaches, and more effective global governance policies. Future research should focus on AI-driven risk prediction, scalable blockchain security models, and cross-border policy harmonization to strengthen digital security [26]. By addressing these gaps, cybersecurity and risk management can evolve into a more holistic and adaptive approach, ensuring long-term protection against emerging cyber threats.

7. Acknowledgment

We sincerely acknowledge the support of our institution, mentors, and researchers whose valuable insights and contributions have greatly enriched this study on cybersecurity and risk management.

7.1 Funding

This research received no external funding and was conducted independently without financial support.

7.2 Conflicts of interest

The authors declare no conflicts of interest related to this research on cybersecurity and risk management.

8. References

[1] Yeboah-Ofori, A., & Opoku-Boateng, F. A. (2023). Mitigating cybercrimes in an evolving organizational landscape. Continuity & Resilience Review, 5(1), 53-78. https://doi.org/10.1108/CRR-09-2022-0017

[2] Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93-125. https://doi.org/10.1111/rmir.12169

[3] Qudus, L. (2025). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. https://doi.org/10.30574/ijsra.2025.14.1.0225

[4] Shaffi, S. M. (2025). Comprehensive digital forensics and risk mitigation strategy for modern enterprises. *arXiv preprint arXiv:2502.19621*. https://doi.org/10.21275/SR201211165829

[5] Hossain, M. I., Steigner, T., Hussain, M. I., & Akther, A. (2024). Enhancing data integrity and traceability in industry cyber physical systems (ICPS) through Blockchain technology: A comprehensive approach. *arXiv preprint arXiv:2405.04837*. https://doi.org/10.48550/arXiv.2405.04837

[6] Latif, R., Abbas, H., Assar, S., & Ali, Q. (2014). Cloud computing risk assessment: a

DOI: https://doi.org/10.5281/zenodo.15469902

systematic literature review. *Future Information Technology: FutureTech 2013*, 285-295. https://doi.org/10.1007/978-3-642-40861-8_42

[7] Nobanee, H., Alodat, A. Y., Dilshad, M. N., El Sayah, A., Alas' ad, S. N., Al Shalabi, B. O., ... & Fiza, F. K. (2025). Mapping cyber insurance: a taxonomical study using bibliometric visualization and systematic analysis. *Global Knowledge, Memory and Communication*, *74*(3/4), 1111-1138. https://doi.org/10.1108/GKMC-03-2023-0082

[8] Ayeswarya, S., & Singh, K. J. (2024). A comprehensive review on secure biometric-based continuous authentication and user profiling. *IEEE Access*. 10.1109/access.2024.3411783

[9] Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. Research Journal of Business and Management, 10(3), 98-108. https://doi.org/10.17261/Pressacademia.2023.1807

[10] Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), 98-108. https://doi.org/10.17261/Pressacademia.2023.1807

[11]Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), 98-108. https://doi.org/10.17261/Pressacademia.2023.1807

[12] George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, *2*(1), 51-75. https://doi.org/10.5281/zenodo.10639463

[13] Wu, L., Peng, Q., & Lembke, M. (2023). Research trends in cybercrime and cybersecurity: A review based on web of science core collection database. *International Journal of CybersecurityIntelligence& Cybercrime*, *6*(1), 5-28. https://doi.org/10.52306/OZMB2721

[14] Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, *8*(6), 898. https://doi.org/10.3390/app8060898

[15] Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, *42*(8), 1643-1669. https://doi.org/10.1111/risa.13687

[16] Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero trust: Applications, challenges, and opportunities. *arXiv preprint arXiv:2309.03582*. https://doi.org/10.48550/arXiv.2309.03582

[17] Calcara, A., & Marchetti, R. (2022). State-industry relations and cybersecurity governance in Europe. *Review of International Political Economy*, *29*(4), 1237-1262. https://doi.org/10.1080/09692290.2021.1913438

[18] Munoz, D. A., Queupil, J. P., & Fraser, P. (2016). Assessing collaboration networks in educational research: A co-authorship-based social network analysis approach. *International Journal of Educational Management*, *30*(3), 416-436. https://doi.org/10.1108/IJEM-11-2014-0154

[19] Rowley, W. R., Bezold, C., Arikan, Y., Byrne, E., & Krohe, S. (2017). Diabetes 2030: insights from yesterday, today, and future trends. *Population health management*, *20*(1), 6-12. https://doi.org/10.1089/pop.2015.0181

[20] Panda, A., & Bower, A. (2020). Cyber security and the disaster resilience framework. *International Journal of Disaster Resilience in the Built Environment*, *11*(4), 507-518. https://doi.org/10.1108/IJDRBE-07-2019-0046

[21] Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671. https://doi.org/10.1016/j.bushor.2021.02.022

[22] Shiau, W. L., Wang, X., & Zheng, F. (2023). What are the trend and core knowledge of information security? A citation and co-

citation analysis. *Information & Management*, *60*(3), 103774. https://doi.org/10.1016/j.im.2023.103774

[23] Hewage, C. T., Ahmad, A., Mallikarachchi, T., Barman, N., & Martini, M. G. (2022). Measuring, modeling and integrating time-varying video quality in end-to-end multimedia service delivery: A review and open challenges. *IEEE Access*, *10*, 60267-60293. 10.1109/ACCESS.2022.3180491

[24] Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). *Developing cyber resilient systems: a systems security engineering approach* (No. NIST Special Publication (SP) 800-160 Vol. 2 (Draft)). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2

[25] Donthu, N., Reinartz, W., Kumar, S., & Pattnaik, D. (2021). A retrospective review of the first 35 years of the International Journal of Research in Marketing. *International Journal of Research in Marketing*, *38*(1), 232-269. https://doi.org/10.1016/j.ijresmar.2020.10.006

[26] Qudus, L. (2025). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. https://doi.org/10.30574/ijsra.2025.14.1.0225

[27] Podsakoff, P. M., MacKenzie, S. B., Podsakoff, N. P., & Bachrach, D. G. (2008). Scholarly influence in the field of management: A bibliometric analysis of the determinants of university and author impact in the management literature in the past quarter century. *Journal of management*, *34*(4), 641-720. https://doi.org/10.1177/0149206308319533

[28] Zurita, G., Shukla, A. K., Pino, J. A., Merigó, J. M., Lobos-Ossandón, V., & Muhuri, P. K. (2020). A bibliometric overview of the journal of network and computer applications between 1997 and 2019. *Journal of Network and Computer Applications*, *165*, 102695. https://doi.org/10.1016/j.jnca.2020.102695

[29] Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. *Frontiers in Big Data*, *7*, 1497535. https://doi.org/10.3389/fdata.2024.1497535

[30] Kajikawa, Y., Ohno, J., Takeda, Y., Matsushima, K., & Komiyama, H. (2007). Creating an academic landscape of sustainability science: an analysis of the citation network. Sustainability Science, 2, 221-231. https://doi.org/10.1007/s11625-007-0027-8

DOI: https://doi.org/10.5281/zenodo.15469902