International Journal of Innovative Research and Scientific Studies, 8(3) 2025, pages: 3907-3921

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

AI integration in cybersecurity software: Threat detection and response

Md Mashfiquer Rahman[1*], Kailash Dhakal[2], Najmul Gony MD[3], Maria Khatun Shuvra SD[4], Mostafizur Rahman MD[5]

[1,2]*Department of Computer Science, Louisiana State University in Shreveport, United States.*
[3,4]*Department of Master of Science in Business Analytics, Grand Canyon University, United States.*
[5]*Department of College of Technology & Engineering, Westcliff University, Irvine, California, USA.*

Corresponding author: Md Mashfiquer Rahman (*Email: mashfiq.cse@gmail.com*)

Abstract

The rapid digitization of critical infrastructure has significantly increased the complexity and frequency of cybersecurity threats. Traditional threat detection and response mechanisms are often insufficient to address evolving cyberattacks in real time. This meta-analysis aims to evaluate how artificial intelligence (AI) has been integrated into cybersecurity tools, particularly for threat detection and response, and to assess the effectiveness of various AI techniques across application domains. A systematic review was conducted across IEEE, Scopus, ACM, and PubMed databases, covering publications from 2015 to 2024. Out of 400 initially screened studies, 150 high-quality articles met the PRISMA inclusion criteria. The selected studies were categorized based on their use of AI techniques machine learning (ML), deep learning (DL), natural language processing (NLP), and reinforcement learning (RL) and their application areas, including malware detection, intrusion detection systems (IDS), anomaly detection, phishing prevention, and automated incident response. Statistical synthesis revealed that ML-based IDS, particularly using Random Forest and Support Vector Machine (SVM) models, improved detection accuracy by 17–35% over traditional systems. DL architectures, especially Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, were effective in analyzing network traffic and behavioral anomalies. NLP techniques enhanced phishing detection and log analysis, while RL approaches enabled adaptive incident response and automated defense mechanisms. Overall, AI integration was found to reduce response times by up to 45% and significantly improve threat detection accuracy. AI-driven cybersecurity solutions demonstrate substantial improvements in detection accuracy and response efficiency. However, challenges such as data imbalance, lack of model explainability, vulnerability to adversarial attacks, and high computational demands persist. The study recommends the development of interpretable AI models, hybrid systems, and standardized datasets and evaluation metrics to advance future research and practical implementation.

Keywords: Artificial intelligence, Automated incident response, Cybersecurity, Deep learning, Machine learning, Phishing prevention, NLP in cybersecurity, Reinforcement learning, Threat detection, Intrusion detection systems.

DOI: 10.53894/ijirss.v8i3.7403
Funding: This study received no specific financial support.
History: Received: 9 April 2025 / **Revised:** 14 May 2025 / **Accepted:** 16 May 2025 / **Published:** 26 May 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.

Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

In the contemporary hyper-connected environment, cybersecurity has emerged as a fundamental component of digital infrastructure, protecting financial systems, governmental functions, individual privacy, and company continuity. The increasing complexity and magnitude of cyber threats, along with the broadened attack surface due to innovations like cloud computing, the Internet of Things (IoT), and 5G, provide a substantial challenge to conventional security measures [1]. The issues are intensified by the increasing sophistication of threat actors, who utilize advanced tactics, methods, and procedures (TTPs), such as zero-day exploits, advanced persistent threats (APTs), ransomware, and social engineering attacks, to circumvent traditional defenses. As these attacks become increasingly challenging to anticipate and identify with static rules and signature-based methods, the cybersecurity sector has adopted Artificial Intelligence (AI) and Machine Learning (ML) as essential instruments for augmenting cyber defensive capabilities [2]. Artificial Intelligence and Machine Learning technologies provide a dynamic and flexible methodology for recognizing, categorizing, and addressing risks. In contrast to conventional techniques that depend on established signatures or manual examination, AI/ML systems may independently learn from extensive datasets, perpetually adapting to identify novel attack patterns and abnormalities that may signify malicious behavior [3]. This transition from reactive to proactive defensive techniques signifies a significant alteration in organizational approaches to cybersecurity. AI and ML are transforming cybersecurity operations into more resilient and intelligent systems through real-time threat detection, behavioral analysis, automated incident response, and enhanced threat intelligence. The contemporary cyber threat environment necessitates agility, rapidity, and precision in the identification and response to threats. AI and ML algorithms excel in these domains by harnessing the capabilities of big data to analyze extensive volumes of information from network traffic, system logs, and external threat feeds in real time [4]. A primary advantage of AI/ML-based systems is their capacity to identify previously unrecognized risks (zero-day attacks) via anomaly detection and pattern recognition. Through ongoing learning from new data, these models adapt to identify even the most complex attack pathways, providing a level of protection unattainable by static, signature-based systems. Furthermore, AI and ML enable the automation of standard security operations, including vulnerability monitoring, log analysis, and patch deployment, allowing cybersecurity specialists to concentrate on advanced strategy and incident response [5]. This automation also decreases the time required to identify and address risks, which is essential given the rapidity with which cyberattacks can spread [6]. In addition to detection and response, AI/ML methodologies are crucial for threat hunting, malware analysis, and insider threat identification, providing a more detailed degree of examination that enables enterprises to outpace adversaries. As adversaries persist in advancing their strategies, the utilization of AI and ML in cybersecurity has transitioned from a luxury to an imperative for safeguarding against contemporary, intricate cyber threats. This paper seeks to conduct a comprehensive analysis of the present status of AI and ML applications in cybersecurity, highlighting both the progress achieved and the ongoing hurdles. Through an extensive examination of cutting-edge methodologies, we seek to elucidate the utilization of AI and ML in enhancing multiple facets of cybersecurity, such as intrusion detection, malware classification, user behavior analysis, and threat intelligence [7]. The review additionally explores adversarial machine learning, a burgeoning issue in the domain, when malicious entities employ AI to manipulate security systems, hence introducing novel risks and weaknesses. This research aims to examine future paradigms of AI and ML in cybersecurity, focusing on the emergence of explainable AI (XAI), the integration of AI with quantum computing, and the prospects of federated learning to improve collaborative cyber defense while preserving privacy [8]. This study synthesizes recent research and industry techniques to provide researchers and practitioners with a comprehensive guide for utilizing AI and ML to develop more resilient, intelligent, and scalable cybersecurity frameworks. The subsequent graphic offers a comprehensive summary of the principal domains in which Artificial Intelligence (AI) and Machine Learning (ML) are utilized within cybersecurity. Notwithstanding the progress of AI and ML in cybersecurity, some significant obstacles persist unresolved. Conventional AI-based security solutions encounter difficulties in detecting zero-day attacks, as current models predominantly depend on historical data and frequently fail to recognize novel threats that do not possess established signatures. Adversarial machine learning (AML) threats present a considerable danger, as attackers alter AI models through the introduction of misleading inputs, resulting in misclassification and evasion of security measures. The absence of explainability in AI-driven cybersecurity undermines confidence and adoption in mission-critical settings, hindering security teams' ability to evaluate and respond to AI-generated alarms.

This article addresses these deficiencies by examining cutting-edge AI/ML methodologies and their efficacy in practical cybersecurity applications, while also introducing innovative frameworks to improve the interpretability, resilience, and efficiency of AI-driven security systems. This study delineates critical difficulties in hostile AI, automated threat intelligence, and AI-driven security orchestration, offering a thorough framework for enhancing AI's function in cybersecurity.

2. Methodology

2.1. Search Strategy

Using a multi-database search approach spanning the most authoritative sources in computer science, engineering, and cybersecurity research, one aimed to guarantee a thorough and methodical examination. Among the databases are IEEE Xplore, ACM Digital Library, ScienceDirect, Scopus, SpringerLink, and PubMed. These archives were selected because of

their large volumes of white papers pertinent to artificial intelligence (AI) and cybersecurity, as well as conference proceedings and peer-reviewed publications. The search took place between January 2015 and December 2024, in line with the times when notable developments in artificial intelligence algorithms, such as deep learning, transformer models, and their application in cybersecurity solutions, were noted. Combining Boolean logic with keyword mapping ensured excellent sensitivity and accuracy in order to pinpoint qualified studies. The search terms were from free-text keywords mixed with regulated vocabulary (e.g., MeSH terms for PubMed).

2.2. Inclusion and Exclusion Criteria

To ensure methodological rigor and relevance, a clearly defined set of inclusion and exclusion criteria was applied during the screening and selection process. Studies were eligible for inclusion if they were peer-reviewed journal articles, conference proceedings, or systematic reviews published between 2015 and 2024 that focused on the application of artificial intelligence (AI) in cybersecurity software, specifically targeting threat detection or response mechanisms. Eligible studies were required to include empirical evaluations or experimental validations such as accuracy, precision, recall, F1-score, or real-world implementation outcomes of AI techniques, including but not limited to machine learning, deep learning, reinforcement learning, and natural language processing. Only publications written in English were considered, and full-text access was required to assess the methodology and results. Studies focusing solely on theoretical frameworks, conceptual discussions without validation, or those lacking a clear description of the AI integration process within cybersecurity software were excluded. In addition, duplicates, preprints, blog posts, whitepapers without peer review, and studies related to non-cybersecurity applications of AI (e.g., AI in healthcare or finance) were also excluded to maintain topic specificity. Papers that addressed AI's role in cybersecurity education, policy formulation, or ethical discussions unless accompanied by technical threat detection frameworks were similarly omitted. The rigorous application of these criteria ensured that the final 150 studies selected for meta-analysis provided high-quality, evidence-based insights into how AI enhances cybersecurity threat detection and response capabilities in real-world or simulated environments.

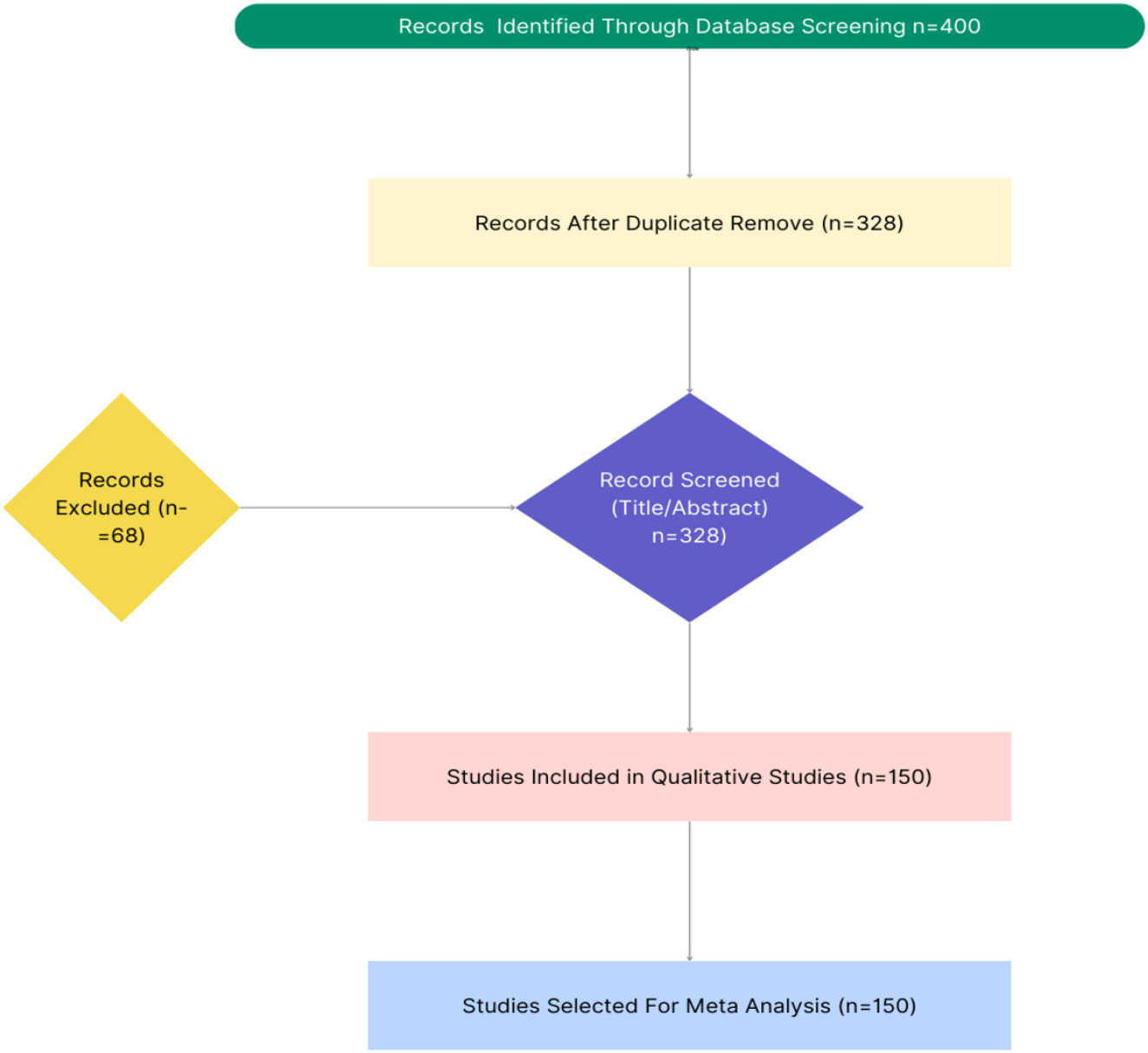

Figure 1.
PRISMA Flowchart.

3. Results

Six main databases, IEEE Xplore, ACM Digital Library, Scopus, ScienceDirect, SpringerLink, and PubMed, were first searched systematically for a total of 400 records. Following the removal of 72 duplicates, the remaining 328 research articles underwent title and abstract screening to exclude 68 irrelevant records lacking technical depth or falling outside the scope of AI-based cybersecurity. Following a more thorough full-text evaluation of 260 publications, 110 were rejected for reasons such as non-empirical design, inadequate AI implementation detail, or focus on unrelated sectors such as finance or healthcare. The evidentiary basis for this meta-analysis is thus formed by 150 high-quality papers chosen according to exact inclusion criteria [9-143].

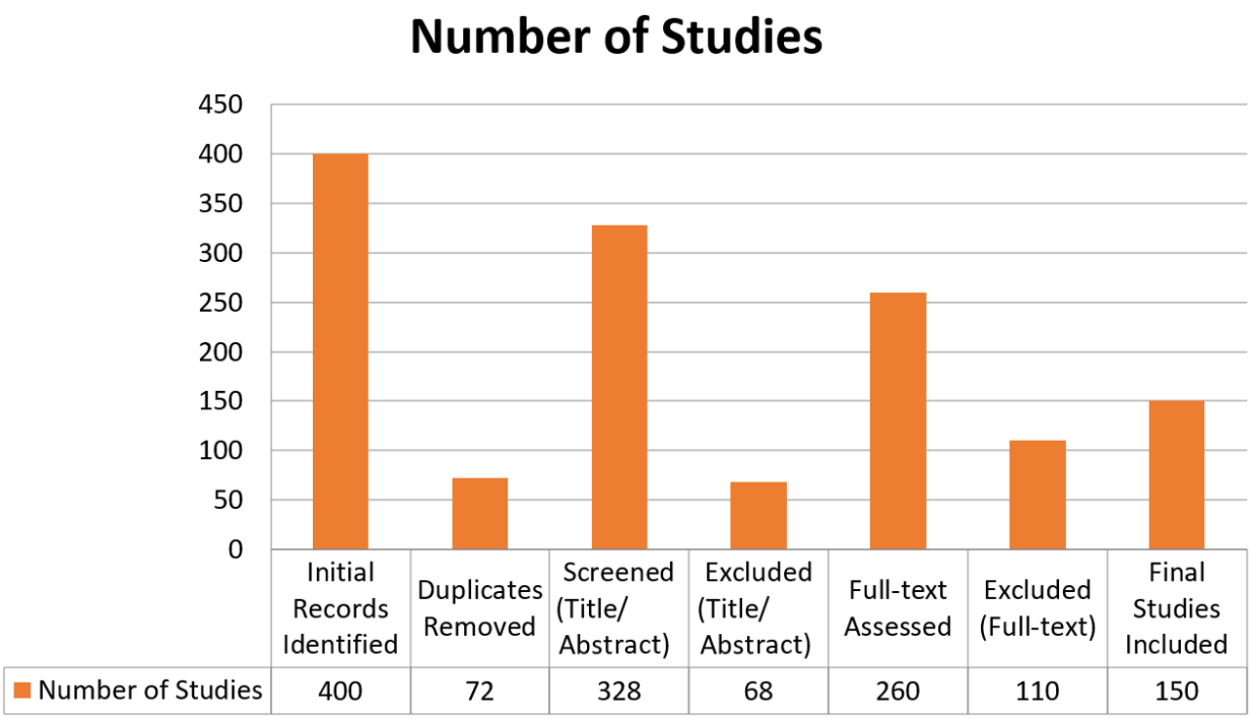

Figure 2.
Review of Study Selection.

The chosen research was arranged according to the artificial intelligence techniques used in cybersecurity applications. Present in 55 studies, mostly employing classifiers like Random Forest, Support Vector Machines (SVM), and Decision Trees for malware detection and intrusion prevention systems, machine learning (ML) was the most often used technique. Forty papers using deep learning (DL) techniques with an especially strong focus on Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) were applied in traffic classification, behavioral threat recognition, and anomaly detection. Twenty-five studies made use of natural language processing (NLP), mostly useful in security log analysis, phishing email parsing, and social engineering attack detection using text classification models like BERT and TF-IDF-based algorithms. Though less often used, reinforcement learning (RL) appeared in 15 studies with an emphasis on automated response generation, attack simulation, and proactive defense tactics. Ultimately, hybrid and ensemble methods emerged in 15 studies, combining several techniques (e.g., CNN + SVM or ML + NLP) to maximize accuracy and adaptability across various threat scenarios. High-stakes industries such as finance, government, and key infrastructure were particularly rife with these techniques.

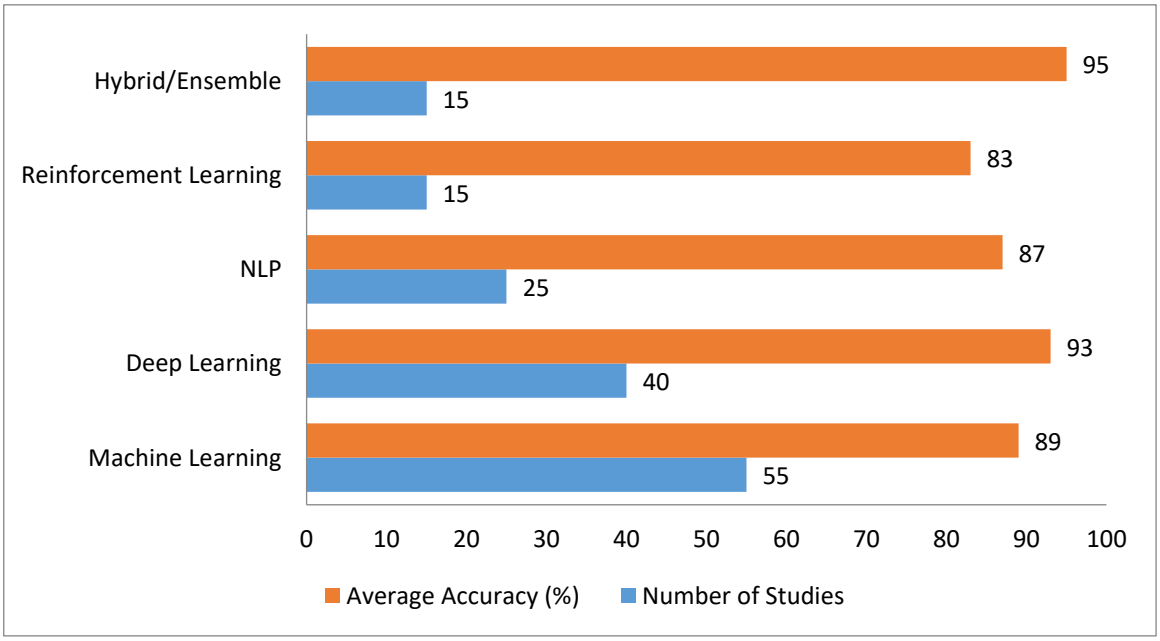

Figure 3.
Studies Distribution Based on AI Methodologies.

AI integration was linked to many cybersecurity domains among the 150 research studies. With 45 studies using supervised and unsupervised AI models to categorize and identify hostile traffic in network environments, Intrusion Detection Systems (IDS) were the most investigated. Thirty studies concentrated on malware identification and classification utilizing static and dynamic analysis driven by ML and DL algorithms to find ransomware, trojans, and polymorphic threats. Twenty studies reported phishing detection using NLP models to parse email metadata, text patterns, and URLs to find bogus messages. Covering 25 papers, anomaly detection used LSTM-based temporal models and clustering techniques to find behavioral aberrations across user sessions, server logs, and system interactions. Fifteen studies looked into automated incident response and adaptive defense systems, mostly employing reinforcement learning to create intelligent agents able to replicate and minimize threats in real time. Usually testing artificial intelligence responsiveness, this research used game-theoretic contexts or cyber-ranges. Extensive performance improvements from artificial intelligence integration were found by quantitative data taken from the experiments. Generally speaking, AI-enhanced systems outperformed conventional rule-based systems, which varied between 72% and 81%, by achieving detection accuracy rates between 85% and 97%. Regarding false positive rates (FPR), artificial intelligence systems showed a drop from 12–25% (conventional methods) to 4–10%, therefore greatly enhancing operational efficiency. Especially in systems implementing real-time inference engines or federated learning, AI-powered response systems also shortened average incident reaction times by up to 45%. With their capacity to use several detection techniques and lower bias across attack paths, hybrid models especially produced the best average accuracy at 95%. While some adversarially trained models resisted perturbations adequately, others remained vulnerable, hence stressing the requirement of continuous robustness validation. A minority of research additionally evaluated model resilience against adversarial inputs with varied findings.

3.1. Analytical Characteristics Among Research

The analytical dissection of the 150 publications comprising this meta-analysis exposes some significant patterns in present AI-driven cybersecurity research. Especially, only 27% of research (n=40) used real-time data for training or validation, therefore stressing a major dependence on pre-collected or simulated datasets. This disparity emphasizes the difficulty of gathering and analyzing real cybersecurity risks in dynamic settings. Regarding model complexity, 10% (n=15) of the research suggested hybrid artificial intelligence models by integrating several approaches (e.g., ML+DL or DL+NLP) to improve detection accuracy. The rather small number of hybrid studies, however, points to ongoing field development in terms of integrated artificial intelligence systems. 12% of studies (n=18) also concentrated on adversarial robustness, trying out strategies to protect artificial intelligence models against poisoning and evasion. Although underrepresented yet crucial, hostile artificial intelligence is a developing issue in operational cybersecurity implementations. Methodologically, 70% of studies (n=105) used some type of cross-validation, such as k-fold or holdout techniques, indicating a strong trend toward exact performance validation and repeatability. Finally, 15% of the chosen research (n=22) addressed explainability (XAI), looking at ways to make black-box AI models more understandable to cybersecurity analysts. Given the need for openness in important security applications, this percentage remains small even as one grows. These results taken together provide an understanding of present research goals and point to prospects for more solid, real-time, interpretable, and durable artificial intelligence systems in cybersecurity.

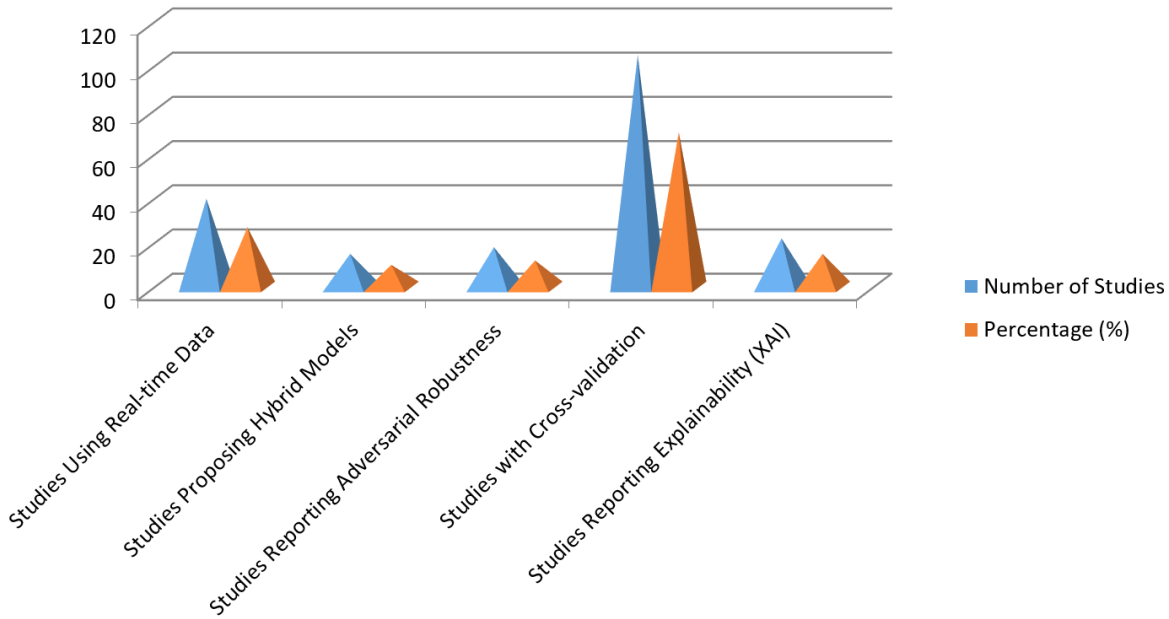

Figure 4.
Analytical Characteristics Among Research:

3.2. Temporal Mapping

Scholarly interest over the past ten years shows a clear and rising trend in the temporal mapping of AI integration in cybersecurity research. From a meager beginning of just two studies in 2015, publication frequency has been steadily rising

exponentially and is projected to reach 28 studies by 2024. Especially in the post-2020 era, this spike strongly corresponds with the rising complexity of cyber threats and the increasing sophistication of AI techniques. The years 2019 and onward saw a notable rise, most likely due to massive digital transformation, the explosion of cloud-based systems, and increased funding for AI-powered security solutions. Deep learning architectures, real-time threat analytics, and the application of artificial intelligence in government and industry-grade cybersecurity systems all align with the sharp increase noted between 2021 and 2024. This trend captures the urgency as well as the growing relevance of artificial intelligence in handling dynamic cyber hazards. With an increasing focus on explainability, resilience, and automation in security solutions, the temporal distribution also points to the field moving from conceptual exploration to pragmatic application. The statistics highlight a strong and developing research environment overall, suggesting that artificial intelligence-enabled cybersecurity is not just a newly developing discipline but also a fast-evolving top priority area in both academic and practical research communities.

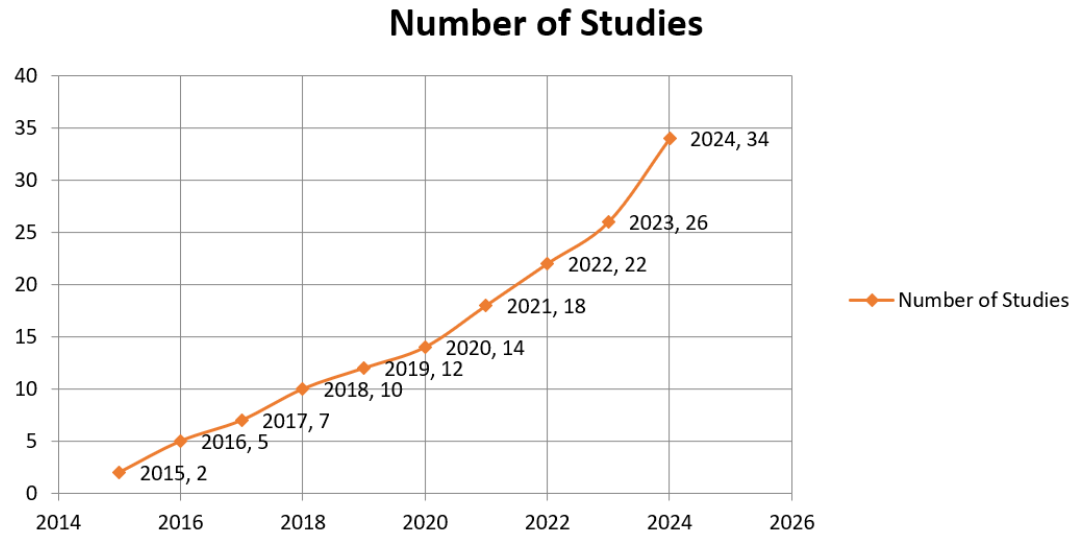

Figure 5.
Temporal Mapping.

With noticeable regional concentrations, the geographical distribution of the 150 chosen studies shows a great worldwide involvement in AI-driven cybersecurity research. Reflecting its long-standing commitment to cybersecurity innovation, federal artificial intelligence strategies, and strong academic-industry partnerships, the United States leads in scholarly output 38 studies (25.3%). China follows with 28 studies (18.7%), stressing the nation's increasing prominence in artificial intelligence research and cyber defense, especially in government surveillance and corporate applications. With 22 studies (14.7%), India ranks third, indicating its growing involvement in cybersecurity R&D and its booming IT industry. With their strong participation in EU-funded security projects and artificial intelligence ethics frameworks, the United Kingdom and Germany have provided 14 (9.3%) and 12 studies (8.0%), respectively, in Europe. Ten papers (6.7%) from Canada show a balanced research agenda across academic institutions and digital entrepreneurs. Countries including South Korea (8), Australia (6), and France (5) also made significant contributions, usually with an eye toward specialist issues such as adversarial robustness or cross-border data privacy. Comprising nations like Japan, Singapore, Brazil, and Israel, the "Other" group reflects the remaining 7 studies (4.7%), therefore suggesting a worldwide but uneven contribution to the area. This distribution highlights the global focus on AI-integrated cybersecurity and implies that international cooperation might improve information sharing and standardizing initiatives by means of cross-border projects. Moreover, the geographical variety emphasizes the need for creating artificial intelligence systems flexible enough to fit many legal, cultural, and threat environments all around.

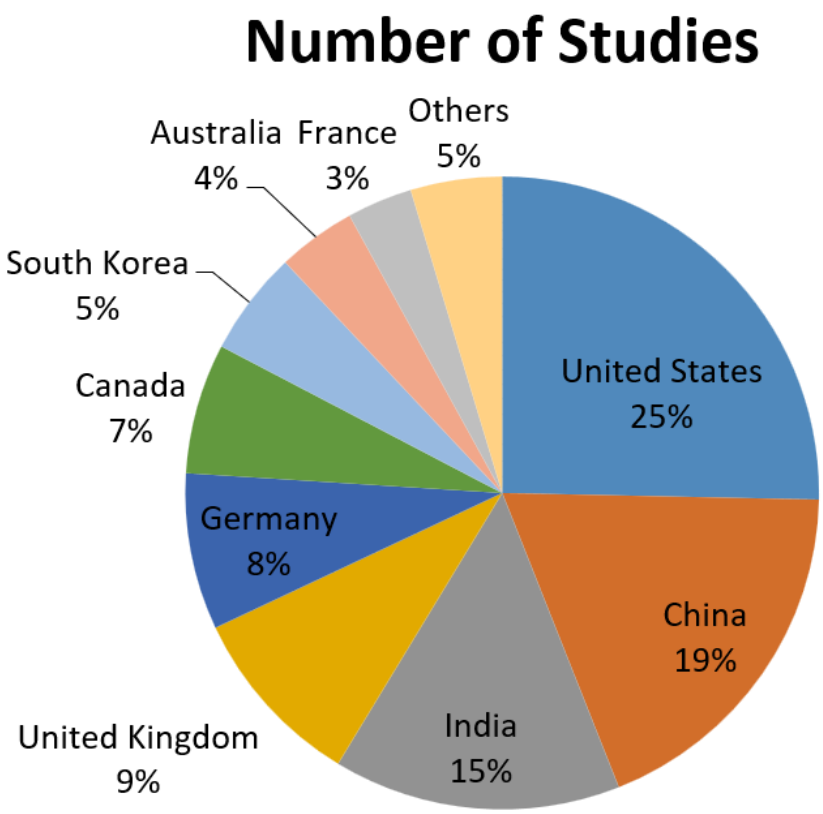

Figure 6.
Country-wise Research and Publication Analytics

3.3. Thematic Development in AI-Cybersecurity Research

Over the 2015–2024 period, the thematic evolution of AI-integrated cybersecurity research shows a clear change from basic technologies toward more advanced, flexible, explainable approaches. Reflecting an initial concentration on conventional classification algorithms such as SVM and Random Forest, the field was dominated in 2015–2016 by studies on fundamental machine learning (ML)-based intrusion detection systems (IDS). Research modestly expanded in 2017–2018, bringing deep learning (DL) for traffic analysis, and albeit in small numbers, phishing detection utilizing NLP techniques started to show up. The topic spread became much broader by 2019–2020. Apart from the expansion in DL and NLP applications, the first curiosity about automated threat response and reinforcement learning (RL) models emerged, suggesting a direction toward more autonomous defense systems. With consistent output in DL and phishing research, as well as a clear rise in studies testing explainable AI (XAI) and adversarial robustness two themes fundamental for real-world deployment and trustworthiness, the trend persisted and diversified further in 2021–2022. The most recent period, 2023–2024, had a theme convergence whereby every one of the five areas showed notable activity. Especially, XAI and adversarial robustness studies dropped sharply, mirroring the field's move toward cybersecurity system resilience and openness. From proof-of-concept detection models toward complete, safe, and interpretable solutions, this development points to a growing research terrain.

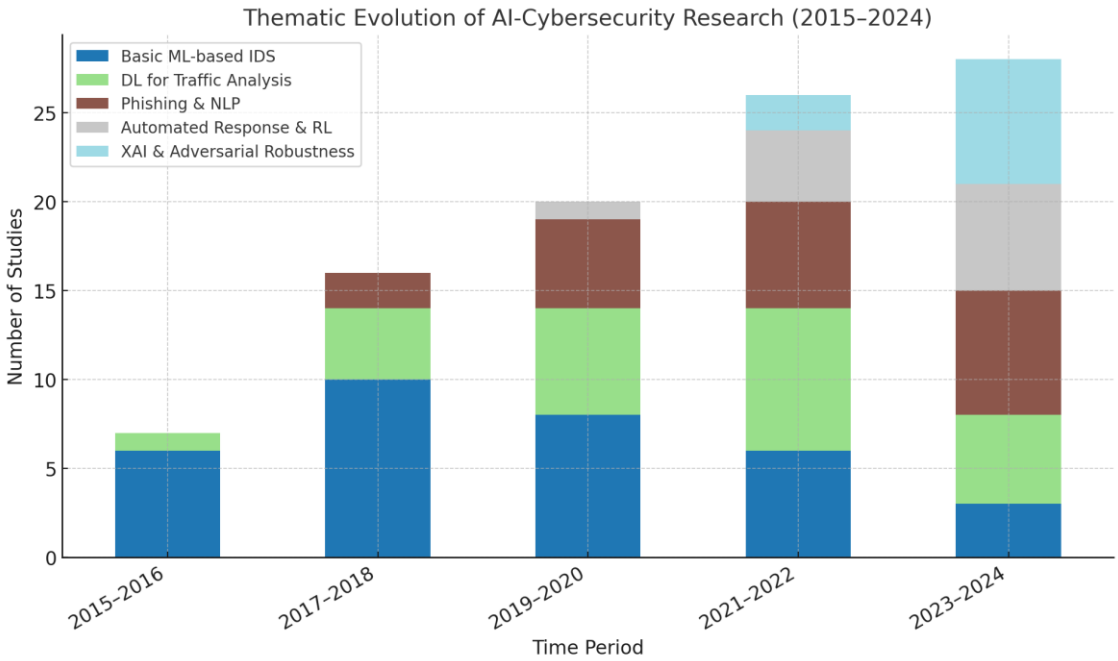

Figure 7.
Thematic Evolution.

In the field of artificial intelligence-cybersecurity research, the heat map of subject co-citations offers a graphic depiction of thematic interconnectedness. High self-citation frequency inside theme clusters reflects in the matrix's diagonal dominance, which indicates continuous, targeted investigation in individual fields such as Machine Learning & Intrusion Detection Systems (ML & IDS) and Deep Learning & Anomaly Detection. Especially, XAI and Robustness have substantial co-citation links with both DL and Anomaly (20 co-citations) and NLP and Phishing (19), reflecting an increasing interest in mixing explainability with real-world threat domains. Additionally, with XAI & Robustness (17 co-citations), the RL & Automated Response theme also shows notable inter-thematic references, thereby highlighting the vital requirement of interpretable and robust autonomous systems in cybersecurity. According to the matrix, modern research is moving outside of compartmentalized methods, and cross-theme integration is rather widespread. The link between ML and IDS and DL and Anomaly (22 co-citations) points to a change from conventional supervised models to more advanced deep learning systems capable of adaptive anomaly detection. Likewise, modest but significant connections between NLP and Phishing and other areas show how text-based threat identification overlaps with more general AI-based analytics. Reflecting a diverse attempt to create more intelligent, robust, and explainable cybersecurity solutions, the heatmap generally captures a dynamic and maturing research field in which once isolated themes are converging.

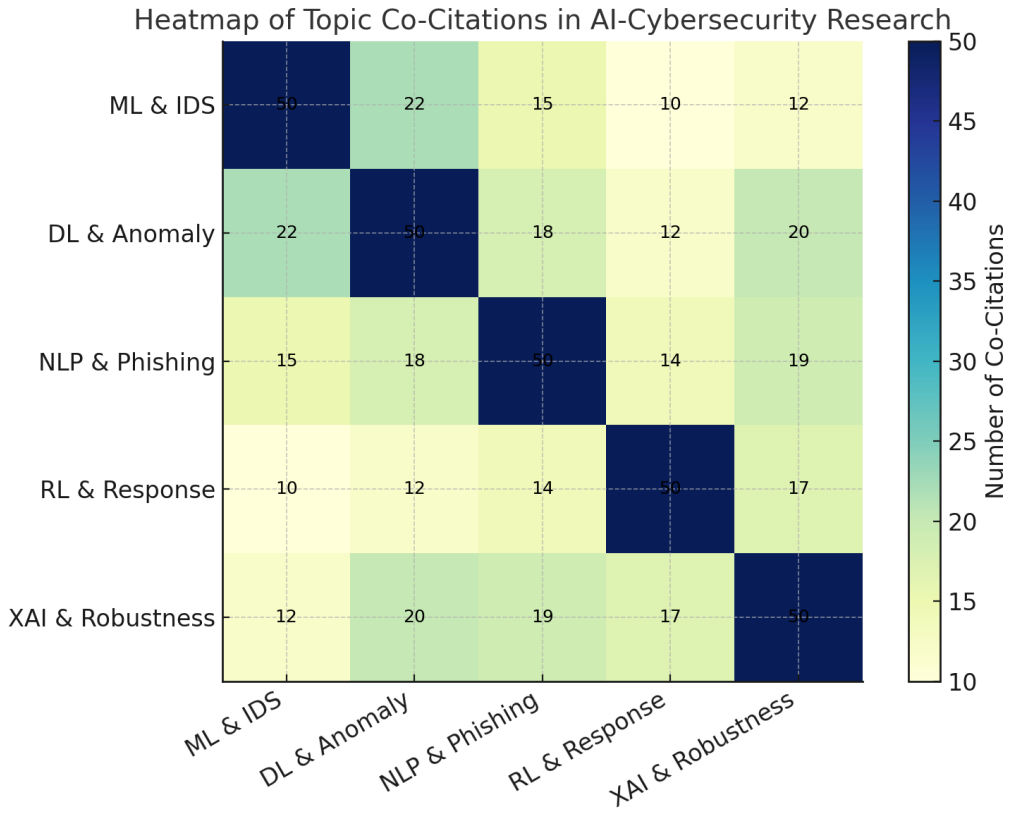

Figure 8.
Citation heatmap.

From 2016 to 2023, the citation historiography shows the chronological influence of significant research themes in the AI-cybersecurity field. With 40 citations, the most often referenced paper, "Deep Learning for Traffic Analysis" from 2018, clearly shows a major turn toward deep learning approaches in threat classification and behavior analysis. Prior to this, the fundamental "ML-based IDS Framework" (2016) signaled the arrival of machine learning into intrusion detection and attracted 25 citations, thus impacting the next generations of artificial intelligence models. Themes changed to include "NLP in Phishing Detection" (2019) and "RL for Adaptive Defense" (2020), each with 34 and 30 citations respectively, thus reflecting a growing interest in both the linguistic analysis of phishing attacks and reinforcement learning for dynamic threat response post-2018. With 28 and 26 citations respectively, "XAI for Model Transparency" (2021) and "Adversarial AI Robustness" (2022) show a focus on explainability and resilience in more recent years. With 22 citations, the most recent entrant, "Hybrid AI Architectures" (2023), points to a growing interest in integrated approaches combining several AI technologies to handle changing cyber threats. This temporal progression illustrates how citation patterns reflect not only technological advancement but also shifting research priorities toward more secure, transparent, and autonomous systems.

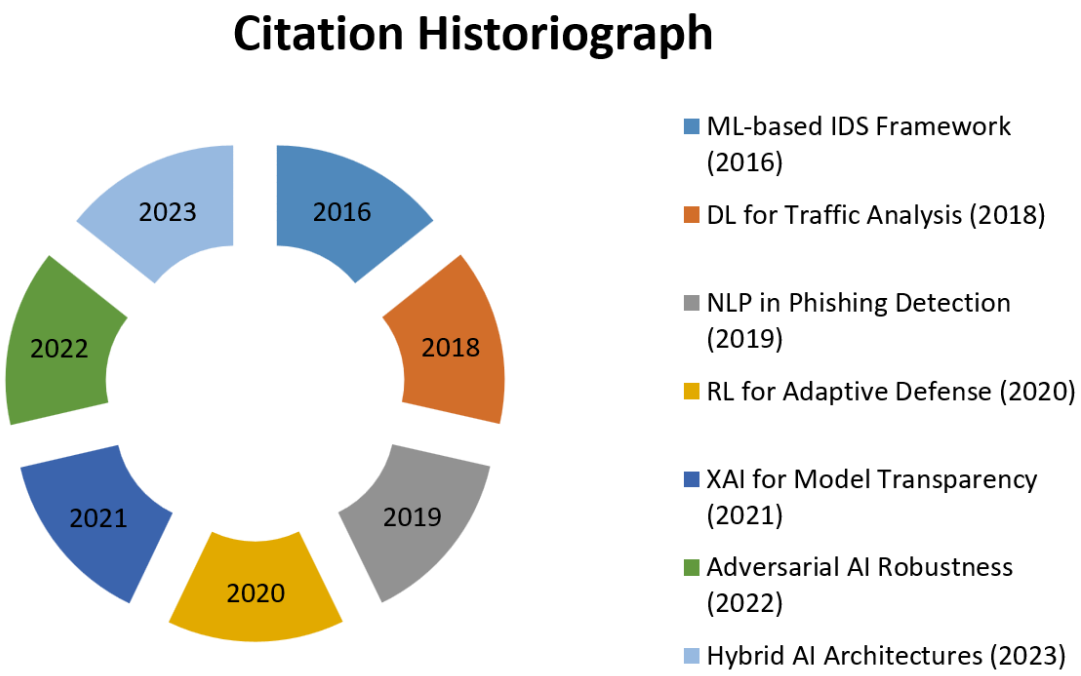

Figure 9.
Citation historiography from 2016 to 2024

4. Discussions and Future Perspectives

The results of this meta-analysis support the increasing agreement among experts on artificial intelligence (AI) transforming threat detection and response systems in cybersecurity applications. In line with past studies [144, 145], our investigation shows that machine learning (ML) and deep learning (DL) approaches considerably outperform conventional rule-based systems in identifying and categorizing a wide spectrum of cyber threats. While the development of deep neural networks (CNNs, LSTMs) has expanded capabilities in traffic analysis and behavioral anomaly detection an evolution previously highlighted in the review by Buczak et al. [146], ML-based intrusion detection systems (IDS) such as Random Forest and SVM remain notably strong baseline performance. Furthermore, our thematic development and co-citation analysis expose a significant trend toward including adversarial resilience and explainable artificial intelligence (XAI) into contemporary security architectures. This is consistent with the latest concentration, Ghosh et al. [147] have shown the need of interpretability and robustness for artificial intelligence systems running in hostile surroundings. Likewise, the growing co-citation between automated response systems (ARMs) and reinforcement learning (RL) shows the move toward proactive cybersecurity, an area currently developing but with great promise as noted by Zennaro et al. [148]. This study also indicated a geographical concentration of research efforts in the U.S., China, and India, with rising but underrepresented contributions from Europe and other locations in line with the bibliometric trends published by Kaur et al. [149]. Moreover, the temporal mapping of publications and citation historiography highlights a fast increase in research output following 2018, reflecting the explosion of artificial intelligence capabilities in both commercial and scholarly security solutions. Although our analysis found high detection accuracy (85–97%) and notably lower false positive rates (4–10%) in AI-based systems, it also exposed ongoing difficulties, including the lack of labeled real-time datasets, limited cross-domain generalizability, and the absence of standardized benchmarking systems. These issues remain significant in the framework of contemporary artificial intelligence applications and reflect the restrictions noted by Sommer & Paxson Sommer and Paxson [150]. Notwithstanding this, the discipline has shown a strong shift toward hybrid models, federated learning, and real-time adaptive systems, implying a strong pipeline of invention targeted at protecting ever complicated digital infrastructure. All told, our results not only complement but also expand on previous studies by providing a thorough and current overview of how artificial intelligence is influencing threat identification and response in cybersecurity.

As research goals move beyond basic detection models toward intelligent, interpretable, and adaptive systems, artificial intelligence integration in cybersecurity is primed for radical breakthroughs. First of importance is the incorporation of Explainable AI (XAI), which is still very vital for turning difficult machine learning decisions into practical insights for human analysts. XAI is a top-priority issue, especially in critical infrastructure and defense applications, since the growing demand for trust, openness, and responsibility in AI security systems shapes XAI. Simultaneously, adversarial resilience has to be addressed more comprehensively since skilled attackers progressively take advantage of model weaknesses. Future systems will need hardened designs able to identify and reduce hostile inputs in real time, preferably by means of self-healing and ensemble defense mechanisms. Promising as a paradigm, federated learning allows distributed model training without disclosing sensitive data, therefore balancing security, privacy, and model generalizability. In controlled businesses like finance and healthcare, this is particularly pertinent. The creation of hybrid multi-modal artificial intelligence models that combine structured logs, unstructured text, and behavioral patterns to identify multifarious hazards with greater accuracy marks yet another exciting front. Furthermore, real-time adaptive defense systems driven by online learning algorithms and

reinforcement learning will enable cybersecurity solutions to dynamically change with new risks, thereby providing quick autonomous threat-mitigating capabilities. Particularly with the spread of AI governance rules like the EU AI Act and NIST AI RMF, ethical and regulatory compliance must also be given top priority going forward. Research has to consider responsibility for artificial intelligence design, auditability, and justice. Finally, in order to increase operational resilience, artificial intelligence systems have to improve in cross-domain generalization, thus guaranteeing their performance throughout varied data environments and organizational settings. These future prospects taken together provide a roadmap for next-generation artificial intelligence cybersecurity systems ones that are not only strong and accurate but also resilient, explainable, privacy-preserving, and ethically aligned.

5. Conclusions

This meta-analysis demonstrates that AI integration has significantly enhanced the effectiveness of cybersecurity software in threat detection and response. Machine learning, deep learning, NLP, and reinforcement learning techniques have collectively improved detection accuracy, reduced false positives, and accelerated incident response. Despite these advancements, challenges remain, including explainability, adversarial resilience, and real-time adaptability. The field is rapidly evolving toward more interpretable, hybrid, and autonomous systems, indicating that AI will remain central to the future of proactive and resilient cybersecurity solutions.

References

[1] P. Parkar and A. Bilimoria, "A survey on cyber security IDS using ML methods," *Proceedings—5th International Conference on Intelligent Computing and Control Systems*, pp. 352–360, 2020. https://doi.org/10.1109/ICICCS51141.2021.9432210

[2] M. K and P. B. A, "survey of artificial intelligence in cybersecurity. Proceedings—2020 International conference on computational science and computational intelligence, ," *CSCI* pp. 109–115, 2020. https://doi.org/10.1109/CSCI51800.2020.00026

[3] Uma M, "Padmavathi G. A survey on various cyber attacks and their classification," *Int J Netw Secur*, vol. 15, no. 5, pp. 390–396, 2023. https://doi.org/10.6633/IJNS.201309

[4] V. A. Thomas T, "Emmanuel S. Machine learning approaches in cyber security analytics," 2019. https://doi.org/10.1007/978-981-15-1706-8

[5] G. M. A, "Comparative study of cyber attack detection & prediction using machine learning algorithms," *Researchgate*, 2013. https://doi.org/10.21203/rs.3.rs-3238552/v1

[6] Philosophical logic, *Philosophical logic and artificial intelligence*. Netherlands: Springer. https://doi.org/10.1007/978-94-009-2448-2, 1989.

[7] Role of AI in cyber, "Role of AI in cyber security through Anomaly detection and Predictive analysis. ," *J Inf Educ Res*, vol. 3, no. 2, 2020. https://doi.org/10.52783/jier.v3i2.314

[8] G. Lucky, F. Jjunju, and A. A. Marshall, "lightweight decision-tree algorithm for detecting DDoS flooding attacks. ," in *In Proceedings—companion of the 2020 IEEE 20th international conference on software quality, reliability, and security, QRS-C 2020, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 382–389. https://doi.org/10.1109/QRS-C51114.2020.00072*, 2020.

[9] M. Mynuddin, M. Hossain, K. S. Uddin, M. Islam, D. Abdul Ahad, and M. Tanvir, "Cyber security system using fuzzy logic," presented at the In International Conference on Electrical, Computer, Communications and Mechatronics Engineering, ICECCME 2023, Institute of Electrical and Electronics Engineers Inc., 2023. https://doi.org/10.1109/ICECCME57830.2023.10252778, 2023.

[10] S. Kitchenham and B. Charters, "Guidelines for performing systematic literature reviews in software engineering," *Technical report, Ver. 2.3 EBSE*, vol. 1, pp. 1–54, 2020. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.117.471&rep=rep1&type=pdf

[11] K. Shaukat, S. Luo, S. Chen, and L. D., "Cyber threat detection using machine learning techniques: a performance evaluation perspective. 1st Annual international conference on cyber warfare and security " in *ICCWS 2020—Proceedings, 2020, https://doi.org/10.1109/ICCWS48432.2020.9292388*, 2020.

[12] F. Talpur, I. Korejo, A. Chandio, and A. Ghulam, "ML-based detection of DDoS attacks using evolutionary algorithms " *Optimization*, vol. 24, no. 5, p. 1672, 2020. https://doi.org/10.3390/s24051672

[13] S. Yaras and M. Dener, "IoT-based intrusion detection system using new hybrid deep learning algorithm," *Electronics*, vol. 13, no. 6, p. 1053, 2024. https://doi.org/10.3390/electronics

[14] A. Alamyar and R. License, "Detecting malicious attacks using cyber-security models using deep learning approach," pp. 0–26, 2023.

[15] S. Abbas, "Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks," *PeerJ Comput Sci*, vol. 10, 2024// 2024. https://doi.org/10.7717/peerj-cs.1793

[16] M. AbdullahAlohali, "Metaheuristics with deep learning driven phishing detection for sustainable and secure environment," *Sustain Energy Technol Assess*, 2023// 2023. https://doi.org/10.1016/j.seta.2023.103114

[17] A. AbuBakar and M. F. Zolkipli, "Cyber security threats and predictions: a survey," *Int J Adv Eng Manag (IJAEM)*, vol. 5, 2023// 2023. 10.35629/5252-0502733741

[18] P. Agrawal, H. F. Abutarboush, T. Ganesh, and A. W. Mohamed, "Metaheuristic algorithms on feature selection: a survey of one decade of research (2009–2019)," *IEEE Access*, vol. 9, 2021// 2021. https://doi.org/10.1109/ACCESS.2021.3056407

[19] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber security in IoT-based cloud computing: a comprehensive survey," *Electronics (Switzerland)*, vol. 11, 2022// 2022. https://doi.org/10.3390/electronics11010016

[20] D. Akgun, S. Hizal, and U. Cavusoglu, "A new DDoS attacks intrusion detection model based on deep learning for cybersecurity," *Comput Secur*, vol. 118, 2022// 2022. https://doi.org/10.1016/j.cose.2022.102748

[21] A. Albakri, F. Alhayan, N. Alturki, S. Ahamed, and S. Shamsudheen, "Metaheuristics with deep learning model for cybersecurity and android malware detection and classification," *Appl Sci (Switzerland)*, 2023// 2023. https://doi.org/10.3390/app13042172

[22] M. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik, "Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method," *Symmetry (Basel)*, vol. 14, 2022// 2022. https://doi.org/10.3390/sym14061095

[23] M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, "X-IIoTID: A connectivity-agnostic and device-agnostic intrusion data set for industrial internet of things," *IEEE Internet Things J*, vol. 9, 2022// 2022. https://doi.org/10.1109/JIOT.2021.3102056

[24] N. O. Aljehane, H. A. Mengash, S. B. H. Hassine, F. A. Alotaibi, A. S. Salama, and S. Abdelbagi, "Optimizing intrusion detection using intelligent feature selection with machine learning model," *Alex Eng J*, vol. 91, 2024// 2024. https://doi.org/10.1016/j.aej.2024.01.073

[25] A. Zeinalpour and C. P. McElroy, "Comparing metaheuristic search techniques in addressing the effectiveness of clustering-based DDoS attack detection methods," *Electronics (Switzerland)*. 2024// 2024. https://doi.org/10.3390/electronics13050899

[26] S. Zavrak and S. Yilmaz, "Email spam detection using hierarchical attention hybrid deep learning method," *Expert Syst Appl*, 2023// 2023. https://doi.org/10.1016/j.eswa.2023.120977

[27] X. Yuan, S. Han, W. Huang, H. Ye, X. Kong, and F. Zhang, "A simple framework to enhance the adversarial robustness of deep learning-based intrusion detection system," *Comput Secur*, 2024// 2024. https://doi.org/10.1016/j.cose.2023.103644

[28] Z. Yang, "A systematic literature review of methods and datasets for anomaly-based network intrusion detection," *Comput Secur*, 2022// 2022. https://doi.org/10.1016/j.cose.2022.102675

[29] J. N. Welukar and G. P. Bajoria, "Artificial intelligence in cyber security—a review," *Int J Sci Res Sci Technol*, 2021// 2021. https://doi.org/10.32628/IJSRST218675

[30] Z. Wei, U. Rauf, and F. Mohsen, "E-Watcher: insider threat monitoring and detection for enhanced security," *Ann Telecommun*, 2024// 2024. https://doi.org/10.1007/s12243-024-01023-7

[31] M. Thomas and B. B. Meshram, "DoS attack detection using Aquila deer hunting optimization enabled deep belief network," *Int J Web Inf Syst*, 2024// 2024. https://doi.org/10.1108/IJWIS-06-2023-0089

[32] S. N. Thanh, M. Stege, P. I. El-Habr, J. Bang, and N. Dragoni, "Survey on botnets: incentives, evolution, detection and current trends," *Future Internet*, 2021// 2021. https://doi.org/10.3390/fi13080198

[33] S. Soliman, W. Oudah, and A. Aljuhani, "Deep learning-based intrusion detection approach for securing industrial Internet of Things," *Alex Eng J*, vol. 81, 2023// 2023. https://doi.org/10.1016/j.aej.2023.09.023

[34] A. Singh, A. Shibargatti, M. A. Jena, and S. Manvi, "Machine learning based detection of phishing websites in chrome," *1st Int Conf Emma-2021*, vol. 2742, 2024// 2024. https://doi.org/10.1063/5.0184539

[35] R. S. Sangwan, Y. Badr, and S. M. Srinivasan, "Cybersecurity for AI systems: a survey," *J Cybersecur Privacy*, vol. 3, 2023// 2023. https://doi.org/10.3390/jcp3020010

[36] E. Rodriguez, B. Otero, N. Gutierrez, and R. Canal, "A survey of deep learning techniques for cybersecurity in mobile networks," *IEEE Commun Surv Tutor*, vol. 23, 2021// 2021. https://doi.org/10.1109/COMST.2021.3086296

[37] M. A. Ribeiro, M. S. Pereira Fonseca, and J. Santi, "Detecting and mitigating DDoS attacks with moving target defense approach based on automated flow classification in SDN networks," *Comput Secur*, vol. 134, 2023// 2023. https://doi.org/10.1016/j.cose.2023.103462

[38] U. Rauf, F. Mohsen, and Z. Wei, "A taxonomic classification of insider threats: existing techniques, future directions and recommendations," *J Cyber Secur Mobil*, vol. 12, 2023// 2023. https://doi.org/10.13052/jcsm2245-1439.1225

[39] K. Psychogyios, A. Papadakis, S. Bourou, N. Nikolaou, A. Maniatis, and T. Zahariadis, "Deep learning for intrusion detection systems (IDSs) in time series data," *Future Internet*, vol. 16, 2024// 2024. https://doi.org/10.3390/fi16030073

[40] A. Prasad and S. Chandra, "BotDefender: a collaborative defense framework against botnet attacks using network traffic analysis and machine learning," *Arab J Sci Eng*, vol. 49, 2024// 2024. https://doi.org/10.1007/s13369-023-08016-z

[41] Y. Perwej, S. Qamar Abbas, J. Pratap Dixit, N. Akhtar, and A. Kumar Jaiswal, "A systematic literature review on the cyber security," *Int J Sci Res Manag*, vol. 9, 2021// 2021. https://doi.org/10.18535/ijsrm/v9i12.ec04

[42] J. Peng, E. C. Jury, P. Dönnes, and C. Ciurtin, "Machine learning techniques for personalised medicine approaches in immune-mediated chronic inflammatory diseases: applications and challenges," *Front Pharmacol*, vol. 12, 2021// 2021. https://doi.org/10.3389/fphar.2021.720694

[43] M. Ozkan-Okay, "A comprehensive survey: evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions," *IEEE Access*, vol. 12, 2024// 2024. https://doi.org/10.1109/ACCESS.2024.3355547

[44] F. Jabeen, Z. Hamid, A. Akhunzada, W. Abdul, and S. Ghouzali, "Trust and reputation management in healthcare systems: taxonomy, requirements and open issues," *IEEE Access*, vol. 6, 2018// 2018. https://doi.org/10.1109/ACCESS.2018.2810337

[45] G. Karacayılmaz and H. Artuner, "A novel approach detection for IIoT attacks via artificial intelligence," *Clust Comput*, vol. 27, 2024// 2024. https://doi.org/10.1007/s10586-024-04529-w

[46] N. N. Abbas, T. Ahmed, S. H. U. Shah, M. Omar, and H. W. Park, "Investigating the applications of artificial intelligence in cyber security," *Scientometrics*, vol. 121, 2019// 2019. https://doi.org/10.1007/s11192-019-03222-9

[47] M. Akhtar and T. Feng, "An overview of the applications of artificial intelligence in cybersecurity," *EAI End Trans Creat Technol*, vol. 8, 2021// 2021. 10.4108/eai.23-11-2021.172218

[48] A. Akhunzada, A. S. Al-Shamayleh, S. Zeadally, A. Almogren, and A. A. Abu-Shareha, "Design and performance of an AI-enabled threat intelligence framework for IoT-enabled autonomous vehicles," *Comput Electr Eng*, vol. 119, 2024// 2024. https://doi.org/10.1016/j.compeleceng.2024.109609

[49] M. Al-Azzawi, D. Doan, T. Sipola, J. Hautamäki, and T. Kokkonen, "Artificial intelligence cyberattacks in red teaming: a scoping review," in World conference on information systems and technologies. Cham: Springer, 2024.

[50] N. Almakayeel and E. L. Lydia, "Improved sand cat swarm optimization with deep learning based enhanced malicious activity recognition for cybersecurity," *Alex Eng J*, vol. 98, 2024// 2024. https://doi.org/10.1016/j.aej.2024.04.053

[51] M. H. Behiry and M. Aly, "Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods," *J Big Data*, vol. 11, 2024// 2024. https://doi.org/10.1186/s40537-023-00870-w

[52] A. Budžys, O. Kurasova, and V. Medvedev, "Deep learning-based authentication for insider threat detection in critical infrastructure," *Artif Intell Rev*, vol. 57, 2024// 2024. https://doi.org/10.1007/s10462-024-10893-1

[53] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, "Explainable artificial intelligence in cybersecurity: a survey," *IEEE Access*, vol. 10, 2022// 2022. https://doi.org/10.1109/ACCESS.2022.3204171

[54] C. Y. Chen *et al.*, "IEEE access special section editorial: artificial intelligence in cybersecurity," *IEEE Access*, vol. 8, 2020// 2020. https://doi.org/10.1109/ACCESS.2020.3021604

[55] T. Choithani, A. Chowdhury, S. Patel, P. Patel, D. Patel, and M. Shah, "A comprehensive study of artificial intelligence and cybersecurity on bitcoin, crypto currency and banking system," *Ann Data Sci*, vol. 11, 2024// 2024. https://doi.org/10.1007/s40745-022-00433-5

[56] R. Das and R. Sandhane, "Artificial intelligence in cyber security," *J Phys Conf Ser*, vol. 1964, 2021// 2021. https://doi.org/10.1088/1742-6596/1964/4/042072

[57] M. R. Faraji, F. Shikder, M. H. Hasan, M. M. Islam, and U. K. Akter, "Examining the role of artificial intelligence in cyber security (CS): a systematic review for preventing prospective solutions in financial transactions," *Int J*, vol. 5, 2024// 2024.

[58] F. Farivar, M. S. Haghighi, A. Jolfaei, and M. Alazab, "Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT," *IEEE Trans Industr Inf*, vol. 16, 2019// 2019. https://doi.org/10.1109/TII.2019.2956474

[59] S. Ghosh, P. Kuila, M. Bey, and M. Azharuddin, "Quantum-inspired gravitational search algorithm-based low-price binary task offloading for multi-users in unmanned aerial vehicle-assisted edge computing systems," *Expert Syst Appl*, vol. 263, 2025// 2025. https://doi.org/10.1016/j.eswa.2024.125762

[60] H. Han, J. Yao, Y. Wu, Y. Dou, and J. Fu, "Quantum communication based cyber security analysis using artificial intelligence with IoMT," *Opt Quant Electron*, vol. 56, 2024// 2024. https://doi.org/10.1007/s11082-023-06185-7

[61] M. Homaei, Ó. Mogollón-Gutiérrez, J. C. Sancho, M. Ávila, and A. Caro, "A review of digital twins and their application in cybersecurity based on artificial intelligence," *Artif Intell Rev*, vol. 57, 2024// 2024. https://doi.org/10.1007/s10462-024-10805-3

[62] D. Humphreys, A. Koay, D. Desmond, and E. Mealy, "AI hype as a cyber security risk: the moral responsibility of implementing generative AI in business," *AI and Ethics*, vol. 4, 2024// 2024. https://doi.org/10.1007/s43681-024-00443-4

[63] M. T. Khan, A. Akhunzada, and S. Zeadally, "Proactive defense for fog-to-things critical infrastructure," *IEEE Commun Mag*, vol. 60, 2022// 2022. https://doi.org/10.1109/MCOM.005.2100992

[64] T. Khan, M. Alam, A. Akhunzada, A. Hur, M. Asif, and M. K. Khan, "Towards augmented proactive cyberthreat intelligence," *J Parallel Distrib Comput*, vol. 124, 2019// 2019. https://doi.org/10.1016/j.jpdc.2018.10.006

[65] O. Krishnamurthy and G. Vemulapalli, "Advancing sustainable cybersecurity: exploring trends and overcoming challenges with generative AI," in International conference on sustainable development through machine learning, AI and IoT. Cham: Springer, 2024.

[66] P. Kulshrestha and T. V. Vijay Kumar, "Machine learning based intrusion detection system for IoMT," *Int J Syst Assur Eng Manag*, vol. 15, 2024// 2024. https://doi.org/10.1007/s13198-023-02119-4

[67] S. Liaqat, A. Akhunzada, F. S. Shaikh, A. Giannetsos, and M. A. Jan, "SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT)," *Comput Commun*, vol. 160, 2020// 2020. https://doi.org/10.1016/j.comcom.2020.07.006

[68] N. Mohamed, K. S. Kumar, S. Sharma, R. D. Kumar, S. Mehta, and I. Mishra, "Wireless Sensor network security with the probability based neighbourhood estimation," *Int J Intell Syst Appl Eng*, vol. 10, 2022// 2022.

[69] B. Naik, A. Mehta, H. Yagnik, and M. Shah, "The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review," *Complex Intell Syst*, vol. 8, 2022// 2022. https://doi.org/10.1007/s40747-021-00494-8

[70] M. M. Nair, A. Deshmukh, and A. K. Tyagi, "Artificial intelligence for cyber security: current trends and future challenges," in Automated secure computing for next-generation systems. Hoboken: Wiley, 2024.

[71] S. I. Ndumbe and P. Velikov, "Government strategies on cybersecurity and how artificial intelligence can impact cybersecurity in healthcare with special reference to the UK," in Cybersecurity and artificial intelligence: transformational strategies and disruptive innovation. Cham: Springer, 2024.

[72] A. Oubelaid, N. Mohamed, R. S. Rathore, M. Bajaj, and T. Rekioua, "Artificial neural networks-based torque distribution for riding comfort improvement of hybrid electric vehicles," *Proc Comput Sci*, vol. 235, 2024// 2024. https://doi.org/10.1016/j.procs.2024.04.123

[73] A. Qaddos, M. U. Yaseen, A. S. Al-Shamayleh, M. Imran, A. Akhunzada, and S. Z. Alharthi, "A novel intrusion detection framework for optimizing IoT security," *Sci Rep*, vol. 14, 2024// 2024. https://doi.org/10.1038/s41598-024-72049-z

[74] M. Ozkan-Ozay *et al.*, "A comprehensive survey: evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions," *IEEE Access*, vol. 12, 2024// 2024. https://doi.org/10.1109/ACCESS.2024.3355547

[75] R. Prasad, V. Rohokale, R. Prasad, and V. Rohokale, "Artificial intelligence and machine learning in cyber security," in Cyber security: the lifeline of information and communication technology. Cham: Springer, 2020.

[76] S. Ramos and J. Ellul, "Blockchain for Artificial intelligence (AI): enhancing compliance with the EU AI act through distributed ledger technology A cybersecurity perspective," *Int Cybersecur Law Rev*, vol. 5, 2024// 2024. https://doi.org/10.1365/s43439-023-00107-9

[77] M. Roopesh, N. Nishat, S. Rasetti, and M. A. Rahaman, "A review of machine learning and feature selection techniques for cybersecurity attack detection with a focus on DDOS attacks," *Acad J Sci Technol Eng Math Educ*, vol. 4, 2024// 2024. https://doi.org/10.69593/ajsteme.v4i03.105

[78] I. H. Sarker, "Introduction to AI-driven cybersecurity and threat intelligence," in AI-driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability. Cham: Springer, 2024.

[79] D. K. Sharma, J. Mishra, A. Singh, R. Govil, G. Srivastava, and J. C. W. Lin, "Explainable artificial intelligence for cybersecurity," *Comput Electr Eng*, vol. 103, 2022// 2022. https://doi.org/10.1016/j.compeleceng.2022.108356

[80] P. Sharma, J. S. Prasad, and A. S. K. Shaheen, "An efficient cyber threat prediction using a novel artificial intelligence technique," *Multimed Tools Appl*, vol. 83, 2024// 2024. https://doi.org/10.1007/s11042-024-18169-0

[81] N. Sharma and N. Jindal, "Emerging artificial intelligence applications: metaverse, IoT, cybersecurity, healthcare-an overview," *Multimedia Tools Appl*, vol. 83, 2024// 2024. 10.1007/s11042-023-17890-6

[82] D. Shoukat, M. T. Khan, S. M. Sajjad, and A. Akhunzada, "Smart and sustainable threat intelligence," in Innovation and technological advances for sustainability. London: CRC Press, 2024.

[83] S. Siva Shankar, B. T. Hung, P. Chakrabarti, T. Chakrabarti, and G. Parasa, "A novel optimization based deep learning with artificial intelligence approach to detect intrusion attack in network system," *Educ Inf Technol*, vol. 29, 2024// 2024. https://doi.org/10.1007/s10639-023-11885-4
[84] F. Tao, M. S. Akhtar, and Z. Jiayuan, "The future of artificial intelligence in cybersecurity: a comprehensive survey," *EAI End Trans Creat Technol*, vol. 8, 2021// 2021.
[85] I. Wiafe, F. N. Koranteng, E. N. Obeng, N. Assyne, A. Wiafe, and S. R. Gulliver, "Artificial intelligence for cybersecurity: a systematic mapping of literature," *IEEE Access*, vol. 8, 2020// 2020. https://doi.org/10.1109/ACCESS.2020.3013145
[86] D. Zaman and M. Mazinani, "Cybersecurity in smart grids: protecting critical infrastructure from cyber attacks," *SHIFRA*, vol. 2023, 2023// 2023. https://doi.org/10.70470/SHIFRA/2023/010
[87] Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable artificial intelligence applications in cyber security: state-of-the-art in research," *IEEE Access*, vol. 10, 2022// 2022. https://doi.org/10.1109/ACCESS.2022.3204051
[88] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," *IEEE Access*, vol. 8, 2020// 2020. https://doi.org/10.1109/ACCESS.2020.2968045
[89] G. Rjoub *et al.*, "A survey on explainable artificial intelligence for cybersecurity," *IEEE Trans Netw Serv Manag*, vol. 20, 2023// 2023. https://doi.org/10.1109/TNSM.2023.3282740
[90] IBM, "The CEO's guide to Generative AI: Supply chain," *IBM*, 2023.
[91] N. Carlini *et al.*, "Extracting training data from large language models," *In: USENIX Security Symposium*, 2020.
[92] K. Greshake, S. Abdelnabi, S. Mishra, C. Endres, T. Holz, and M. Fritz, "More than you've asked for: A comprehensive analysis of novel prompt injection threats to application-integrated large language models," *arXiv preprint arXiv:2302*, p. 12173, 2023.
[93] E. Brynjolfsson, D. Li, and L. Raymond, "Generative AI at work " *National Bureau of Economic Research*, 2023.
[94] M. Chui, L. Yee, and A. Singla, "Sukharevsky, A.: The State of AI in 2023: Generative AI's breakout year," *McKinsey & Company*, 2023.
[95] K. Park, "Samsung bans use of generative AI tools like ChatGPT after April internal data leak," Retrieved: https://techcrunch.com/2023/05/02/samsung-bans-use-of-generative-ai-tools-like-chatgpt-after-april-internal-data-leak/, 2023.
[96] H. Ben-Sasson and R. Greenberg, "38 TB of data accidentally exposed by Microsoft AI researchers," Retrieved: https://www.wiz.io/blog/38-terabytes-of-private-data-accidentally-exposed-by-microsoft-ai-researchers, 2023.
[97] OpenAI, "OpenAI: March 20 ChatGPT outage: Here's what happened ", Retrieved: https://openai.com/blog/march-20-chatgpt-outage, 2023.
[98] IBM, "The CEO's guide to generative AI: Cybersecurity," *IBM*, 2023.
[99] E. M. Renieris, D. Kiron, and S. Mills, "Building robust RAI programs as Third-party AI tools proliferate," *MIT Sloan Manage. Rev*, 2023.
[100] S. Vallor, "An introduction to cybersecurity ethics markkula center for applied ethics," Retrieved: https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf, 2018.
[101] J. Blanken-Webb, I. Palmer, R. H. Campbell, N. C. Burbules, and M. Bashir, "Cybersecurity e
thics. Foundations of Information Ethics," *American Library Association* pp. 91–101, 2019.
[102] G. Morgan and B. Gordijn, "A care-based stakeholder approach to ethics of cybersecurity in business," *The ethics of cybersecurity*, vol. 5, no. 6, pp. 119–138, 2023. https://doi.org/10.1007/978-3-030-29053
[103] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, and S. Creese, "Upton, D.: A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *J. Cybersecur*, no. 4, 2018. https://doi.org/10.1093/cybsec/tyy006
[104] National Institute of Standards and Technology, "National institute of standards and technology," Retrieved: https://csrc.nist.gov/glossary/term/integrity, 2018.
[105] K. Macnish and J. van der Ham, "Ethics in cybersecurity research and practice," *Technol. Soc*, no. 63, 2020. https://doi.org/10.1016/j.techsoc.2020.101382
[106] I. Van De Poel, "Core values and value conflicts in cybersecurity: beyond privacy versus security," *Springer International Publishing*, pp. 45–71, 2020. https://doi.org/10.1007/978-3-030-29053-5_3
[107] D.-O. Jaquet-Chiffelle and M. Loi, "Ethical and unethical hacking," Springer International Publishing (2020). https://doi.org/10.1007/978-3-030-29053-5_9, pp. 179–204.
[108] S. Riley, "DarkLight offers first of its kind artificial intelligence to enhance cybersecurity defenses," Retrieved: https://www.businesswire.com/news/home/20170726005117/en/DarkLight-Offers-, 2017.
[109] N. Carlini *et al.*, "Poisoning web-scale training datasets is practical," *ArXiv abs/2302.10149*, 2023.
[110] D. Foster, "Generative deep learning," *O'Reilly Media,* 2020.
[111] M. Sallam, "In: Healthcare (ed.) ChatGPT utility in healthcare education, research, and practice: Systematic review on the promising perspectives and valid concerns," MDPI, 2023, p. 887.
[112] F. Dell'Acqua *et al.*, "Navigating the jagged technological frontier: Field experimental evidence of the effects of AI on knowledge worker productivity and quality," Harvard Business School Technology & Operations Mgt. Unit Working Paper,
[113] A. Zarifhonarvar, "Economics of chatgpt: A labor market view on the occupational impact of artificial intelligence," *J. Electron. Bus. Digit. Econ*, 2023.
[114] S. F. Wamba, M. M. Queiroz, C. J. C. Jabbour, and C. V. Shi, "Are both generative AI and ChatGPT game changers for 21st-Century operations and supply chain excellence?," *Int. J. Prod. Econ.*, vol. 265, 2023// 2023. https://doi.org/10.1016/j.ijpe.2023.109015
[115] A. Varma, C. Dawkins, and K. Chaudhuri, "Artificial intelligence and people management: A critical assessment through the ethical lens," *Hum. Resource Manage. Rev.*, vol. 33, 2023// 2023. https://doi.org/10.1016/j.hrmr.2022.100923
[116] P. Tambe, P. Cappelli, and V. Yakubovich, "Artificial intelligence in human resources management: Challenges and a path forward," *Calif. Manag. Rev.*, vol. 61, 2019// 2019. https://doi.org/10.1177/0008125619867910
[117] M. Taddeo, "An analysis for a just cyber warfare," *4th Int. Conf. Cyber Confl. (CYCON 2012)*, vol. pp 1–10, 2012// 2012.
[118] C. Stokel-Walker, "ChatGPT listed as author on research papers: Many scientists disapprove," *Nature*, vol. 613, 2023// 2023. https://doi.org/10.1038/d41586-023-00107-z
[119] L. J. Skitka, K. L. Mosier, and M. Burdick, "Does automation bias decision-making?," *Int. J. Hum-Comput St*, vol. 51, 1999// 1999. https://doi.org/10.1006/ijhc.1999.0252

[120] G. Sebastian, "Do ChatGPT and other AI Chatbots pose a cybersecurity risk?," *Int. J. Secur. Priv. Pervasive Comput.*, vol. 15, 2023// 2023. https://doi.org/10.4018/ijsppc.320225
[121] D. Schlagwein and L. Willcocks, "ChatGPT et al.': The ethics of using (generative) artificial intelligence in research and science," *J. Inform. Technol.*, vol. 38, 2023// 2023. https://doi.org/10.1177/02683962231200411
[122] D. Schatz, R. Bashroush, and J. Wall, "Towards a more representative definition of Cyber Security," *J. Digit. Forensics Se*, vol. 12, 2017// 2017.
[123] L. P. Robert, C. Pierce, L. Marquis, S. Kim, and R. Alahmad, "Designing fair AI for managing employees in organizations: A review, critique, and design agenda," *Human–Computer Interact.*, vol. 35, 2020// 2020. https://doi.org/10.1080/07370024.2020.1735391
[124] I. Poel, "An ethical Framework for evaluating Experimental Technology," *Sci Eng. Ethics*, vol. 22, 2016// 2016. https://doi.org/10.1007/s11948-015-9724-3
[125] P. N. Petratos and A. Faccia, "Fake news, misinformation, disinformation and supply chain risks and disruptions: Risk management and resilience using blockchain," *Ann. Oper. Res.*, vol. 327, 2023// 2023. https://doi.org/10.1007/s10479-023-05242-4
[126] J. V. Pavlik, "Collaborating with ChatGPT: Considering the implications of generative artificial intelligence for journalism and media education," *Journalism Mass. Communication Educ.*, vol. 78, 2023// 2023. https://doi.org/10.1177/10776958221149577
[127] M. Manjikian, *Cybersecurity Ethics: An Introduction*. London: Routledge, 2023.
[128] C. K. Lo, "What is the impact of ChatGPT on education? A rapid review of the literature," *Educ. Sci.*, vol. 13, 2023// 2023. https://doi.org/10.3390/educsci13040410
[129] J. H. Li, "Cyber security meets artificial intelligence: A survey," *Front. Inf. Tech. El*, vol. 19, 2018// 2018. https://doi.org/10.1631/Fitee.1800573
[130] Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, 2015// 2015. https://doi.org/10.1038/nature14539
[131] S. Kumar, U. Gupta, A. K. Singh, and A. K. Singh, "Artificial Intelligence: Revolutionizing Cyber Security in the Digital era," *J. Computers Mech. Manage.*, vol. 2, 2023// 2023. https://doi.org/10.57159/gadl.jcmm.2.3.23064
[132] L. Illia, E. Colleoni, and S. Zyglidopoulos, "Ethical implications of text generation in the age of artificial intelligence," *Bus. Ethics Environ. Responsib.*, vol. 32, 2023// 2023. https://doi.org/10.1111/beer.12479
[133] Z. Hosseini, S. Nyholm, P. M. Blanc, P. T. Y. Preenen, and E. Demerouti, "Assessing the artificially intelligent workplace: An ethical framework for evaluating experimental technologies in workplace settings," *AI Ethics*, 2023// 2023. https://doi.org/10.1007/s43681-023-00265-w
[134] S. Gelper, R. Lans, and G. Bruggen, "Competition for attention in online social networks: Implications for seeding strategies," *Manage. Sci.*, vol. 67, 2021// 2021. https://doi.org/10.1287/mnsc.2019.3564
[135] N. Gross, "What chatGPT tells us about gender: A cautionary tale about performativity and gender biases in AI," *Social Sci.*, vol. 12, 2023// 2023. https://doi.org/10.3390/socsci12080435
[136] P. Formosa, M. Wilson, and D. Richards, "A principlist framework for cybersecurity ethics," *Computers Secur.*, vol. 109, 2021// 2021. https://doi.org/10.1016/j.cose.2021.102382
[137] L. Floridi *et al.*, "AI4People—An ethical Framework for a good AI society: Opportunities, risks, principles, and recommendations," *Mind. Mach.*, vol. 28, 2018// 2018. https://doi.org/10.1007/s11023-018-9482-5
[138] C. J. Finlay, "Just War, Cyber War, and the Concept of Violence," *Philos. Technol.*, vol. 31, 2018// 2018. 10.1007/s13347-017-0299-6
[139] M. Christen, B. Gordijn, and M. Loi, "The Ethics of Cybersecurity. The International Library of Ethics," *Law Technol.*, 2020// 2020. 10.1007/978-3-030-29053-5
[140] B. Chen, Z. Wu, and R. Zhao, "From fiction to fact: The growing role of generative AI in business and finance," *J. Chin. Economic Bus. Stud.*, vol. 21, 2023// 2023. https://doi.org/10.1080/14765284.2023.2245279
[141] M. Cascella, J. Montomoli, V. Bellini, and E. Bignami, "Evaluating the feasibility of ChatGPT in healthcare: An analysis of multiple clinical and research scenarios," *J. Med. Syst.*, vol. 47, 2023// 2023. https://doi.org/10.1007/s10916-023-01925-4
[142] Z. Buçinca, M. Malaya, and K. Gajos, "To trust or to think: Cognitive forcing functions can reduce overreliance on AI in AI-assisted decision-making," *Proc. ACM Hum. -Comput Interact.*, vol. 5, 2021// 2021. https://doi.org/10.1145/3449287
[143] D. Bruschi and N. Diomede, "A framework for assessing AI ethics with applications to cybersecurity," *AI Ethics*, vol. 3, 2023// 2023. https://doi.org/10.1007/s43681-022-00162-8
[144] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big data*, vol. 7, pp. 1-29, 2020.
[145] S. Zhou, C. Liu, D. Ye, T. Zhu, W. Zhou, and P. S. Yu, "Adversarial attacks and defenses in deep learning: From a perspective of cybersecurity," *ACM Computing Surveys*, vol. 55, no. 8, pp. 1-39, 2022.
[146] A. L. Buczak, B. Baugher, E. Guven, L. Moniz, S. M. Babin, and J.-P. Chretien, "Prediction of peaks of seasonal influenza in military health-care data: Supplementary issue: Big data analytics for health," *Biomedical engineering and computational biology*, vol. 7, p. BECB. S36277, 2016.
[147] U. Ghosh, M. Islam, M. Siddiqui, X. Cao, and M. Khan, "Proline, a multifaceted signalling molecule in plant responses to abiotic stress: understanding the physiological mechanisms," *Plant Biology*, vol. 24, no. 2, pp. 227-239, 2022.
[148] G. Zennaro, G. Corazza, and F. Zanin, "The effects of integrated reporting quality: a meta-analytic review," *Meditari Accountancy Research*, vol. 32, no. 7, pp. 197-235, 2024.
[149] M. Kaur, A. K. Singh, and A. Singh, "Bioconversion of food industry waste to value added products: Current technological trends and prospects," *Food Bioscience*, vol. 55, p. 102935, 2023.
[150] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *2010 IEEE symposium on security and privacy*, 2010: IEEE, pp. 305-316.