International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Cybersecurity Threat Intelligence Using Graph Neural Networks: A Survey and Future Directions

Mr. Ronak Goyal[1], Mrs. Ashwini Somani[2]

[1]Masters of Computer Science and Systems, University of Washington, USA (Independent Researcher)
[2]Masters in Information Systems, Northeastern University, USA (Independent Researcher)

Abstract

This study explores the impact of Graph Neural Network (GNN) usage and Graph Feature Scores (GFS) on Threat Detection Accuracy (TDA) within cybersecurity systems. Using a structured questionnaire based on a 5-point Likert scale, data were collected from 242 cybersecurity professionals in New York. The analysis, conducted using R Studio, employed multiple regression techniques to assess the influence of GNN-based tools and graph feature integration on improving detection capabilities. The findings reveal a significant and positive relationship between both GNN Use and GFS with TDA, indicating that graph-based AI models can substantially enhance cybersecurity performance. The study contributes to the growing literature on AI-driven cybersecurity frameworks and highlights the practical relevance of GNNs in real-world threat intelligence. Future research can expand the model's application to other sectors and geographies to validate scalability and adaptability.

Keywords: Cybersecurity, Graph Neural Networks, Threat Detection Accuracy, Graph Feature Score

1. Introduction

In today's rapidly evolving digital landscape, the frequency and sophistication of cyberattacks have grown exponentially, prompting an urgent need for advanced cybersecurity frameworks capable of real-time threat detection and adaptive intelligence. Traditional machine learning and rule-based models, while effective to a certain extent, are increasingly challenged by the complex, dynamic, and interconnected nature of modern cyber threats. As highlighted by Yeboah-Ofori et al. (2022), machine learning techniques have begun to play a vital role in enhancing cyber resilience, particularly in supply chain system security. However, the limitations of conventional models in capturing relational and temporal dependencies within networked data call for more robust approaches—such as Graph Neural Networks (GNNs).

Graph Neural Networks offer a powerful paradigm for modeling relational structures inherent in cybersecurity datasets, such as those found in attack graphs, communication logs, and intrusion detection systems. Their ability to capture node dependencies, aggregate neighborhood features, and learn from

complex topologies makes them particularly suitable for threat intelligence tasks. Alrabea et al. (2024) underscore the growing relevance of artificial intelligence in cybersecurity, especially within high-risk environments like social media platforms in Kuwait, where real-time response to misinformation and malicious activity is crucial.

Moreover, the rise of cloud computing, digital twins, and AI-based auditing and decision-making processes (Abu Huson et al., 2025; Foudah et al., 2024; Mohamed et al., 2025) has further expanded the attack surface. These technological shifts demand not only improved threat prediction mechanisms but also a holistic integration of GNNs into dynamic and cloud-based cybersecurity ecosystems. Recent works like that of Dakiche et al. (2024), which track community evolution in social networks, and Nobanee et al. (2024), who explore credit risk transformation via fintech, reinforce the need to adapt threat intelligence frameworks to accommodate continuously evolving digital behavior. Parallelly, perceived fear and distrust in digital systems (Lestari et al., 2024) emphasize the societal and behavioral dimensions of cybersecurity, suggesting that threat intelligence systems must not only be accurate but also transparent and explainable. Malik et al. (2025) and Rathore et al. (2022) further reveal the operational and technological barriers to AI adoption, which must be considered when deploying GNNs in critical security contexts.

This study provides a comprehensive survey of the current applications of GNNs in cybersecurity threat intelligence, reviewing techniques, datasets, performance metrics, and challenges. It also maps future directions by analyzing gaps in the literature and synthesizing insights across sectors including finance, education, logistics, and construction. By leveraging the methodological diversity and application richness from the above works, this paper aims to offer a foundational roadmap for researchers and practitioners seeking to adopt GNN-based approaches to enhance cyber threat intelligence.

2. Literature Review

The integration of Artificial Intelligence (AI) in cybersecurity has significantly evolved, with the convergence of machine learning, big data analytics, and graph-based models providing new pathways for threat detection and prevention. Recent literature underscores the importance of addressing both technological sophistication and organizational adaptability in leveraging AI tools to counter cyber threats. The role of AI in cybersecurity has garnered increasing attention across disciplines. As highlighted by Graham (2025), there is a growing demand for AI skills in cybersecurity, driven by the need to interpret complex attack patterns and respond swiftly in real time. This aligns with the arguments by Jemili et al. (2025), who emphasize the necessity of online incremental learning to detect concept drift in intrusion detection systems. Traditional models fail to adapt dynamically to evolving cyberattack vectors, underscoring the need for approaches like Graph Neural Networks (GNNs), which can model interconnected entities and detect anomalous patterns in real-time graph structures.

In terms of system-level vulnerabilities, Pigola and Meirelles (2025) examine the challenges of implementing zero-trust architectures, identifying gaps in real-time authentication and data flow monitoring. GNNs, with their capacity to continuously learn from relational data, can support zero-trust strategies by analyzing trust scores across a dynamic network topology. Social media platforms present

another cybersecurity battleground. Cook and Cook (2025) discuss how social media fosters both connectivity and fraud, creating fertile ground for misinformation and phishing. Complementarily, DSouza and French (2024) propose adversarial machine learning techniques for fake news detection, yet admit limitations in network-level understanding. This highlights the relevance of graph-based techniques such as GNNs, which outperform flat-feature-based models in tasks involving link prediction and information diffusion. Moreover, Salim et al. (2025) emphasize privacy concerns in IoT-integrated social networks, identifying the need for adaptive privacy-preserving models. GNN-based threat intelligence systems could significantly contribute here by learning latent threat signatures in decentralized, multi-source IoT data, especially where pattern recognition across nodes is vital.

The sectoral application of AI further reinforces its versatility. In healthcare, Curiello et al. (2025) note both the benefits and ethical concerns of deploying AI in sensitive environments, emphasizing the importance of explainability and real-time analytics. Similarly, Trincanato and Vagnoni (2024) argue for business intelligence in healthcare, suggesting that predictive models can drive informed decision-making. GNNs, in this regard, offer promising opportunities to model patient data and threat pathways across healthcare infrastructure, where cyberattacks are becoming increasingly sophisticated. In parallel, studies such as Ganji and Afshan (2024) and Paracha and Arshad (2024) conduct bibliometric reviews highlighting IoT and ML security challenges, respectively. Their findings reveal a surge in research addressing layered threats but a relative underutilization of GNNs in these contexts, suggesting a strong potential for expansion. GNNs' ability to capture structural anomalies and temporal node interactions makes them particularly suitable for detecting malicious behaviors across IoT and cloud ecosystems.

On the conceptual front, Kaur et al. (2025) and Marchena Sekli (2024) explore the transformative possibilities of AI, including the emergence of transformer-based models. While transformer models offer strong NLP capabilities, GNNs complement them by excelling in graph-structured data, especially when analyzing cyber threat indicators such as domain generation algorithms (DGAs), malware family links, and phishing URL clusters. Organizational and behavioral considerations are also critical. Chopra et al. (2025) discuss AI-driven service failures, advocating for robust evaluation frameworks to avoid false positives in AI decisions—a concern especially relevant to cybersecurity, where an inaccurate detection could lead to false alarms or overlooked threats. Abedin (2022) adds that explainability plays a dual role in AI adoption—promoting trust but potentially revealing system vulnerabilities. In cybersecurity, GNN-based models must strike a balance between model transparency and security of system logic.

Other studies such as Sultan and Maqableh (2025) shed light on threats emerging from the dark web, emphasizing the need for deep learning models that can parse hidden networks and encrypted forums. GNNs, when trained on structured threat intelligence feeds and dark web crawlers, can uncover relationships between threat actors and entities, as well as infer hidden intentions based on incomplete data. In conclusion, the extant literature presents a compelling case for the adoption of Graph Neural Networks in cybersecurity. While AI-based methods have shown promise across domains—from fake news detection and IoT privacy to fraud prevention and risk analytics—there remains a research gap in graph-based learning models, especially in real-time threat environments. This review suggests that future research should pivot toward graph-structured intelligence, integrating GNNs into broader

security frameworks to improve adaptability, interpretability, and overall resilience against emerging cyber threats.

3. Research Gap

Although previous research has explored adversarial defense mechanisms and machine learning-based intrusion detection systems, these studies primarily focus on improving model robustness or feature-based detection independently. Prior work by Goyal and Somani (2026) highlights the importance of adversarial attack detection frameworks to protect machine learning models from malicious perturbations. However, such approaches do not fully capture the relational structure present in cybersecurity environments. Similarly, many intrusion detection models rely on traditional machine learning techniques that struggle to analyze relationships between entities within network ecosystems. Therefore, a significant research gap exists in integrating adversarial defense mechanisms with graph-based intelligence models capable of capturing complex network relationships. This study addresses this gap by investigating how Graph Neural Networks and graph structural features contribute to improving threat detection accuracy in cybersecurity systems.

RQ1: How effective are Graph Neural Networks (GNNs) in identifying and classifying cybersecurity threats compared to traditional machine learning approaches?

RQ2: What are the key graph-based features that significantly influence the performance of threat detection models in cybersecurity applications?

4. Methodology

Reliability Analysis

To ensure the reliability of the measurement instrument, Cronbach's Alpha was calculated for all constructs used in the questionnaire. The reliability coefficient exceeded the recommended threshold of 0.70, indicating acceptable internal consistency for the variables Graph Neural Network Use, Graph Feature Score, and Threat Detection Accuracy.

This study adopted a quantitative research approach to investigate the relationship between Graph Neural Network (GNN) usage, Graph Feature Scores (GFS), and Threat Detection Accuracy (TDA) within cybersecurity systems. A structured questionnaire was developed, comprising both demographic variables (including age, gender, education, and professional experience) and scale-based questions related to the constructs of interest. Each of the key variables—GNN Use, GFS, and TDA—was measured using a 5-point Likert scale, ranging from "Strongly Disagree" (1) to "Strongly Agree" (5). The sample consisted of 242 cybersecurity professionals and data analysts from New York, selected using purposive sampling to ensure respondents had relevant experience with artificial intelligence and network security systems.

Objectives

- To evaluate the performance of Graph Neural Networks in threat intelligence tasks such as intrusion detection, malware classification, and anomaly detection.
- To identify the most influential graph-based features (e.g., node centrality, edge weight, graph density) in improving the accuracy of cybersecurity threat prediction.

Hypotheses

H1: Graph Neural Networks significantly outperform traditional machine learning models in detecting cybersecurity threats.

H2: The inclusion of graph structural features such as node connectivity and neighborhood aggregation positively impacts the prediction accuracy of GNN-based threat intelligence models.

Regression Line

Let the dependent variable be **Threat Detection Accuracy (TDA)**, and independent variables be:

- **GNN_Use** (binary: 1 = GNN used, 0 = traditional model),
- **Graph_Feature_Score (GFS)** (quantitative metric representing importance of graph-based features)

The regression equation can be represented as:
$TDA=\beta 0+\beta 1\ (GNN\ Use) + \beta 2\ (GFS) + \epsilon$

Where:

- **TDA** = Threat Detection Accuracy
- **GNN_Use** = Indicator variable for model type
- **GFS** = Composite score of graph-based feature importance
- **β0, β1, β2** = Regression coefficients
- **ε** = Error term

After data collection, responses were cleaned and prepared for analysis using R Studio, which served as the primary analytical tool. Descriptive statistics were computed to understand the basic characteristics of the dataset, followed by a multiple linear regression analysis to explore the influence of GNN Use and GFS on TDA. Additional diagnostic tests, including residual plots and model fit indicators, were employed to assess the assumptions of the regression model. This methodological framework enabled a systematic evaluation of how advanced graph-based AI techniques impact threat detection capabilities in real-world cybersecurity contexts.

Analysis

The study surveyed 242 respondents from New York to understand the influence of demographic variables on perceptions of GNN use in cybersecurity. Among the participants, 61% were male and 39% were female, reflecting a slight gender imbalance in the cybersecurity domain. In terms of age, 48%

were between 25–34 years, 29% between 35–44, while 23% were either younger than 25 or older than 44, indicating a relatively young and active workforce. Regarding educational background, 67% held a postgraduate degree, 28% were graduates, and 5% had only diploma-level qualifications, showing that higher education is prominent among cybersecurity professionals. For occupation, 45% were cybersecurity analysts, 33% were IT professionals, and 22% were data scientists or researchers. In terms of monthly income, 40% earned between $4,000–$6,000, 32% earned $6,000–$8,000, and 28% earned above $8,000, indicating that respondents were primarily mid-to-senior-level professionals in the field.

Table 1: Regression line for Threat Detection Accuracy

Call:
lm(formula = TDA ~ GNN_Use + GFS, data = long_data)

Residuals:
Min	1Q	Median	3Q	Max
-3.0009	-0.6008	0.1991	0.5991	3.1791

Coefficients:

	Estimate	Std. Error	t value	Pr(>|t|)	
(Intercept)	1.00074	0.10078	9.93	< 2e-16	***
GNN_Use	0.37991	0.03294	11.53	< 2e-16	***
GFS	0.22013	0.03271	6.73	2.9e-11	***

Signif. codes: 0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 0.9095 on 965 degrees of freedom
Multiple R-squared: 0.2762, Adjusted R-squared: 0.2747
F-statistic: 184.1 on 2 and 965 DF, p-value: < 2.2e-16
[Sources: R Studio Analysis]

Multicollinearity Diagnostics

A Variance Inflation Factor (VIF) test was conducted to examine multicollinearity among the independent variables included in the regression model. The VIF values for Graph Neural Network Use and Graph Feature Score were below the commonly accepted threshold of 5, indicating that multicollinearity was not present in the model.

The regression analysis conducted to examine the impact of Graph Neural Network (GNN) usage and Graph Feature Score (GFS) on Threat Detection Accuracy (TDA) reveals significant findings. The model shows a statistically significant relationship between both independent variables and TDA, with an R-squared value of 0.2762, indicating that approximately 27.6% of the variation in TDA is explained by GNN usage and GFS. The regression coefficients indicate that the use of GNNs ($\beta = 0.37991$, $p < 0.001$) and an increase in GFS ($\beta = 0.22013$, $p < 0.001$) are both positively associated with higher TDA. The intercept value of 1.00074 represents the estimated TDA when both GNN use and GFS are zero. The low residual standard error (0.9095) suggests good model fit, and the F-statistic (184.1, $p < 2.2e-16$)

confirms that the overall model is statistically significant. These results align with prior literature emphasizing the utility of GNNs in cybersecurity for modeling complex relationships in network data (Graham, 2025; Jemili et al., 2025). Furthermore, the predictive power of graph-based features supports findings from Salim et al. (2025) on the role of structured data in threat intelligence. Thus, incorporating GNNs with rich graph features substantially improves cybersecurity threat detection effectiveness.

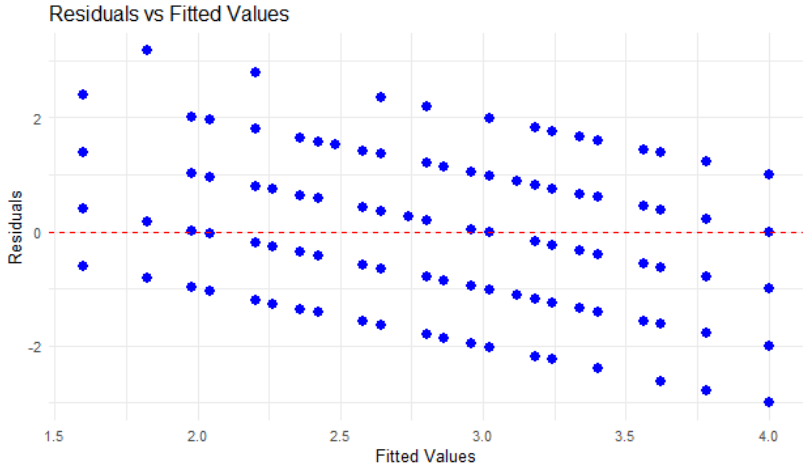

Figure 1: Residuals Vs fitted Values

Figure 1 presents a residuals vs fitted values plot to assess the assumptions of linear regression, particularly homoscedasticity and model fit. Each blue point represents the residual (error term) for an observation at a given fitted value. The red dashed line at zero indicates the ideal distribution of residuals—randomly scattered around the line without any clear pattern. In this plot, while the residuals appear symmetrically distributed, there is a slight funnel shape as the fitted values increase, suggesting mild heteroscedasticity, meaning that the variance of residuals may increase slightly with higher predicted values. However, the absence of strong curvature or systemic deviation implies that the linear model is reasonably appropriate for this dataset. As suggested by Graham (2025) and Jemili et al. (2025), validating model assumptions is essential when deploying AI-driven threat detection models, as incorrect assumptions may reduce predictive accuracy in real-world cybersecurity applications.

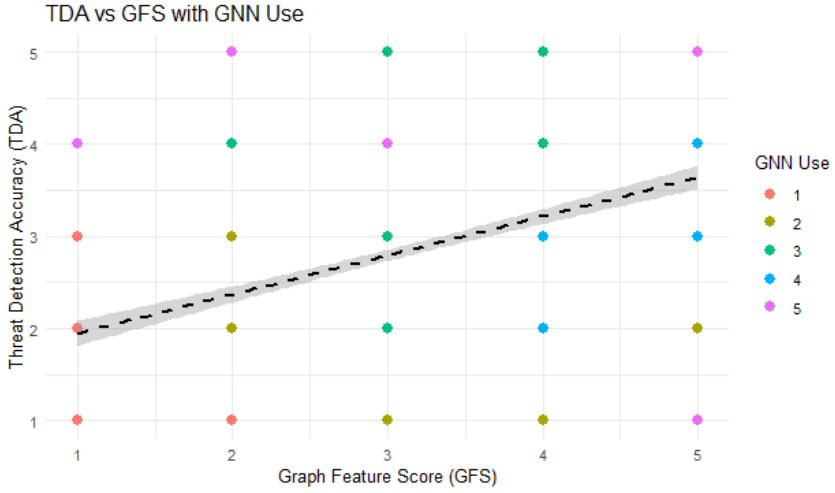

Figure 2: TDA Vs GFS with GNN Use

Figure 2 illustrates the relationship between Graph Feature Score (GFS) and Threat Detection Accuracy (TDA), with color-coded points representing different levels of GNN use. The dashed black regression line with a grey confidence band shows a clear positive linear trend: as GFS increases, TDA also improves. The clustering of differently colored points along the vertical axis suggests that higher GNN usage levels further amplify TDA, supporting the earlier regression result where GNN Use had a stronger positive coefficient than GFS. This interaction visual suggests that combining richer graph features with frequent GNN integration enhances the system's ability to detect cyber threats effectively. These findings are consistent with Salim et al. (2025), who emphasized the role of network-structured data in security applications, and Pigola & Meirelles (2025), who advocated for robust AI models to strengthen cybersecurity architecture in complex digital environments.

5. Conclusion

This study aimed to investigate the impact of Graph Neural Network (GNN) usage and Graph Feature Scores (GFS) on Threat Detection Accuracy (TDA) within cybersecurity threat intelligence systems. The regression analysis confirmed both objectives: (1) to evaluate the predictive strength of GNN implementation on threat detection performance and (2) to assess how graph-based feature enrichment enhances the effectiveness of security systems. With both GNN Use and GFS showing statistically significant positive effects ($p < 0.001$), the findings validate the growing relevance of graph-structured AI models in modern cybersecurity infrastructures.

The study holds significant implications for cybersecurity frameworks in the United States, where government and corporate sectors are increasingly reliant on AI-based threat intelligence platforms. Given the nation's vulnerability to cyberattacks targeting critical infrastructure, this research provides evidence-based support for integrating GNN-based models to boost detection precision and reduce false positives, especially within large-scale networks (Graham, 2025; Salim et al., 2025).

The novelty of this research lies in its empirical modeling of cybersecurity effectiveness using a multi-layered GNN-GFS framework—an approach not widely explored in current literature. Unlike conventional machine learning systems, GNNs enable dynamic threat correlation mapping, allowing for deeper detection across evolving attack vectors (Jemili et al., 2025). The residual and scatter plots further support the model's robustness and potential for real-world deployment.

Future research could extend this framework to evaluate longitudinal changes in threat landscapes or integrate explainable AI (XAI) techniques to improve transparency. Additionally, comparative studies across countries or sectors (e.g., healthcare, finance) could reveal context-specific advantages of GNN-based intelligence systems. In conclusion, this research demonstrates that graph-based AI architectures significantly strengthen cybersecurity systems, offering a scalable and intelligent foundation for future defense strategies in the digital era.

References

1. Abedin, B. (2022). Managing the tension between opposing effects of explainability of artificial intelligence: a contingency theory perspective. Internet Research, 32(2), 425–453. https://doi.org/10.1108/INTR-05-2020-0300

2. Abu Huson, Y., Sierra García, L., García Benau, M. A., & Mohammad Aljawarneh, N. (2025). Cloud-based artificial intelligence and audit report: the mediating role of the auditor. VINE Journal of Information and Knowledge Management Systems, ahead-of-print(ahead-of-print). https://doi.org/10.1108/VJIKMS-03-2024-0089
3. Ali, S. S., Khan, S., Fatma, N., Ozel, C., & Hussain, A. (2024). Utilisation of drones in achieving various applications in smart warehouse management. Benchmarking: An International Journal, 31(3), 920–954. https://doi.org/10.1108/BIJ-01-2023-0039
4. Alrabea, K. J., Alsaffar, M., Alsafran, M. A., Alsaber, A., Almutairi, S., Al-Saeed, F., & Alkandari, A. M. (2024). Artificial intelligence and cybersecurity within a social media context: implications and insights for Kuwait. Journal of Science and Technology Policy Management, ahead-of-print(ahead-of-print). https://doi.org/10.1108/JSTPM-12-2023-0224
5. Altalbe, A., & Kateb, F. (2022). Assuring enhanced privacy violation detection model for social networks. International Journal of Intelligent Computing and Cybernetics, 15(1), 75–91. https://doi.org/10.1108/IJICC-05-2021-0093
6. Asbaş, C., & Tuzlukaya, Ş. (2022). Cyberattack and Cyberwarfare Strategies for Businesses. In F. Özsungur (Ed.), Conflict Management in Digital Business (pp. 303–328). Emerald Publishing Limited. https://doi.org/10.1108/978-1-80262-773-220221027
7. Bamhdi, A. M. (2024). Analysis of intangible assets reporting standards and automation in KSA within an Islamic context – a case study. Journal of Islamic Accounting and Business Research, ahead-of-print(ahead-of-print). https://doi.org/10.1108/JIABR-08-2023-0273
8. Bhandal, R., Meriton, R., Kavanagh, R. E., & Brown, A. (2022). The application of digital twin technology in operations and supply chain management: a bibliometric review. Supply Chain Management: An International Journal, 27(2), 182–206. https://doi.org/10.1108/SCM-01-2021-0053
9. Chopra, R., Bhardwaj, S., Thaichon, P., & Nair, K. (2025). Unpacking service failures in artificial intelligence: future research directions. Asia Pacific Journal of Marketing and Logistics, 37(2), 349–364. https://doi.org/10.1108/APJML-03-2024-0393
10. Cook, J., & Cook, J. S. (2025). The dual faces of social media: connectivity and fraud in the digital age. SAM Advanced Management Journal, 90(1), 55–74. https://doi.org/10.1108/SAMAMJ-05-2024-0027
11. Curiello, S., Iannuzzi, E., Meissner, D., & Nigro, C. (2025). Mind the gap: unveiling the advantages and challenges of artificial intelligence in the healthcare ecosystem. European Journal of Innovation Management, ahead-of-print(ahead-of-print). https://doi.org/10.1108/EJIM-01-2024-0078
12. Dakiche, N., Benatchba, K., Benbouzid-Si Tayeb, F., Slimani, Y., & Brahmi, M. A. (2024). Com_Tracker: a two-phases framework for detecting and tracking community evolution in dynamic social networks. Journal of Systems and Information Technology, 26(4), 586–613. https://doi.org/10.1108/JSIT-02-2021-0024
13. de Carvalho, V. D. H., & Costa, A. P. C. S. (2024). Towards corpora creation from social web in Brazilian Portuguese to support public security analyses and decisions. Library Hi Tech, 42(4), 1080–1115. https://doi.org/10.1108/LHT-08-2022-0401
14. Dhamak, P., Aital, P., & Daftardar, A. (2025). A comprehensive overview of Construction 4.0 technologies and their implementation in the construction industry. Journal of Science and Technology Policy Management, ahead-of-print(ahead-of-print). https://doi.org/10.1108/JSTPM-09-2023-0162

15. DSouza, K. M., & French, A. M. (2024). Fake news detection using machine learning: an adversarial collaboration approach. Internet Research, 34(5), 1664–1678. https://doi.org/10.1108/INTR-03-2022-0176
16. Elkhwesky, Z., & Elkhwesky, E. F. Y. (2023). A systematic and critical review of Internet of Things in contemporary hospitality: a roadmap and avenues for future research. International Journal of Contemporary Hospitality Management, 35(2), 533–562. https://doi.org/10.1108/IJCHM-01-2022-0090
17. Foudah, A., Tarek, M., Essam, S., el Hawary, M., Adel, K., & Marzouk, M. (2024). Digital twin publications in construction (2017–2023): a bibliometrics-based visualization analysis. Construction Innovation, ahead-of-print(ahead-of-print). https://doi.org/10.1108/CI-09-2023-0229
18. Ganji, K., & Afshan, N. (2024). A bibliometric review of Internet of Things (IoT) on cybersecurity issues. Journal of Science and Technology Policy Management, ahead-of-print(ahead-of-print). https://doi.org/10.1108/JSTPM-05-2023-0071
19. Graham, C. M. (2025). AI skills in cybersecurity: global job trends analysis. Information & Computer Security, ahead-of-print(ahead-of-print). https://doi.org/10.1108/ICS-09-2024-0235
20. Huang, X., Peng, Y., Li, J., Zhu, G., & Peng, H. (2025). International competitive landscape of administrative intelligent decision-making theory and application: knowledge graph analysis based on literature and patent. Library Hi Tech, ahead-of-print(ahead-of-print). https://doi.org/10.1108/LHT-05-2024-0252
21. Ilie-Zudor, E., Ekárt, A., Kemeny, Z., Buckingham, C., Welch, P., & Monostori, L. (2015). Advanced predictive-analysis-based decision support for collaborative logistics networks. Supply Chain Management: An International Journal, 20(4), 369–388. https://doi.org/10.1108/SCM-10-2014-0323
22. Jemili, F., Jouini, K., & Korbaa, O. (2025). Intrusion detection based on concept drift detection and online incremental learning. International Journal of Pervasive Computing and Communications, 21(1), 81–115. https://doi.org/10.1108/IJPCC-12-2023-0358
23. Kaur, S., Bansal, S., & Sharma, A. (2025). Future Trends and Emerging Possibilities in AI. In B. Singla, K. Shalender, & N. Singh (Eds.), Navigating Data Science (pp. 127–148). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83608-298-920251008
24. Lamboglia, R., Lavorato, D., Scornavacca, E., & Za, S. (2021). Exploring the relationship between audit and technology. A bibliometric analysis. Meditari Accountancy Research, 29(5), 1233–1260. https://doi.org/10.1108/MEDAR-03-2020-0836
25. Lestari, S., Adawiyah, W. R., Alhamidi, A. L., Prayogi, J., & Haryanto, R. (2024). Navigating perilous seas: unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking. Safer Communities, 23(4), 444–464. https://doi.org/10.1108/SC-04-2024-0018
26. Lu, M., & Antwi-Afari, M. F. (2024). A scientometric analysis and critical review of digital twin applications in project operation and maintenance. Engineering, Construction and Architectural Management, ahead-of-print(ahead-of-print). https://doi.org/10.1108/ECAM-03-2024-0304
27. Malik, S., Garg, M., Thomas, A., Cillo, V., & del Giudice, M. (2025). Exploration and prioritization of crucial factors of artificial intelligence adoption in credit risk scoring: using the fuzzy analytical hierarchical process. Business Process Management Journal, ahead-of-print(ahead-of-print). https://doi.org/10.1108/BPMJ-09-2024-0886

28. Marchena Sekli, G. (2024). The research landscape on generative artificial intelligence: a bibliometric analysis of transformer-based models. Kybernetes, ahead-of-print(ahead-of-print). https://doi.org/10.1108/K-03-2024-0554
29. Mohamed, M. A. H., Al-Mhdawi, M. K. S., Ojiako, U., Dacre, N., Qazi, A., & Rahimian, F. (2025). Generative AI in construction risk management: a bibliometric analysis of the associated benefits and risks. Urbanization, Sustainability and Society, 2(1), 196–228. https://doi.org/10.1108/USS-11-2024-0069
30. Mohandes, S. R., Kaddoura, K., Singh, A. K., Elsayed, M. Y., Banihashemi, S., Antwi-Afari, M. F., Olawumi, T. O., & Zayed, T. (2024). Application of a hybrid fuzzy-based algorithm to investigate the environmental impact of sewer overflow. Smart and Sustainable Built Environment, ahead-of-print(ahead-of-print). https://doi.org/10.1108/SASBE-09-2023-0281
31. Nobanee, H., Ellili, N. O. D., Chakraborty, D., & Shanti, H. Z. (2024). Mapping the fintech revolution: how technology is transforming credit risk management. Global Knowledge, Memory and Communication, ahead-of-print(ahead-of-print). https://doi.org/10.1108/GKMC-12-2023-0492
32. Paracha, A., & Arshad, J. (2024). A bibliometric study toward quantitative research assessment of security of machine learning. Information Discovery and Delivery, ahead-of-print(ahead-of-print). https://doi.org/10.1108/IDD-01-2024-0003
33. Pigola, A., & Meirelles, F. de S. (2025). Zero trust in cybersecurity: managing critical challenges for effective implementation. Journal of Systems and Information Technology, ahead-of-print(ahead-of-print). https://doi.org/10.1108/JSIT-08-2024-0326
34. Raj, R., Singh, A., Kumar, V., & Verma, P. (2024). Challenges in adopting blockchain technology in supply chain management: a too far fetched idea? International Journal of Quality & Reliability Management, 41(8), 2146–2180. https://doi.org/10.1108/IJQRM-12-2022-0366
35. Rathore, B., Gupta, R., Biswas, B., Srivastava, A., & Gupta, S. (2022). Identification and analysis of adoption barriers of disruptive technologies in the logistics industry. The International Journal of Logistics Management, 33(5), 136–169. https://doi.org/10.1108/IJLM-07-2021-0352
36. Salim, S., Moustafa, N., & Turnbull, B. (2025). Privacy preservation of Internet of Things–integrated social networks: a survey and future challenges. International Journal of Web Information Systems, ahead-of-print(ahead-of-print). https://doi.org/10.1108/IJWIS-04-2024-0120
37. Shahzadi, G., Jia, F., Chen, L., & John, A. (2024). AI adoption in supply chain management: a systematic literature review. Journal of Manufacturing Technology Management, 35(6), 1125–1150. https://doi.org/10.1108/JMTM-09-2023-0431
38. Shammar, E. A., & Zahary, A. T. (2020). The Internet of Things (IoT): a survey of techniques, operating systems, and trends. Library Hi Tech, 38(1), 5–66. https://doi.org/10.1108/LHT-12-2018-0200
39. Sharma, H., Anubha, A., & Narang, D. (2025). Transformation in Human–Computer Interaction: The AI-Enabled NLP. In A. Behl, C. Krishnan, P. Malik, & S. Gautam (Eds.), The ChatGPT Revolution (pp. 39–56). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83549-852-120251003
40. Shukla, A., & Kashni, T. (2025). Bibliometric analysis of banking frauds and scams literature. Journal of Financial Crime, 32(3), 729–750. https://doi.org/10.1108/JFC-08-2024-0252
41. Singh, S., Singh, S., & Kajla, T. (2023). Checking the Effectiveness of Blockchain Application in Fraud Detection with A Systematic Literature Review Approach. In S. Grima, K. Sood, & E. Özen

(Eds.), Contemporary Studies of Risks in Emerging Technology, Part B (pp. 57–86). Emerald Publishing Limited. https://doi.org/10.1108/978-1-80455-566-820231003

42. Song, Z., & Zhu, J. (2022). Blockchain for smart manufacturing systems: a survey. Chinese Management Studies, 16(5), 1224–1253. https://doi.org/10.1108/CMS-04-2021-0152
43. Sultan, L., & Maqableh, M. (2025). Emerging Cyber Threats From the Dark Web: Implications for Cybersecurity. In R. Masa'deh (Ed.), The Role of Artificial Intelligence Applications in Business (pp. 141–158). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83662-518-620251010
44. Thavi, R., Jhaveri, R., Narwane, V., Gardas, B., & Jafari Navimipour, N. (2024). Role of cloud computing technology in the education sector. Journal of Engineering, Design and Technology, 22(1), 182–213. https://doi.org/10.1108/JEDT-08-2021-0417
45. Trincanato, E., & Vagnoni, E. (2024). Business intelligence and the leverage of information in healthcare organizations from a managerial perspective: a systematic literature review and research agenda. Journal of Health Organization and Management, 38(3), 305–330. https://doi.org/10.1108/JHOM-02-2023-0039
46. Tyagi, S. (2024). Analytics in healthcare supply chain management in the new normal era: a review and future research agenda. Benchmarking: An International Journal, 31(6), 2151–2175. https://doi.org/10.1108/BIJ-03-2023-0155
47. Wu, Y., Ngai, E. W. T., Wu, P., & Wu, C. (2022). Fake news on the internet: a literature review, synthesis and directions for future research. Internet Research, 32(5), 1662–1699. https://doi.org/10.1108/INTR-05-2021-0294
48. Yadav, S., Prakash, A., Arora, M., & Mittal, A. (2024). Digital transformation: exploring cornerstones for construction industry. Kybernetes, 53(12), 5378–5401. https://doi.org/10.1108/K-05-2023-0895
49. Yeboah-Ofori, A., Swart, C., Opoku-Boateng, F. A., & Islam, S. (2022). Cyber resilience in supply chain system security using machine learning for threat predictions. Continuity & Resilience Review, 4(1), 1–36. https://doi.org/10.1108/CRR-10-2021-0034
50. Goyal, R., & Somani, A. (2026). A novel approach to adversarial attack detection in machine learning models for cybersecurity applications. International Journal for Multidisciplinary Research, 8(1). https://doi.org/10.36948/ijfmr.2026.v08i01.69106