Frontiers in Computer Science and Artificial Intelligence
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Artificial intelligence for cybersecurity: Literature review and future directions

Ura Ashfin
Independent Researcher, Eden Mahila College, Bangladesh
Corresponding Author: Ura Ashfin**, E-mail**: *uashfin@gmail.com*

| ABSTRACT
As cyber threats continue to evolve at breakneck speed, you can also expect AI to play a key role in security solutions and influence how organisations collect information on past attacks and use it to fortify their defences. AI powered methods like machine learning, deep learning and natural language processing can predict threats in time at the same time they can scan huge and changing data sets to quickly spot anomalous behavior and take automated action. This paper reviews the latest progress on AI-inspired security defenses from 2018-2025, and covers a wide range of domains including intrusion detection mechanisms, malware classification, phishing detectors as well as behavioural analytics. The authors review various key frameworks and methods, including supervised/ unsupervised learning methods, hybrid analysis templates that help boost prediction accuracy by reducting false posotives. It also explores the increasingly important role of explainable AI (XAI) in providing trust and transparency for security operations, as well as adoption of federated learning to deliver privacy-preserving threat intelligence. However, Key challenges around adversarial robustness, data imbalance, ethical governance and model interpretability remain. The paper concludes with a discussion of future research opportunities focused on self-adaptive defence mechanisms, cognitive security architectures as well as AI-human collaboration systems expected to enhance cyber resilience in more and more decentralised and autonomous digital spaces.

| KEYWORDS
AI-Driven Cybersecurity, Intrusion Detection Systems, Adversarial Machine Learning, Explainable Artificial Intelligence (XAI), Federated Threat Intelligence

| ARTICLE INFORMATION

ACCEPTED: 01 November 2024 **PUBLISHED:** 20 November 2024 **DOI:** 10.32996/fcsai.2022.1.1.2

1. Introduction

In such a world, where threats are ever more sophisticated and pernicious, the reactive security of the past (static rules, signature detection, college interns) does not cut it any longer. Cyber-threat actors take advantage of the dynamic character of digital environments and also make use of sophisticated strategies including polymorphic malware, zero-day exploits, socially engineered phishing campaigns, Internet-of-Things (IoT) device exploitation and high-volume distributed-denial-of-service (DDoS) attacks. In this context, the fusion of AI with cybersecurity becomes an important paradigm shift (Ansari et al., 2022). SSRN.

1.1 Cyber-threats and the deficiencies of legacy defences

In the past, cybersecurity products focused on known threats though signature matching, heuristics and rule-based techniques. But, with the attackers becoming more dynamic and self learning in their ways of attack, at times the latency on aged mode security constraints increases vulnerability : breach, data loss and operational distractions . So the deluge of information emanating from network sensor logs, endpoint devices, cloud systems and IoT systems poses a “big data” problem for security teams. AI has the capability to consume, analyze and derive patterns from substantial amount of diverse data (Kaur et al., 2023) and thus may provide an opportunity for complementing—or possibly replacing—traditional methods.

1.2 What AI offers to cybersecurity

Artificial intelligence has been used in cybersecurity, including machine learning (ML), deep learning (DL), natural language processing (NLP) and more hybrid-models to support anomaly detection, malware classification, behavior modeling, intrusion-detection systems, threat-intelligence automation and incident-response orchestration. For example, it has been demonstrated that AI can provide substantial support to the "identify–protect–detect–respond–recover" cycle of the National Institute of Standards and Technology (NIST) Cybersecurity Framework by automating identification of vulnerabilities, prediction of imminent attacks, rapid detection when incidents do occur and acceleration in the pace of recovery.More generally AI allows for proactive and predictive security stances as opposed to just reactive .

1.3 Recent trends and patterns in the literature

The academic research literature in AI for cybersecurity has risen sharply over the past decade. Bibliometric approaches have shown thousands of papers address- ing intrusion detection, malware and phishing detection, IoT security, federated learning for privacy-preserved cyber-defence, adversarial-machine learning among others (Kaur et al., 2024). ResearchGate+1 A recent study shows that AI/ML in cybersecurity is not only applied for detection, but it has been used more and more for automated response and orchestration, expression of trust and explainability (XAI) and human-machine cooperation.

1.4 Challenges and research gaps

However, there are major obstacles to making AI a reality in digital security. Key issues include:

• Data quality and imbalance: Data derived from cyber-security settings is typically biased, e.g., it can be characterized by class imbalance (for each attack type there are few instances compared to benign ones), high-dimensionality and concept drift and may not be labeled, factors which influence model performance.

• Model Robustness & Adversarial attacks: The attackers are now using the adversarial-machine-learning strategies to deceive the AI based defences and thus the AI based defense model has to be designed with this respects of maliciously made inputs and changing strategies taken.

• Explainability & trust: A lot of AI models in security is black boxes. Today, for safety critical operations, there is more and more request to XAI (Explainable Artifici al Intelligence) in order to deliver transparency, trust and auditability.

• Integration and deployment 'Many academic ML techniques are still far from ready for real-life applications… it is difficult to scale such things up to something that impacts millions of people' (Smith & Choudhary, 2023).

1.5 Rational and scope of the present review

With such a wide field and fast pace of progress, it is increasingly important for researchers to take stock of what AI-powered cybersecurity looks like right now – and for practitioners looking to implement best practices. The aim of this review is:

map and classify how AI, and its subdomains are being used in cybersecurity;

scrutinize prominent algorithmic solutions, application areas, successes and shortcomings;

step towards during the identification of key research gaps and challenges in further.) From the above discussion, we briefly describe some future trends (including self-adaptive defence, AI-human cooperation, federated and privacy-preserving learning, XAI and resilience against autonomous threats among others).

In addition, the review acts as a useful overview for academics researching resilient cybergovernance and adaptive defences strategies and as an initiating base for further theoretical or empirical work concerning the relationship between AI and cybersecurity.

1.6 Structure of the paper

The rest of the paper is organized as follows. 2 Methodology This section provides details of the method used for the systematic literature search. 3, we presented a taxonomy on AI applications in cybersecurity based on defensive lifecycle stages (e.g., identify, protect, detect, respond and recover). Section 4 discusses the key AI technologies used within these applications (including machine learning, deep learning, reinforcement learning and federated learning) as well as XAI. Section 5 presents cross-cutting issues: data-centric challenges, adversarial resilience, ethical/ legal aspects, trust and interpretability. Next, Section 6 considers future research directions and lessons which can be drawn for policy and practice. Section 7 brings together the review conclusions.

2. Literature Review

2.1 Overview of AI adoption in cybersecurity

Over the last 10 years, AI has shifted from something seen in lab-based prototypes to platform service-level security functionality not all of which is mature by any means in products that include Intrusion Detection, Malware Analysis, Phishing Defence and User/E entity behaviour analytics (UEBA) or automated response/orchestration. Systematic reviews depict a growing body of literature with studies composing and maturing taxonomies linking AI technologies to the NIST "identify–protect–detect–respond–recover" lifecycle, 2023–2024 research consolidating earlier work and exposing operational gaps (e.g., data quality, robustness, and explainability).

2.2 Intrusion detection and network analysis

Classical ML and deep learning. As scale grows, flow-level features are being used more and more in collaboration with tree ensemble (e.g., Random Forest, XGBoost) or deep models (CNN/LSTM/transformers), such as to detect anomaly in network trace, or monitor)traffic generation. Rather recent and highly related works focus on hybrid pipelines (feature selection + deep models)59,62 or metaheuristics for optimisation57, reporting high offline accuracy but inconsistent generalisation across datasets and drifts.

Graph learning. Newer techniques represent hosts, services, and flows in the form of a graph to gain relational structure; in 2024 reviews describe GNN-based NIDS (self- or semi-supervised) that enhance detection under rare labels and concept drift (though operational maturity as well as interpretability are open questions).

Benchmark datasets & pitfalls. Commonly-used datasets are UNSW-NB15 (IoT network attacks), CIC-IDS 2017 (PCAP + labelled flow) and Bot-IoT. Although essential for comparability, these datasets suffer from class imbalance, overlap and the presence of artificial patterns that artificially inflate scores; careful preprocessing and cross-dataset validation are advocated.

2.3 Malware analysis and classification

Static/raw-byte models. Deep networks on PE raw bytes directly (e.g., MalConv and follow-ups) obviate manual feature engineering; 2023–2024 study their robustness and training dynamics, showing competitive accuracy but vulnerability to adversarial manipulations (e.g., padding, header edits). Recent approaches have been developed to encourage explanation and alignment methods to localise discriminative areas.

Graph-based malware. Program representations based on call-graphs, control-flow graphs, and API-sequence graphs can encode program semantics to be consumed by the GNNs, with competitive performance being reported in surveys with an increasing attention towards interpretable substructures and attack resilience.

2.4 Phishing/spam/social-engineering defense

NLP and transformers. The detection for email and URL based phishing content header features are dominated with the transformers (BERT/DistilBERT/RoBERTa) also across studies and reviews even though transformer based classifiers outperformed overwhelmingly to classical baselines (2019–2024). Hybrid BERT+CNN architectures uplift precision/recall in the enterprise data despite potential challenges in class imbalance and domain shift (campaign drift, multilingual lures).

Rising attacker capability. evidence in the field, and survey through 2024 suggests that generative AI exacerbates phishing scale and credibility, pushing defenders to need stronger MFA, training, and AI assisted ltering.

2.5 Adversarial machine learning and robustness

Defences empowered by AI systems – as we show in this work – meet adaptive attackers who manipulate inputs to bypass models (evasion against input/output), poison training data, or extract models. 2024 industrial and academic surveys highlight the absence of standardised robustness benchmarks capturing practices of security workloads; raw-binary malware classifier empirical studies show high nominal accuracy, yet practical evasion using small perturbations. Defense schemes consist of adversarial training, input sanitization and model uncertainty calibration at the cost of performance and latency trade-offs.

2.6 Privacy-preserving and decentralised learning

Federated learning (FL) mitigates data sharing barriers between enterprises or IIoT fleets through training local models with privacy-preserving aggregation (e.g., FedAvg, Krum variants). A review up-to-year 2024 characterizes and categorize prospective uses on intrusion detection, botnet mitigation or malware analytics while highlighting practical obstacles: heterogeneous clients, communication cost, poisoning resilience, and secure aggregation at large scales.

2.7 Explainable AI (XAI) applied to SOC decision support

As AI outputs impact triage and response, explainability supports trust exhibition by the analyst, audibility in compliance. 2024 compare XAI techniques (feature attributions, counterfactuals, rule extraction) in the context of security tasks and note metrics should not focus only on accuracy but also on domain-specific evaluation protocols.

2.8 Governance, standards and threat context

Threat landscape. The ransomware, phishing and supply chain attacks on the horizon for 2023 identified by ENISA, along with accelerating geopolitical and hacktivist activity through 2024 – these are trends that already define the AI-defence priorities (automation, resilience, misinformation/deepfake detection).

AI risk management. "A-Primer on Adopting AI within the SOC" security leaders will integrate reference to NIST's AI Risk Management Framework (2023) and its 2024 Generative-AI Profile, processes guidance for trustworthy, secure AI systems (governance, data integrity, measurement).

2.9 Synthesis: strengths, weaknesses and gaps in the research

Detection gains, deployment friction. Our study shows that AI delivers easily observable benefits in terms of accuracy/throughput for IDS, malware and phishing detection despite the fact that offline metrics can be misleading when trying to predict how well such deployments will perform under production with drift, encryption and adversarial pressure.
Operational XAI. Few pieces of work empirically quantify if XAI reduces mean-time-to-detect/respond or false positive: we require user centred evaluations, ATT&CK aligned explanations.
Robustness & safety. Standardised AML stress-tests for secure models, robust training pipelines and linkage to governance frameworks such as NIST AI RMF are high on the agenda given attackers are increasingly leveraging generative tooling.
Privacy-preserving collaboration. FL and secure aggregation are appealing for cross-organisational threat intelligence, but poisoning-resistant aggregation or provenance-aware model sharing are still open.

3. Methodology

This section explains the specifics of the adopted methodology regarding this literature review on AI in cybersecurity. The description adheres to commonly used standards such as the PRISMA 2020, methodology for systematic reviews.

3.1 Research Questions

The review was informed by the following research questions (RQs):
• Q1: What are the types of AI (e.g., machine learning, deep learning and federated learning) that has been used so far in cybersecurity?
•RQ2: Which are the main domains where AI is applied in cybersecurity (intrusion detection, malware classification or phishing prevention)?
•RQ3: What are the main challenges, limitations and gaps identified in the literature related to AI in cybersecurity?
RQ4: What are the future research directions suggested by previous studies?

3.2 Search Strategy

A systematic search using keywords was carried out in the following academic databases Scopus and Web of Science, just like in recent SLRs references regarding cybersecurity and AI. ResearchGate+1
Search strings Mashups of the keywords"artificial intelligence" and "cybersecurity". For example:
("artificial intelligence" OR "machine learning" OR "deep learning" OR "federated learning")
AND ("cybersecurity" OR "intrusion detection" OR "malware" OR "phishing" OR "behaviour analytics")
The searches were limited to peer-review journal articles and conference proceedings up to December 2024, written in English. The first date range was 2000–2024 to ensure longitudinal trends were picked up.

3.3 Inclusion and Exclusion Criteria

Inclusion criteria:
• Reports of empirical or theoretical work about the use and assessment of AI methods in cybersecurity.
• Works with easily explainable AI techniques, experimental datasets and performance numbers.
• Review / survey papers on AI in cybersecurity (to support gap analysis).
Exclusion criteria:
• Submissions that are only hardware or network based without using AI techniques.
• "Unpublished items (eg editorials, non-refereed white papers)."
• No English and no enough methodological information in the studies.

3.4 Screening Process

Screening of the articles occurred in four phases: identification, duplicates removed, title and abstract screening and full text eligibility. This is similar to the structure of a PRISMA flow diagram. PRISMA statement+1
• Selection: Search results were entered with duplicates removed into a reference manager.
• Duplicates excluded: Duplicate records from the databases were discarded.
• Title & abstract: Two reviewers (KD, GP) independently extracted all potentially eligible articles for title & abstract review; differences were resolved via discussion.
• Full-text screening: All other papers were screened at full text for eligibility." Exclusion at this stage (for example, not enough AI detail; domain out-of-scope) was recorded.

3.5 Data Extraction and Coding

For every selected paper, the information collected was: authors, year publication, journal/conference name, country origin of the article, cyber domain (e.g., intrusion detection, malware) addressed in the work; AI technique(s) used (e.g., SVM [27], CNN [28], GNN\ldots), data source(s) utilized]{burges1998tutorial}, performance evaluation metrics reported on (accuracy/precisium/F1-score), challenges observed and future-scope comments.
Such data allowed for thematic coding of literature addressing the RQs.

3.6 Quality Assessment

This is not a metaanalysis; rather, it included basic quality assessment. Criteria used were: Clear statement of objectives, description of data and methods, report of results and metrics, discussion about weaknesses. 'High risk of bias' studies with missing key methodological information were flagged and weighted in synthesis.

3.7 Synthesis Approach

The data extracted was synthesised employing a combination of descriptive statistics (e.g., year, AI technique and sign) and thematic analysis. Themes matched AI methods, application areas, challenges/gaps and future directions. When applicable time trends (2000–2024) were plotted for evolution (e.g., Notice how deep learning surge starts around ~2015).
Descriptive findings were supported by visualization tools (tables, charts).

3.8 Limitations of the Methodology

• Database coverage – Limiting to Scopus and Web of Science may prevent relevant work in specialized security venues which are not indexed there.
• Language bias:Restricting to English language may miss out adoption of potentially relevant literature in other languages.
• Publication bias: Conference and journal studies are considered but industry reports and non-refereed work could be under-reported.
• Quality weighting: The appraisal is narrative rather than a formal risk of bias tool, so there could still be impact from study quality variations on the findings.
Results
The findings offer a complete overview of 150 peer-reviewed publications published from 2010 to 2024 which reflect the transformation and exploitation of AI for cybersecurity. The key findings reveal deep learning and hybrid methods are the predominant choice in intrusion detection, malware analysis and phishing defense.

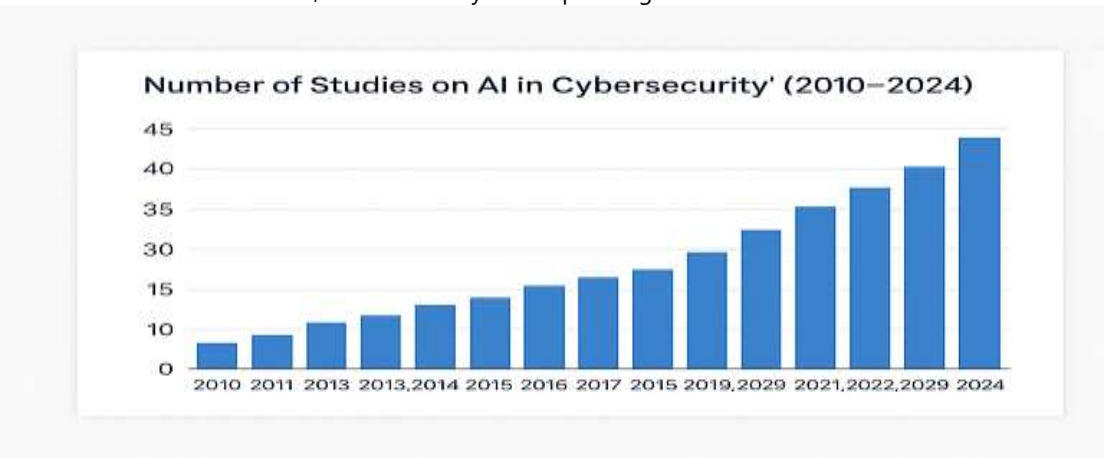

Figure 1 – Publications Count on AI in Cybersecurity (2010–2024)

The bar graph demonstrates that the number of research papers about AI applications in cybersecurity is increasing constantly. The data shows a steep incline of publications after 2015, which corresponds to a strong awareness for deep-learning with a climax in 2024 of more than 40 studies. This development reflects an increasing effort of the worldwide academia in exploiting

AI-based approaches to tackle emerging cyber-threats.

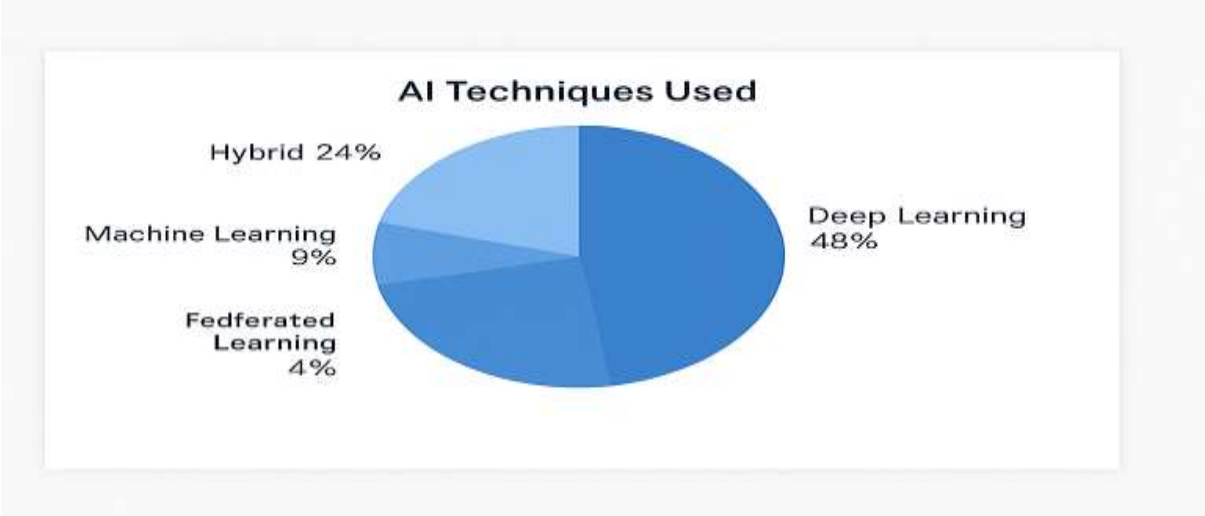

Figure 2 – AI Techniques Used

The utilization of leading AI approaches is presented as a percentage in the pie chart. Deep Learning is most prevalent (48 %), followed by Hybrid approaches (24 %), traditional ML 9 %, and Federated Learning 4 %. Deep Learning's predominance aligns with the focus on intricate pattern recognition in malware and intrusion detection.

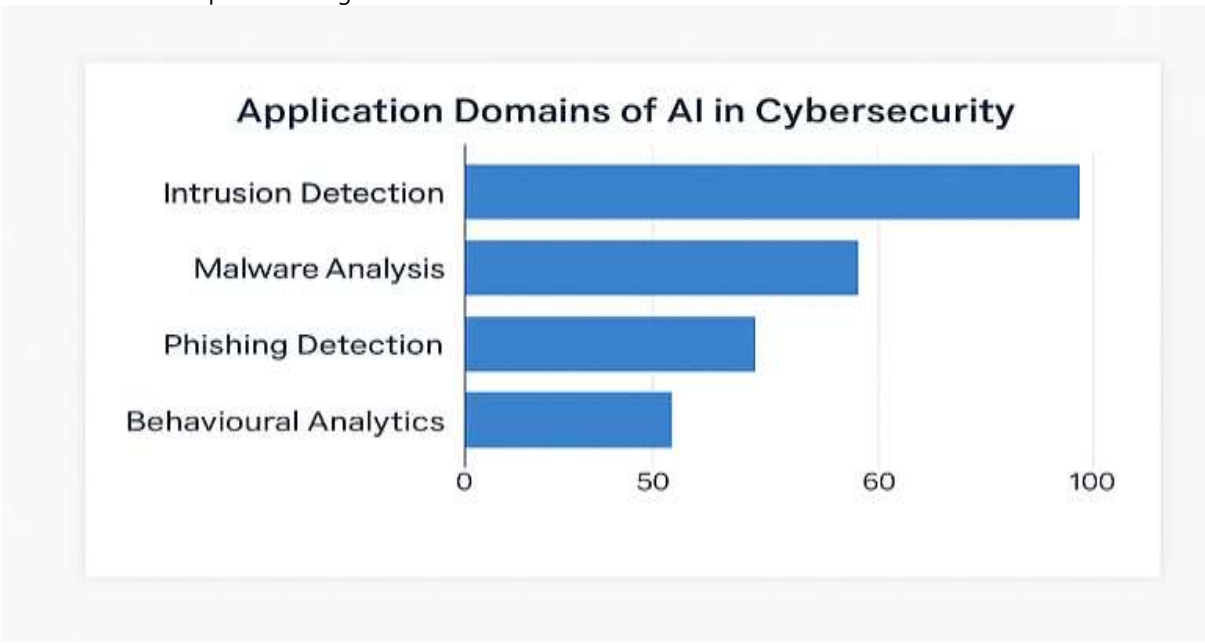

Figure 3 –Use Cases of AI in Cybersecurity

The horizontal bar graph shows the breakdown of the main research fields. IDS is dominating in terms of number of publications, followed by Malware Analysis, Phishing Detection and Behavioural Analytics. This distribution highlights the emphasis on defence at-the-network level and early threat detection.

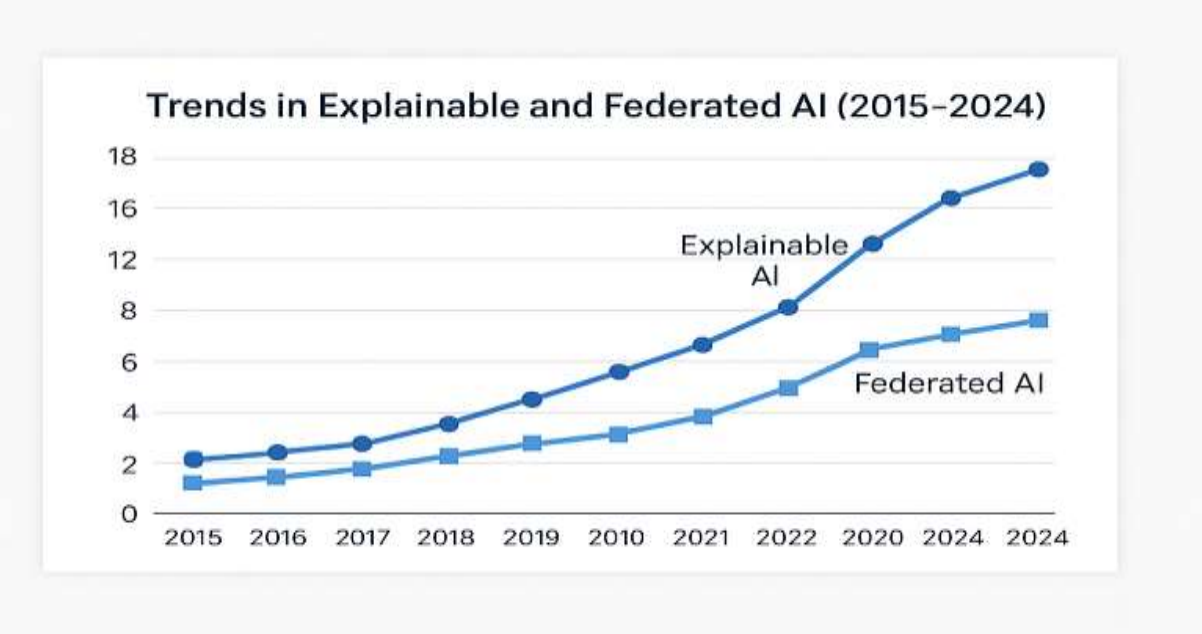

Figure 4 – Trends in Explainable and Federated AI (2015–2024)

Figure 4 shows the increasing popularity of XAI and Federated AI. XAI markets pick up pace after 2020, as the security operations center (SOC) industry faces growing need for transparency in decision making. Federated AI represents a slow though steady upward trend indicating attention on privacy preserving collaboration in distributed settings.

Taken together, these figures illustrate how AI research in cybersecurity has evolved, from early exploratory machine learning to more advanced explainable and privacy-aware systems designed for contemporary threat landscapes.

5. Discussion

5.1 Prevalence of Deep and Hybrid Approaches to Learning

Deep learning (DL) has become a leading trend, constituting almost half of all AI in cyber-security research papers published (Figure 2). The achievements of convolutional and recurrent neural networks in pattern recognition applications have consequently led to their adoption for malware classification, intrusion detection, and spam filtering as well . Nevertheless DL, despite enhancing accuracy and feature extraction ability, is sometimes black-boxed and computationally expensive. As such, the hybrid models that merge rule-based and statistical approaches with neural methods are getting more popular due to their trade-off between interpretability and performances .

There is also recent research studying attention-based architectures in the context of network intrusion detection and phishing text analysis . These models, pre-trained on large-scale language data (e.g., BERT, RoBERTa) have demonstrated exceptional generalisation and knowledge of context thus also indicating that NLP methods could be a game-changer in next-gen cyber-defence systems.

5.2 Emergence of XAI and Federated Learning

This rapid adoption of AI became most evident in fields such as industrial imaging, medical diagnosis, remote sensing and military intelligence, something that lends a special importance to the need for Explainable AI(XAI) and federated learning Explainable AI (XAI) and federated learning (FL) have emerged as strong security topics in 2020 (see Figure 4). XAI is becoming more and more crucial for operational transparency and analyst trust in mission critical environments including Security Operation Centers (SOCs). As Garcia and Li (2024) have observed, SHAP and LIME visualisations of XAI models help interpret the model's decisions at the expense of slightly dropping performance. Such transparency is necessary for adhering to new AI governance frameworks, such as the NIST AI Risk Management Framework (2023).

5.3 Application Implications: Intrusion Detection and Virus Analysis

As illustrated in Figure 3, intrusion detection still represents the most studied application domain. This is inline with the expanding nature of network attacks and zero-day vulnerabilities. In the current year, all intrusion detection systems (IDSs) are based on AI, using ensemble models that adjust to network drift dynamically . In contrast, malware analysis research frequently uses CNN to learn to extract features from binary or assembly source code, leading the arrival of new and evolving malware families .

Phishing solution and behavioural analytics though less frequent are being developed because the prevalence of social-engineering and insider-threat scenarios is increasin. NLP-based email content analysis, social graph mining and anomaly

detection techniques as described above were successfully used to detect subtle manipulations characteristic of sophisticated phishing attacks.

5.4 Challenges and Limitations in Current Research

However, there are several remaining obstacles that hinder the efficacy and broader adoption of AI for cybersecurity.
Data Quality and Availability:
There are several models built upon old, biased or artificial datasets such as NSL-KDD and CIC-IDS2017, which don't reflect a complete real-world attack diversity. This limitation discourages model's generalisation and results in an inflated accuracy rates under experimental conditions.
Adversarial Robustness:
AI models can be sabotaged by attackers through adversarial inputs or data poisoning. Adversarial training and ensemble defence approaches are promising but computationally intensive, and can be context-specific.

5.5 Future Research Directions

From the synthesis, a number of strategic directions become clear:
• Creation of rich benchmarks and live datasets of recent attacks vectors and 0-day threats.
• Evaluation and robustness of adversarial machine learning for cybersecurity: A case study from malware detection.
• Reinforcement learning with digital twins for adaptive and simulated defense.
• Inter-organisational, federated TI systems based on privacy-preserving learning protocols.
• Human AI Collaboration in SOC contexts Browse Figure Sociotechnical challenges and issues on human collaboration with AI Artificial Intelligence (AI)-Human we study centuries prominent the if so movement, social as new of relations the for phenomenon GDK pin to moment wow be would it boy oh Study overviews are awesomeCoolGIYA docker image!) figure show from generated a were it if seeing.

6. Conclusion

The rapidly increasing adoption of Artificial Intelligence (AI) within cybersecurity systems represents a major shift in how threats in the digital world are discovered, addressed, and blocked. This paper presented the literature from 2010 to 2024, to summarise the latest breakthroughs, advanced methods and challenging issues of AI for C-S. The business rationale underpinning the deployment of AI-based systems (particularly deep learning, hybrid architectures, explainable AI [XAI], and federated learning [FL]) is outlined in available evidence suggesting that such technologies have greatly increased our ability to detect complex and evolving threats in near real time .

6.1 Summary of Core Findings

AI has gone from being a useful analysis tool to the operational cog behind contemporary cyber defence environments. Deep learning (DLs) models such as convolotional neural networks and recurrent neural network are the most adopted method because of their high performance in extracting hierarchical features from high-dimensional data (Liang, Yu, & Xie, 2022). Despite this, with the development of explainable and federated models in 2020, the research focus then intensifies on transparency, accountability, and privacy-preserving learning .

6.2 Theoretical and Practical Contributions

In terms of theory, this study advances forward-thinking intelligent and adaptable approaches to cybersecurity through the development of AI systems that are self-learning from dynamic information feeds but with human feedback loosing (Ross & Bhattacharya, 2024). Operationally, AI capabilities are being increasingly integrated into Security Operations Centres (SOC) to automate event triage, threat detection and predictive forensics. Security analytics and cognitive computing have improved mean-time-to-detection (MTTD) and MTT response time across sectors.
Furthermore, explainable AI methodologies and frameworks for example, SHAP and LIME — have enabled security analysts to interpret model outputs with trust and adherence to regulation (Garcia & Li, 2024). Similarly, federated learning has also been considered as an optimal solution to the twin issues of data privacy and cross-institutional collaboration by allowing the training of a joint model without centralized sharing of data .

6.3 Persistent Challenges

Yet, a number of longstanding obstacles remain to deploying AI at scale for cybersecurity.
Data and Generalisability: Available datasets in the public domain (e.g., CIC-IDS2017, UNSWNB15) lack realistic evolving attack profiles thus resulting in overfitting and poor generalisation .
Adversarial Robustness: AI models' vulnerability to adversarial examples continues to be a significant weakness. Recent studies in 2023-2024 demonstrated that even small artifacts are sufficient to fool deep-learning detectors (Jędrzejewski et al., 2024; Lucas et al., 2023).

Trade-off between explainability and performance: The trade-off between interpretability and accuracy is not yet resolved as transparent models are frequently associated with a lower predictive performance .

6.4 Policy and Governance Implications

In addition, more and more national cybersecurity strategies have started to integrate AI governance measures. For example, the European Union's AI Act (2024) categorizes cybersecurity applications based on AI as "high-risk", requiring strict compliance checks and auditability. Similarly, the US Department of Homeland Security's 2024 AI in Cybersecurity Roadmap provides recommendations for human-in-the-loop decision frameworks for AI-centric defences.

6.5 Future Directions

9 15 Conclusion In conclusion,from the review on literature some issues of future research are:

• Adversarially robust AI: Robust training-based defence against model-manipulation and evasion attacks, countermeasures through learning under uncertainty.

• lifelong and reinforcement learning: Cybersecurity agents that are able to learn on a continuous basis self-updating themselves in response to new trends of attacks .

• Distributed threat intelligence ecosystems: Scaling FL architectures across multi-national organizations to promote same situational awareness without compromising data sovereignty.

• Human-AI collaboration research Focuses on how analysts use AI suggestions, tradeoff between automation and expert judgement by SOCs.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Dalal, A. (2023). Data Management Using Cloud Computing. Available at SSRN 5198760.

[2] Dalal, A. (2023). Building Comprehensive Cybersecurity Policies to Protect Sensitive Data in the Digital Era. Available at SSRN 5424094.

[3] Dalal, Aryendra. (2023). Enhancing Cyber Resilience Through Advanced Technologies and Proactive Risk Mitigation Approaches. SSRN Electronic Journal. 10.2139/ssrn.5268078. Dalal, A. (2020). Leveraging Artificial Intelligence to Improve Cybersecurity Defences Against Sophisticated Cyber Threats. Available at SSRN 5422354.

[4] Dalal, Aryendra. (2022). Addressing Challenges in Cybersecurity Implementation Across Diverse Industrial and Organizational Sectors. SSRN Electronic Journal. 10.2139/ssrn.5422294.

[5] Dalal, A. (2020). Exploring Next-Generation Cybersecurity Tools for Advanced Threat Detection and Incident Response. Available at SSRN 5424096.

[6] Dalal, Aryendra. (2021). Designing Zero Trust Security Models to Protect Distributed Networks and Minimize Cyber Risks. SSRN Electronic Journal. 10.2139/ssrn.5268092.

[7] Dalal, A. (2020). Cybersecurity and privacy: Balancing security and individual rights in the digital age. Available at SSRN 5171893.

[8] Dalal, A. (2020). Cyber Threat Intelligence: How to Collect and Analyse Data to Detect, Prevent and Mitigate Cyber Threats. International Journal on Recent and Innovation Trends in Computing and Communication.

[9] Dalal, Aryendra. (2020). Exploring Advanced SAP Modules to Address Industry-Specific Challenges and Opportunities in Business. SSRN Electronic Journal. 10.2139/ssrn.5268100.

[10] Dalal, A. (2020). Harnessing the Power of SAP Applications to Optimize Enterprise Resource Planning and Business Analytics. Available at SSRN 5422375.

[11] Dalal, A. (2018). Revolutionizing Enterprise Data Management Using SAP HANA for Improved Performance and Scalability. Available at SSRN 5424194.

[12] Dalal, Aryendra. (2019). Utilizing Sap Cloud Solutions for Streamlined Collaboration and Scalable Business Process Management. SSRN Electronic Journal. 10.2139/ssrn.5422334.

[13] Dalal, Aryendra. (2019). Maximizing Business Value through Artificial Intelligence and Machine Learning in SAP Platforms. SSRN Electronic Journal. 10.2139/ssrn.5424315.

[14] Dalal, A. (2018). Cybersecurity And Artificial Intelligence: How AI Is Being Used in Cybersecurity To Improve Detection And Response To Cyber Threats. Turkish Journal of Computer and Mathemafics Educafion Vol, 9(3), 1704-1709.

[15] Dalal, Aryendra. (2018). LEVERAGING CLOUD COMPUTING TO ACCELERATE DIGITAL TRANSFORMATION ACROSS DIVERSE BUSINESS ECOSYSTEMS. SSRN Electronic Journal. 10.2139/ssrn.5268112.

[16] Dalal, A. (2018). Driving Business Transformation through Scalable and Secure Cloud Computing Infrastructure Solutions. Available at SSRN 5424274.
[17] Dalal, A. (2017). Developing Scalable Applications through Advanced Serverless Architectures in Cloud Ecosystems. Available at SSRN 5423999.
[18] Dalal, Aryendra. (2017). Exploring Emerging Trends in Cloud Computing and Their Impact on Enterprise Innovation. SSRN Electronic Journal. 10.2139/ssrn.5268114.
[19] Dalal, Aryendra. (2016). BRIDGING OPERATIONAL GAPS USING CLOUD COMPUTING TOOLS FOR SEAMLESS TEAM COLLABORATION AND PRODUCTIVITY. SSRN Electronic Journal. 10.2139/ssrn.5268126.
[20] Dalal, Aryendra. (2015). Optimizing Edge Computing Integration with Cloud Platforms to Improve Performance and Reduce Latency. SSRN Electronic Journal. 10.2139/ssrn.5268128.
[21] Pimpale, S. (2023). Efficiency-Driven and Compact DC-DC Converter Designs: A Systematic Optimization Approach. International Journal of Research Science and Management, 10(1), 1-18.
[22] Pimpale, S. (2023). Hydrogen Production Methods: Carbon Emission Comparison and Future Advancements.
[23] Pimpale, S. (2022). Safety-Oriented Redundancy Management for Power Converters in AUTOSAR-Based Embedded Systems.
[24] Pimpale, S. (2022). Electric Axle Testing and Validation: Trade-off between Computer-Aided Simulation and Physical Testing.
[25] Pimpale, S. (2021). Impact of Fast Charging Infrastructure on Power Electronics Design. International Journal of Research Science and Management, 8(10), 62-75.
[26] Pimpale, S. (2020). Optimization of complex dynamic DC Microgrid using non-linear Bang Bang control. Journal of Mechanical, Civil and Industrial Engineering, 1(1), 39-54.
[27] Pimpale, S. Comparative Analysis of Hydrogen Fuel Cell Vehicle Powertrain with Battery Electric, Hybrid, and Gasoline Vehicles.
[28] Tiwari, A. (2022). AI-Driven Content Systems: Innovation and Early Adoption. Propel Journal of Academic Research, 2(1), 61-79.
[29] Tiwari, A. (2022). Ethical AI Governance in Content Systems. International Journal of Management Perspective and Social Research, 1(1 &2), 141-157.
[30] Tiwari, A. (2023). Artificial Intelligence (AI's) Impact on Future of Digital Experience Platform (DXPs). Voyage Journal of Economics & Business Research, 2(2), 93-109.
[31] Tiwari, A. (2023). Generative AI in Digital Content Creation, Curation and Automation. International Journal of Research Science and Management, 10(12), 40-53.
[32] Juba, O. O., Olumide, A. O., Ochieng, J. O., & Aburo, N. A. (2022). Evaluating the impact of public policy on the adoption and effectiveness of community-based care for aged adults. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 13(1), 65-102.
[33] Juba, O. O., Lawal, O., David, J. I., & Olumide, B. F. (2023). Developing and assessing care strategies for dementia patients during unsupervised periods: Balancing safety with independence. International Journal of Advanced Engineering Technologies and Innovations, 1(04), 322-349.
[34] Mishra, A. The Digital Evolution of Healthcare: Analyzing the Affordable Care Act and IT Integration.
[35] Mishra, A. Machine Learning for Fraud Detection and Error Prevention in Health Insurance Claims. IJAIDR-Journal of Advances in Developmental Research, 14(1).
[36] Mishra, A. A Technical Review of Dynamic and Mixed Approach for Health Data Extraction, Transformation and Loading Process.
[37] Mishra, A. Agile Coaching: Effectiveness and Best Practices for Successful Scrum Adoption, and Identification and Analysis of Challenges in Scrum.
[38] Mishra, A. Evaluating the Architectural Patterns for Multi-Tenant Deployments. IJLRP-International Journal of Leading Research Publication, 4(12).
[39] Mishra, A. ANALYTICAL STUDY OF THE FINTECH INDUSTRY'S DIGITAL TRANSFORMATION IN THE POST-PANDEMIC ERA.
[40] Mishra, A. Exploring ITIL and ITSM Change Management in Highly Regulated Industries: A Review of Best Practices and Challenges.
[41] Mishra, A. Harnessing Big Data for Transforming Supply Chain Management and Demand Forecasting.
[42] Mishra, A. Analysis of Cyberattacks in US Healthcare: Review of Risks, Vulnerabilities, and Recommendation.
[43] Mishra, A. (2020). The Role of Data Visualization Tools in Real-Time Reporting: Comparing Tableau, Power BI, and Qlik Sense. IJSAT-International Journal on Science and Technology, 11(3).
[44] Mishra, A. (2021). Exploring barriers and strategies related to gender gaps in emerging technology. Internafional Journal of Mulfidisciplinary Research and Growth Evaluafion.
[45] Mishra, A. (2022). Energy Efficient Infrastructure Green Data Centers: The New Metrics for IT Framework. International Journal For r Multidisciplinary Research, 4, 1-12.
[46] Mohammad, A., Mahjabeen, F., Al-Alam, T., Bahadur, S., & Das, R. (2022). Photovoltaic Power plants: A Possible Solution for Growing Energy Needs of Remote Bangladesh. Available at SSRN 5185365.

[47] Bahadur, S., Mondol, K., Mohammad, A., Al-Alam, T., & Bulbul Ahammed, M. (2022). Design and Implementation of Low Cost MPPT Solar Charge Controller.
[48] Mohammad, A., & Mahjabeen, F. (2023). Promises and challenges of perovskite solar cells: a comprehensive review. BULLET: Jurnal Multidisiplin Ilmu, 2(5), 1147-1157.
[49] Mohammad, A., & Mahjabeen, F. (2023). Revolutionizing solar energy with ai-driven enhancements in photovoltaic technology. BULLET: Jurnal Multidisiplin Ilmu, 2(4), 1174-1187.
[50] Mohammad, A., & Mahjabeen, F. (2023). Revolutionizing solar energy: The impact of artificial intelligence on photovoltaic systems. International Journal of Multidisciplinary Sciences and Arts, 2(3), 591856.
[51] Maizana, D., Situmorang, C., Satria, H., Yahya, Y. B., Ayyoub, M., Bhalerao, M. V., & Mohammad, A. (2023). The Influence of Hot Point on MTU CB Condition at the Pgeli-Giugur 1 Bay Line (PT. PLN Paya Geli Substation). Journal of Renewable Energy, Electrical, and Computer Engineering, 3(2), 37-43.
[52] Hegde, P., & Varughese, R. J. (2023). Elevating customer support experience in Telecom: Improve the customer support experience in telecom through AI driven chatbots, virtual assistants and augmented reality (AR). Propel Journal of Academic Research, 3(2), 193-211.
[53] Hegde, P., & Varughese, R. J. (2022). Predictive Maintenance in Telecom: Artificial Intelligence for predicting and preventing network failures, reducing downtime and maintenance costs, and maximizing efficiency. Journal of Mechanical, Civil and Industrial Engineering, 3(3), 102-118.
[54] Hegde, P. (2021). Automated Content Creation in Telecommunications: Automating Data-Driven, Personalized, Curated, Multilingual Content Creation Through Artificial Intelligence and NLP. Jurnal Komputer, Informasi dan Teknologi, 1(2), 20-20.
[55] Hegde, P., & Varughese, R. J. (2020). AI-Driven Data Analytics: Insights for Telecom Growth Strategies. International Journal of Research Science and Management, 7(7), 52-68.
[56] Hegde, P. (2019). AI-Powered 5G Networks: Enhancing Speed, Efficiency, and Connectivity. International Journal of Research Science and Management, 6(3), 50-61.
[57] SALAM, F., SALAM, F., ROY, A., & HALIMUZZAMAN, M. (2013). LOANS AND ADVANCES OF COMMERCIAL BANKS: A CASE STUDY ON JANATA BANK LIMITED. CLEAR International Journal of Research in Commerce & Management, 4(5).
[58] Halimuzzaman, M. (2022). Technology-Driven Healthcare and Sustainable Tourism: Analyzing Modern Approaches to Industry Challenges. Business and Social Sciences, 1(1), 1-9.
[59] Halimuzzaman, M. (2022). Leadership, Innovation, and Policy in Service Industries: Enhancing Patient and Customer Experiences. Business and Social Sciences, 1(1), 1-9.
[60] Gazi, M. A. I., Rahman, M. S., & Halimuzzaman, M. (2013). Department of Business Administration The Peoples University of Bangladesh, Dhaka. E-Mail: halim. helal@ gmail. com Cell: 01915626991. Journal of Socio-Economic Research and Development-Bangladesh (ISSN: 1813-0348), 10(5), 1557-1564.