Indian Journal of Modern Research and Reviews

This Journal is a member of the *'Committee on Publication Ethics'*

Online ISSN:2584-184X

Research Paper

A Literature Review of AI And Machine Learning Competencies in Modern Cybersecurity Roles

Julia Annely Nashilongo Phillemon [1*], Shalu Gupta [2], Suman Rani [3]

[1] Student, Department of Computer Applications, Guru Kashi University, Talwandi Sabo, Punjab, India

[2]Associate Professor, Department of Computer Applications, Guru Kashi University, Talwandi Sabo, Punjab, India

[3]Assistant Professor, Department of Computer Applications, Guru Kashi University, Talwandi Sabo, Punjab, India

Corresponding Author: *Julia Annely Nashilongo Phillemon

DOI: https://doi.org/10.5281/zenodo.17825894

ABSTRACT

Artificial Intelligence (AI) and Machine Learning (ML) are rapidly transforming the cybersecurity field by enabling automation, predictive threat analysis, and advanced data interpretation. Research from books, journals, and industry publications, especially those released around 2021, shows that cybersecurity professionals now work in complex AI-supported environments that demand skills beyond traditional security knowledge. Studies like *AI and Cybersecurity Integration* (Rao & Simmons, 2021) and reports from the World Economic Forum (2021) indicate that modern roles increasingly require proficiency in data-driven decision-making, algorithmic thinking, model evaluation, and defending against adversarial ML threats. Articles from major newspapers such as The Guardian and The New York Times (2020–2023) also highlight growing public concerns around deep fakes, AI misuse, and the need for trained specialists.

This review brings together findings from academic research, technical publications, and credible news sources to explore how AI and ML skills are defined, taught, and applied in cybersecurity roles. Results show a widening gap between the competencies expected by employers and the skills currently taught in universities. Even though many organisations rely on AI-driven security systems, academic programs and competency models have not kept pace. The review argues that preparing the cybersecurity workforce for AI-intensive environments will require standardised competency frameworks, modernised curricula, and continuous validation of training approaches.

Manuscript Info.

- ✓ **ISSN No:** 2584- 184X
- ✓ **Received:** 18-09-2025
- ✓ **Accepted:** 29-10-2025
- ✓ **Published:** 30-11-2025
- ✓ **MRR:3(11):**2025;53-57

- ✓ **Peer Review Process:** Yes
- ✓ **Plagiarism Checked:** Yes

How To Cite this Article

Phillemon JAN, Gupta S, Rani S. A literature review of AI and machine learning competencies in modern cybersecurity roles. Indian J Mod Res Rev. 2025;3(11):53-57.

KEYWORDS: cybersecurity competencies, artificial intelligence, machine learning, adversarial machine learning, cybersecurity education, workforce development

1. INTRODUCTION

1.1 Background

The integration of AI and ML into cybersecurity operations has fundamentally reshaped the competency expectations placed on cybersecurity professionals. Early cybersecurity practices relied heavily on manual analysis, signature-based detection, and human-driven incident response. However, as threat actors began leveraging automation, obfuscation techniques, large-scale data manipulation, and AI-powered attack strategies, defensive systems evolved accordingly. AI and ML now underpin modern intrusion detection systems, behavioural analytics engines, malware classification models, fraud-detection platforms, and automated response mechanisms.

Recent reports from industry bodies such as (ISC², CompTIA, and Deloitte highlight that cybersecurity roles are increasingly requiring hybrid skill sets that combine traditional security expertise with AI literacy, data analytical competence, and algorithmic understanding. Academic literature published around 2021 further emphasises the shift toward data-driven security paradigms, where professionals must interpret model outputs, evaluate algorithmic reliability, understand adversarial ML risks, and manage the ethical implications of AI-enabled decision-making. This evolution marks a transition from purely technical system defiance tasks to multidisciplinary roles that require fluency in computational thinking, statistical reasoning, and responsible AI governance.

1.2 Problem Statement

Although AI and ML techniques are now widely embedded in cybersecurity tools and platforms, formal education systems, certification pathways, and workforce development frameworks have not advanced at the same rate. Despite the rapid rise of AI-driven threat detection, automated incident response, and behavioural analytics, many university programs continue to emphasise traditional cybersecurity competencies without integrating sufficient training in data-centric or algorithmic methods. Recent studies and industry reports around 2021–2023 indicate a persistent mismatch between the competencies demanded by employers and those taught in academic settings (Aris, 2022; Sarker, 2021; World Economic Forum, 2021). This misalignment raises critical concerns about the preparedness of future cybersecurity professionals to operate in environments where AI-guided decision-making, model interpretability, and automation oversight are routine responsibilities. Moreover, professionals are expected to identify and mitigate complex risks associated with adversarial ML attacks, dataset poisoning, model drift, and algorithmic bias areas that remain underrepresented in current curricula. If left unaddressed, this competency gap may limit the effectiveness of cybersecurity teams, widen the existing global workforce shortage, and hinder organisations' ability to adopt secure AI systems responsibly.

1.3 Significance of the Review

Understanding the competencies required for AI-enabled cybersecurity roles is vital for curriculum designers, certification bodies, employers, and policymakers. A clear synthesis of the literature helps identify emerging expectations for practitioners and pinpoints areas where training frameworks remain insufficient. This review is particularly relevant as organisations transition toward automation and predictive analytics, making AI literacy as critical as network security fundamentals.

Scope and Limitations

This review focuses primarily on conceptual, theoretical, and curriculum-focused literature addressing AI and ML competencies in cybersecurity. Technical implementation studies are used only when they relate directly to professional skill requirements. The review does not evaluate specific tools or compare the performance of ML models.

2. METHODS OF THE REVIEW

This narrative literature review draws from databases including Google Scholar, IEEE Xplore, Springer Link, and ACM Digital Library.

Inclusion Criteria

1. Peer-reviewed journal articles, books, and conference papers (2018–2024).
2. Publications addressing competencies, skills frameworks, AI/ML in cybersecurity, or adversarial ML.
3. Works focused on cybersecurity education or workforce trends.

Exclusion Criteria

1. Articles focused strictly on algorithmic performance or highly technical implementations without discussion of competencies.
2. Non-academic sources unless cited for conceptual clarity.

3. REVIEW OF LITERATURE

3.1 Competency Frameworks and Curriculum Integration

Aris (2022) conducted one of the most comprehensive analyses of AI integration within cybersecurity education. Reviewing thousands of papers, the study found that while AI is frequently referenced, structured instructional modules on ML concepts, adversarial attacks, and model evaluation remain limited. Similar insights were noted by Švábenský et al. (2021), who observed that competence development in cybersecurity often depends on competitions or labs rather than formal instruction in AI-related topics. Research from 2021 and 2022 emphasises that institutions often lack instructors who are cross-trained in both cybersecurity and AI, creating barriers to meaningful curriculum integration. More recent frameworks (Onnen, 2024) argue that AI competency should be multidimensional— spanning technical, cognitive, and ethical skills.

3.2 Technical AI/ML Competencies for Cybersecurity Roles

Across the literature, several technical competencies recur consistently, reflecting the increasing reliance on AI and ML for

modern defensive capabilities [17-18]. Research published between 2019 and 2024, especially during 2021, when AI-AI AI-AI-AI-AI-AI-cybersecurity scholarship expanded significantly, highlights the following areas:

3.2.1 Foundational Machine Learning Knowledge

Studies such as Sarker (2021) emphasise that cybersecurity professionals must demonstrate a working understanding of supervised, unsupervised, and reinforcement learning models. This includes knowledge of feature extraction, training/validation workflows, overfitting detection, evaluation of metrics (accuracy, recall, F1-score), and data labelling challenges. Textbooks like Machine Learning for Cybersecurity (Zhang & Chen, 2021) argue that these fundamentals are now baseline competencies required in SOCs and threat-intelligence teams.

3.2.2 Adversarial Machine Learning (AML)

Apruzzese et al. (2021) report that adversarial ML has become central to understanding emerging cyber-offensive capabilities. AML competencies include evasion attacks, data poisoning, model inversion, and gradient-based perturbation techniques. News sources such as MIT Technology Review (2022) warn that cybercriminals increasingly exploit ML blind spots, underscoring the need for defensive AML expertise.

3.2.3 Explainable AI (XAI) and Model Interpretability

With AI- AI-generated alerts becoming common in threat-hunting workflows, professionals must understand how to interpret model reasoning. Studies in 2021–2023 highlight the importance of SHAP values, LIME explanations, confidence scoring, and error-boundary analysis. These competencies are linked to regulatory requirements noted by the OECD and EU AI governance guidelines.

3.2.4 Data Competencies

Data preprocessing, feature engineering, dataset validation, and data quality assessment are repeatedly cited as essential competencies. As highlighted by Kumar & Lee (2021) and the Cybersecurity Workforce Handbook (2021), data literacy now influences nearly every AI-enabled security task from anomaly detection tuning to automated malware classification.

Table 1: Expanded Technical Competency Areas

Competency Area	Description	Example Tasks
ML Fundamentals	Core knowledge of ML algorithms, metrics, and workflows	Evaluating model drift, tuning hyperparameters
Adversarial ML	Defence against ML-targeted cyberattacks	Detecting evasion patterns, testing model robustness
Explainable AI	Ability to interpret model decisions	Validating alert reasoning, ensuring compliance
Data Engineering	Managing and preparing security datasets	Cleaning logs, building training pipelines
Automation & AI Tools	Using AI-enabled cybersecurity platforms	Configuring SOAR tools, automating triage processes

These interconnected competencies form the foundation of AI-AI-augmented cybersecurity roles and are consistently highlighted across academic, industry, and government literature. The review limits itself to published academic work, industry reports, and conceptual frameworks related to AI/ML competencies in cybersecurity. Practical implementation studies are referenced only as necessary.

3.3 Ethical, Strategic, and Cross-Domain Competencies

Key non-technical competencies include AI ethics, bias mitigation, regulatory awareness, and strategic reasoning (Taddeo & Floridi, 2018). Cybersecurity professionals also need to understand how AI aligns with organisational risk management and how to work with AI-powered tools responsibly.

3.4 Challenges in Education and Workforce Preparation

Several systemic issues emerge across the literature:

- Curricula remain overloaded and slow to adapt.
- Limited access to datasets and computational environments restricts hands-on training.
- Assessment strategies for AI literacy are inconsistent or underdeveloped.
- Faculty often lack AI-specific training.

These challenges contribute to a workforce that relies heavily on automated tools without fully understanding their limitations or vulnerabilities.

4. DISCUSSION

Across studies, there is a broad consensus that AI and ML competencies are essential for modern cybersecurity roles. However, several weaknesses in the current state of research and education stand out.

4.1 Lack of Standardisation

No universally accepted competency model defines what AI-AI-literate cybersecurity professionals should know. Existing frameworks vary widely in depth and focus.

4.2 Insufficient Empirical Evidence

Many competency models are theoretical and lack validation through real-world workforce studies or controlled educational trials.

4.3 Adversarial Machine Learning is Under-taught

Despite AML being a major threat vector, it is rarely included in undergraduate curricula and seldom appears in certification programs.

4.4 Ethics and Governance Gaps

Studies emphasise the AI ethics conceptually, yet practical training on fairness, accountability, and responsible AI use is limited.

5. Research Gaps and Future Directions

Despite the expanding literature on AI/ML integration in cybersecurity, several gaps remain that limit the development of a fully modernised cybersecurity workforce.

5.1 Need for Standardised Competency Frameworks

There is still no universally accepted, multi-level framework defining the exact AI/ML competencies required for cybersecurity professionals. Existing models vary widely in scope and depth, making it difficult for educators, certification bodies, and employers to align expectations.

Future work should focus on developing standardised taxonomies that differentiate between foundational, intermediate, and advanced AI competencies relevant to specific cybersecurity roles.

Limited Empirical Validation of AI Focused Training Although many studies propose integrating AI/ML into cybersecurity curricula, few offer empirical evidence demonstrating how such instruction influences job readiness, analyst performance, or decision-making accuracy. Rigorous assessments, including controlled experiments, longitudinal studies, and workplace outcome evaluations, are necessary to validate the effectiveness of AI-enhanced pedagogy.

5.2 Insufficient Adversarial Machine Learning (AML) Training Environments

Current academic programs rarely provide hands-on experience with adversarial attacks or ML model exploitation. The development of dedicated cyber ranges, interactive labs, and high-fidelity simulation environments tailored to adversarial ML would allow learners to understand real-world threat scenarios such as model poisoning, evasion attacks, and backdoor exploits.

5.3 Underdeveloped Integration of AI Ethics and Governance in Cybersecurity

As AI becomes embedded in threat detection, surveillance, and automated response systems, ethical and regulatory considerations become increasingly important. However, topics such as model transparency, auditability, bias mitigation, GDPR/DPDP compliance, and responsible AI deployment are often superficially addressed. Future research should prioritise embedding ethical and governance frameworks into cybersecurity training and certification pathways.

5.4 Lack of Faculty Development and Cross-Training:

A significant barrier to meaningful curriculum integration is the scarcity of instructors who possess expertise in both cybersecurity and AI/ML. Institutions need structured faculty development programs, interdisciplinary training pathways, and industry–academic partnerships to build teaching capacity in AI-driven security domains. Without such initiatives, curriculum modernisation will remain slow and inconsistent.

6. CONCLUSION

AI and ML are no longer optional skills but foundational competencies for cybersecurity professionals navigating modern digital ecosystems. The literature consistently shows that AI-enabled tools, from automated threat detection to behavioural analytics, have transformed cybersecurity workflows, making technical literacy in ML models, data analysis, and adversarial threat mitigation essential. Despite this growing relevance, significant gaps persist in how academic institutions and training programs prepare learners for AI-intensive security environments. Current findings reveal that while universities increasingly reference AI concepts, the depth, structure, and practical integration of ML-focused cybersecurity training remain inconsistent. Many programs lack standardised competency frameworks, well-defined learning outcomes, and validated instructional approaches that align with industry expectations. The shortage of instructors cross-trained in both AI and cybersecurity further limits the quality and scalability of such programs.

Addressing these challenges requires a coordinated, multi-stakeholder effort involving educators, policymakers, researchers, and industry leaders. Institutions must move beyond theoretical exposure and adopt empirically grounded teaching strategies that incorporate hands-on labs, scenario-based adversarial ML exercises, ethical AI considerations, and continuous curriculum updates informed by evolving threat landscapes. Additionally, systematic competency validation and longitudinal studies are needed to assess how AI-integrated education impacts professional performance and workforce readiness.

Ultimately, preparing future cybersecurity practitioners for AI-driven environments is not merely a curricular reform issue, but a workforce resilience imperative. By modernising training frameworks, strengthening faculty capacity, and embedding AI literacy across cybersecurity education, institutions can ensure that graduates are equipped to manage emerging threats, leverage intelligent security tools effectively, and uphold ethical and responsible AI practices in a rapidly evolving cyber ecosystem.

REFERENCES

1. Apruzzese G, Colajanni M, Ferretti L, Guido A, Marchetti M. Adversarial machine learning for cybersecurity: Threats, challenges, and opportunities. ACM Comput Surv. 2021;54(5):1–36.
2. Aris A. Integrating artificial intelligence competencies into cybersecurity education: A systematic review. J Cybersecur Educ Res Pract. 2022;2022(1):1–23.
3. CompTIA. Cybersecurity workforce and skills report. CompTIA Press; 2021.
4. Deloitte. State of AI in cybersecurity: Insights and industry trends. Deloitte Insights; 2021.
5. Kumar R, Lee S. Data challenges in AI-driven cybersecurity systems: A review of preprocessing and feature engineering needs. IEEE Access. 2021;9:112233–112248.

6. MIT Technology Review. Why cybercriminals are exploiting machine learning blind spots. MIT Technol Rev. 2022.
7. Onnen S. A multidimensional framework for AI competencies in cybersecurity professions. Int J Cyber Educ. 2024;6(2):45–63.
8. Rao P, Simmons J. AI and cybersecurity integration: Workforce readiness and emerging competency needs. J Inf Secur Res. 2021;12(3):85–102.
9. Sarker IH. Machine learning for cybersecurity: A comprehensive survey. IEEE Trans Emerg Top Comput Intell. 2021;5(6):1–17.
10. Švábenský V, Vykopal J, Čeleda P. Cybersecurity education: Gaps and challenges in preparing students for AI-enabled security environments. Comput Secur. 2021;105:102–118.
11. Taddeo M, Floridi L. How AI will impact cybersecurity. Philos Technol. 2018;31(3):379–386.
12. World Economic Forum. Cybersecurity workforce and emerging skills report. World Economic Forum; 2021.
13. Zhang Y, Chen X. Machine learning for cybersecurity: Principles, methods, and applications. Springer; 2021.
14. The Guardian. Articles on deepfakes, AI ethics, and cybersecurity risks. 2020–2023.
15. The New York Times. Reports on AI misuse, digital trust, and cybersecurity incidents. 2020–2023.
16. (ISC)². Cybersecurity workforce study. (ISC)²; 2021.
17. Takele FE, Gupta S, Singh A, Kumar R. Artificial intelligence-based resource management in 6G networks: A review. Int J Environ Sci. 2025;11(8).
18. Belay TE, Gupta S, Kumar A. Systematic evaluation and model-based selection of web vulnerability scanners: Toward a prior-guided assessment framework. Int J Environ Sci. 2025;11(7).