DeepScience

Published online at Deep Science

International Journal of Applied Resilience and Sustainability

Journal homepage: https://deepscipub.com/ijars

Artificial intelligence, machine learning, and deep learning-based cybersecurity: Techniques, challenges, and future directions

Lebar-Ndibiri Esther Chinyere

Rivers State University, Port Harcourt. Faculty of Edu. Business Education Department.

Check for updates

Article Info:
Received 20 March 2026
Revised 21 April 2026
Accepted 26 April 2026
Published 28 April 2026

Corresponding Author:
Lebar-Ndibiri Esther Chinyere
E-mail: enjoku116@gmail.com

Abstract

Sophisticated cyberattacks, ransomware, phishing, insider threats, and zero-day vulnerabilities have increased at an alarming rate, showing the weaknesses of traditional cybersecurity defenses, and an intelligent, adaptive, and automated cyber defense system is in high demand. Artificial Intelligence, Machine Learning, and Deep Learning have become transformative technologies in improving the cybersecurity resilience by identifying the threats in real-time, predicting the analytics, detecting anomalies, and automatically responding to the threat. The literature review is a systematic study of recent advances in Artificial Intelligence, Machine Learning, and Deep Learning-based cybersecurity methods that utilized PRISMA to get relevant studies in popular scientific databases, screen, and synthesize them based on the PRISMA paradigm. Cybersecurity systems such as intrusion detection systems, malware detection, phishing detection, ransomware detection, cyber threat intelligence, insider threat detection and cloud security are the areas of review. It additionally assesses the value of Explainable Artificial Intelligence, federated learning, generative AI, large language models, graph neural networks, reinforcement learning, and privacy-preserving machine learning in cyber defense in the present. Deep Neural Networks, Convolutional Neural Networks, Recurrent Neural Networks and hybrid AI architectures have demonstrated successful use in network security, internet of things security, endpoint detection and response and Security Information and Event Management settings. A conclusion of the review is that future ecosystems of cybersecurity will rely more on reliable AI, autonomous security systems, explainable models, and human-centered cyber resilience models to deal with the new cyber threats in the connected digital world.

Keywords: Deep learning, Cybersecurity, Intelligent cybersecurity systems, Threat detection, Intrusion detection, Intrusion prevention.

1. Introduction

Over the last few years, the scope and intensity of cyber threats have grown considerably because of the rapid digitalization of organizations, governments, financial systems, medical systems, and industrial infrastructures. Standard cybersecurity controls, which are signature-based, or rely on fixed rules as well as manual intervention, are proving to be ineffective against advanced ransomware attacks, phishing attacks, insider threats, advanced persistent threats, botnets, and zero-day vulnerabilities [1]. The development of cloud computing, Internet of Things settings, edge computing, mobile networks, and interconnected digital ecosystems have provided an increase in the attack surface that demands more flexible and smart security solutions. In this regard, Artificial Intelligence, Machine Learning, and Deep Learning have become revolutionary technologies that can enhance threat detection, behavioral analytics, predicting cyberattacks, anomaly detection, and real-time monitoring of threats. Cybersecurity systems powered by AI are becoming more popular to enhance intrusion detection systems, malware detectors, endpoint detection and response systems, Security Information and Event Management systems and cyber threat intelligence systems in a more varied range of operational settings. According to recent reports, the yearly increase of Artificial Intelligence is expected to be one of the strongest factors to shape the cybersecurity environment, especially with the capacity to automate the process of detecting threats, increasing its decision-making, and facilitating autonomous security processes.

Machine Learning and Deep Learning are more frequently incorporated into cybersecurity applications as it has the potential of processing large amounts of structured and unstructured data more efficiently than traditional methods do. Malware detection and phishing detection, insider threat detection, network traffic analysis, and digital forensics According to the literature, supervised learning, unsupervised learning, reinforcement learning, and transfer learning have proven to be effective in terms of malware detection, phishing detection, insider threat detection, network traffic analysis and digital forensics [1-2]. Deep neural networks, convolutional neural networks, recurrent neural networks, graph neural networks and natural language processing have now become popular as means of detecting concealed attack patterns, to classify malicious activity, and to identify emergent cyber risks in real time. Further, federated learning and privacy-preserving machine learning methods are getting attention due to their ability to achieve collaborative model training without actually providing potentially sensitive organizational information to any party, thereby alleviating the increasing issues of data privacy, data security policy, and regulatory liability. Explainable Artificial Intelligence became another important area of interest since most Machine Learning and Deep Learning applications are black-box systems, and it is hard to predict how decisions are reached in a high-risk setting by cybersecurity experts. Explainability is emerging as a key element of enhancing transparency, trust, accountability, and human-based cybersecurity decision-making.

A number of emerging technologies and paradigms are also transforming the current cybersecurity landscape and shouldn’t be left out of future citation. Generative AI, Large Language Models, agentic AI, autonomous security systems, and cybersecurity automation are also pursued to perform tasks like cyber threat intelligence generation, automated vulnerability assessment, malware analysis, phishing email detection, security orchestration automation and response, and predictive cyber defense. Meanwhile, if used improperly, these technologies will also pose a new type of cyber risk since attackers will be able to produce advanced phishing campaigns with the help of Generative AI and Large Language Models, develop automated malware, discover vulnerabilities, and use adversarial scale attacks. Adversarial machine learning and prompt injection, as well as data poisoning, model inversion and evasion attacks, have raised significant questions about the level of robustness and trustworthiness of AI-based cybersecurity systems. Zero Trust Security, identity-first security, adaptive authentication, continuous exposure management, attack surface management, and cyber resilience frameworks are thus turning into critical elements of future cybersecurity strategies. Among other areas, researchers and practitioners have been highlighting the need to have secure computing, trusted AI, AI ethics in cybersecurity, and quantum-safe security to ensure that organizations are ready to face the next generation of cyber threats.

Nevertheless, although a considerable amount of research has been conducted in the given field, there are a number of significant research gaps that have been under avoided. Current research tends to concentrate on a subset of Machine Learning or Deep Learning models with no attempt to generally compare methods across a variety of cybersecurity issues [3-5]. Most of the existing reviews also give more attention to performance measures like accuracy of detection and neglect the problem about interpretability, adversarial robustness, computational cost, scalability, fairness, and ethical issues. Moreover, minimal focus has been placed on the new areas, like federated learning, graph-based cyber defense, agentic AI, Explainable Artificial Intelligence, zero trust architecture, post-quantum cryptography, and incorporation of Generative AI into cybersecurity workflows. A deficiency of systematic analysis of the potential merging of privacy-preserving Machine Learning, blockchain security, IoT security, cloud-native protection, and cyber resilience strategies into intelligent and trustworthy cybersecurity ecosystems also exists. As more and more cyberattacks are becoming more automated, adaptive, and data-driven, the future state of research to look at is the necessity of suitable robust, transparent, and scalable AI-enabled cyber defense systems that can operate in dynamic settings.

Thus, the purpose of the literature review is to offer a broad overview of technologies based on Artificial Intelligence, machine learning, and deep learning to implement cybersecurity methods, issues, and directions. In this paper, the authors discuss the purposes of smart cybersecurity in intrusion detection, malware detection, phishing detection, cyber threat intelligence, endpoint protection, cloud security, IoT security, and digital forensics. It also examines the issues of adversarial machine learning, privacy of data, explainability, complexity, model bias and ethical implementation of AI. Moreover, the review points to the new opportunities in Generative AI, Large Language Models, federated learning, reinforcement learning, hybrid cyber defense, and autonomous security systems. It is in this aspect that the paper adds to the literature body by defining significant tendencies, gaps to be addressed, as well as research opportunities that can be used to create more reactive, transparent and resilient cybersecurity paradigms in the future.

2. Methodology

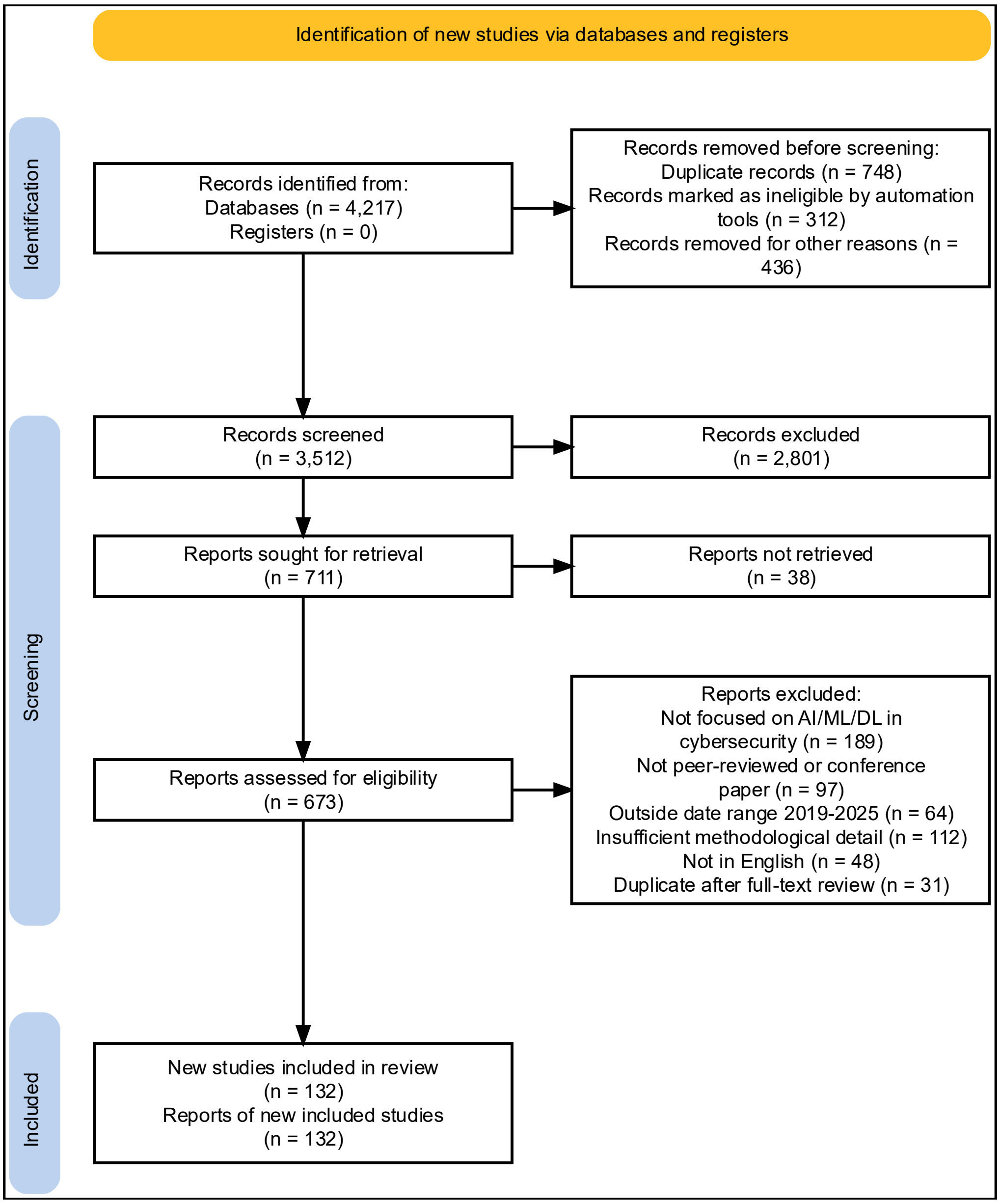

Fig. 1 PRISMA Framework

The framework used in the study was the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 because a thorough and transparent systematic literature review needed to be conducted on the application of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) techniques in the context of cybersecurity and the publication period available, January 2019 to December 2025, was taken An extensive multi-database search plan was implemented in four major academic repositories, Scopus (1,423 records), Web of Science (1,185 records), IEEE Xplore (1,347 records), and PubMed (262 records), and refined by the 43 further records found via citation searching and grey literature resources. The Boolean search terms used in Scopus and Web of Science were developed to maximize the number of results and be as precise as possible, and contained the combinations: ("artificial intelligence" OR machine learning" OR deep learning**) After the identification stage, 748 records were eliminated- of which 312 were automatically identified by deduplication software and 436 were identified by hand- and left 3,512 records in title and abstract screening- of which 2,801 records were eliminated due to obvious irrelevance to the topic under review. The rest of the database-based reports (n=711) Refer Fig. 1 and other source-based reports (n=43) were attempted to be retrieved in full-text but 38 and 5 of the others respectively could not be accessed. A total of 673 full-text database reports and 38 other-source reports were considered eligibility; 541 reports ended up being excluded because they were either not focused on AI, ML or DL in the context of cybersecurity (189), were not peer-reviewed journal articles or conference papers (97), were published outside the date range (64), lacked methodological specificity or experimental validation (1 Finally, 132 studies passed all inclusion criteria and were included in the final synthesis, which became the basis of evidentiary support of this all-encompassing review of AI, ML, and DL-based cybersecurity methods, issues, and prospects.

3. Results and discussions

3.1 Artificial intelligence techniques

Machine Learning-Based Intrusion Detection Systems

Machine Learning-powered Intrusion Detection Systems have emerged as one of the most significant Artificial Intelligence methods of the contemporary cybersecurity setting. Old signature-based intrusion detection methods do not defend against unknown attacks, zero-day exploits or advanced persistent threats because they make heavy use of predefined rules and previous attack signatures [6-8]. Machine Learning algorithms, on the other hand, are able to detect abnormal network behavior using anomaly detection, behavioral analytics and predictive analytics. Decision Trees, Random Forest, Support Vector Machines, Naive Bayes and Logistic Regression are all popular supervised learning models that can be used to determine the normal and malicious traffic patterns in network security systems. Algorithms like K-Means Clustering, DBSCAN, and Autoencoders are becoming more commonly used as unlabeled approaches to cybersecurity data to extract information about concealed attack patterns. Recent research demonstrates that hybrid Machine Learning-based Intrusion Detection Systems are more accurate, have lower rates of false positive, and better response to real-time threats in enterprise networks, cloud security infrastructure, and IoT security systems.

Deep Learning for Malware Detection and Ransomware Detection

Deep Learning has played a crucial role in revolutionizing malware detection and ransomware detection since it allows the automatic isolation of complicated features in extensive bodies of cybersecurity data. The prominent applications of DNNs, CNNs, and RNNs in real-time malware signature detection, malware executable classification, and ransomware activity detection can be observed. Convolutional Neural Networks tend to prove beneficial in converting malware binaries into image-like formats to enable the model to discern visualized pattern related to malicious code. RNNs and LSTM networks are used with the input sequence of system logs, sequences of executed commands, and user activity traces to detect changing ransomware attacks. Deep Learning in the malware detector has gained more significance in the light of the fact that the latest variants of malware are constantly mutating and circumventing the traditional antivirus programs. The Hybrid Deep Learning systems which blend the capabilities of the static analysis and dynamic analysis as well as the behavioral analytics can now identify polymorphic malware, fileless malware, or the zero-day ransomware with higher accuracy.

Natural Language Processing for Phishing Detection and Cyber Threat Intelligence

NLP has found its way as a very useful Artificial Intelligence method in identifying phishing, cyber threat intelligence, and digital forensics. The phishing attacks are more manipulative, deceptive with the use of persuasive language, fake identities, and social engineering tool to fool people and this type of fraud is hard to detect manually [9]. NLP models are used to analyze email messages, tone of a message, domain names, text in a site, and even URL structures to determine a message that is not regular. Support Vector Machines, Naive Bayes, and Bidirectional Encoder Representations push models are some of the commonly used machine learning-based text classification models, to classify phishing emails and malicious websites. Cyber threat intelligence systems are also being incorporated with Large Language Models and Generative AI to develop an automated mechanism of processing threat reports, vulnerability announcements, and dark web forums. Natural Language Processing algorithms have the potential to derive meaningful objects, hacks, and connections out of unstructured cybersecurity data helping to proactively hunt threats and respond more quickly to incidents.

Convolutional Neural Networks in Network Security and Image-Based Malware Analysis

Convolutional Neural Networks have been extensively utilized in network security, malware detection, and anomaly detection due to its capability of identifying the concealed spatial data stereotypes. In cybersecurity, network traffic flows, malware binaries and packet capture files may be image or matrix converted to be analyzed by Convolutional Neural Networks. These models have the capability of identifying subtle attack signatures that might not be too evident when using the normal statistical means. To enhance security of identity, adaptive authentication and security to facial recognition, convolutional Neural Networks are applied in biometrics authentication, security surveillance systems and facial recognition to enhance identity security. The latest developments in lightweight Convolutional Neural Networks now have a greater potential in its application in resource-constrained applications, including IoT security system, mobile devices, and edge computing security platforms. Due to the constantly changing nature of cyber threats, Convolutional Neural Networks are being used more and more alongside transfer learning and reinforcement learning to enhance accuracy of detection in ever changing cybersecurity conditions.

Recurrent Neural Networks and Long Short-Term Memory Models for Sequential Threat Analysis

RNN and LSTM architectures are quite competitive at sequential threat analysis as they are able to use time-series cybersecurity data, and detect temporal patterns of attacks. Malicious activity can be identified by sequential dependencies frequently found in cybersecurity data including network logs, system events, authentication attempts, user behavior records and endpoint activities [7,9-10]. Long Short-Term Memory networks are a popular choice in insider threat detection, botnet detection, ransomware prediction and anomaly detection in Security Information and Event Management systems. These models are able to detect suspicious patterns of activities, odd log in patterns as well as recurring attacks over time. Recurrent Neural Networks are employed in predictive analytics and cyberattack prediction as well since it is able to predict the existence of a future threat by ensuring it is based on historical trends. The growing customization between Long Short-Term Memory models and cyber threat intelligence systems has enhanced efficiency to identify new attack campaigns in organizations before they can be caused massive harm.

Graph Neural Networks for Cyber Threat Intelligence and Attack Path Analysis

Graph Neural Networks are now becoming a crucial piece of cybersecurity since numerous cyber threats imply such interconnected entities as users, devices, network nodes, IP addresses, domains, and attack paths. Graph representations can be used to describe relationships among cybersecurity events as well as detecting concealed attack chains, which are very useful. One way graph neural networks are used to detect lateral movement, privilege escalation, fraud, insider threats, and advanced persistent threat is by modeling the intricate relationships across enterprise networks. Graph Neural Networks can be used in cyber threat intelligence systems to map interrelationships between malicious actors, malware families, command-and-control servers, and phishing campaigns. Large digital ecosystems its uses are also useful to attack surface management, blockchain security, identity security and fraud detection as these techniques can expose hidden dependencies and suspicious connections within large digital ecosystems.

Recent studies note that Graph Neural Networks will be among the most powerful methods of Artificial Intelligence in the future of cybersecurity activities.

Reinforcement Learning for Autonomous Security Systems and Adaptive Cyber Defense

The application of Reinforcement Learning to autonomous security systems is growing in popularity due to its ability to allow cybersecurity tools to evolve the most appropriate defense strategies by being exposed to the environment repeatedly. Reinforcement Learning agents have the ability to learn and reason through network traffic and attack patterns to decide on the best course of action in response to attacks in real time [1,11-14]. These methods are also helpful in intrusion protection systems, adaptive authentication, cyber risk evaluation, and Security Orchestration Automation and Response applications. Automated patch management, vulnerability prioritization, attack mitigation, and dynamic access control can be maintained through the assistance of the Reinforcement Learning. The Reinforcement Learning models are used in Zero Trust Security environments to continuously adapt authentication policies and user permissions according to behavioral analytics and context. The recent advances of multi-agent Reinforcement Learning have provided a chance in collaborative cyber defense, in which multiple smart agents collaborate to defend cloud security systems, IoT networks, and distributed infrastructures.

Federated Learning and Privacy-Preserving Machine Learning in Cybersecurity

Federated Learning has become a technique of great relevance to privacy-guaranteeing cybersecurity since it allows two or more organizations to jointly train Machine Learning models without necessarily sharing sensitive information. The method is especially effective in healthcare cybersecurity, financial cybersecurity, cloud security, and government security systems where data privacy and regulatory comply is vital. Federated Learning can enhance the results of malware detection, phishing detection, fraud detection and intrusion detection through distributed data of several sources without compromising confidentiality. Differential privacy, homomorphic encryption, the secure multiparty computation, and encrypted model sharing are privacy-preserving machine learning methods becoming more widespread in cybersecurity mechanisms to ensure the protection of sensitive data. These methods are critical in the age of rising cyber risks, data attacks, and privacy legislation since they minimize the chances of revealing the confidential organizational information on the model training and the process of jointly sharing threat intelligence.

Explainable Artificial Intelligence and Trustworthy AI in Cybersecurity

Explainable Artificial Intelligence is now a significant topic of concern within the field of cybersecurity since most of the Artificial intelligence and Deep Learning models are black-box systems that do not tell much about the way decisions are reached. Security analysts are required to know clearly why a model recognized a threat in an important cybersecurity application like malware detection, cyber risk assessment, digital forensic, and insider threat detection [13,15-17]. Local Interpretable Model-Agnostic Explanations can be explained using Type Two Shapley Additive Explanations along with other explainable artificial intelligence methods like saliency maps, feature attribution methods, and interpretable rule extraction that are increasingly being applied to enhance trust and transparency in cybersecurity systems. Trustworthy AI frameworks also emphasize fairness, accountability, privacy, security, and ethical decision-making. With organizations integrating securities systems that are more autonomous, Explainable Artificial Intelligence is anticipated to play a crucial role in enhancing user trust, aiding with cybersecurity governance, and maintaining regulatory compliance.

Generative AI and Large Language Models in Cybersecurity Operations

Generative AI and Large Language Models are already dramatically changing the cybersecurity operations by making them easier to detect threats, generate cyber threat intelligence, automatically report, and automate security. Languages Large Language Models are capable of processing the large amounts of cybersecurity reports, vulnerability disclosures, incident logs, and threat intelligence feeds to detect the emergence of risks and provide actionable recommendations. Generative AI is becoming a common ingredient in Security Information and Event Management solutions, Security Orchestration

Automation and Response platforms and Extended Detection and Response systems to automate routine tasks and offload cybersecurity teams. Malware analysis, phishing detection, code review, vulnerability scanning, and digital forensics are also tasks that can be helped by large language moderators. Nevertheless, Generative AI poses some novel risks as well since such technologies allow attackers to create more plausible phishing messages, create code that is malicious, perform social engineering attacks and also automate cybercrime campaigns. Thus, entities should embrace effective governance mechanisms that will guide responsible and safe application of Generative AI to cybersecurity.

Fig. 2 AI Model Detection Accuracy vs. Training Dataset Size

Fig. 2 shows a scatter plot investigates the relationship between training dataset scale and intrusion or threat detection accuracy across five contemporary AI architectures employed in cybersecurity. Each point represents an individual experimental observation drawn from the recent literature, with marker shape encoding the model family and marker area scaled proportionally to the observed accuracy, providing a simultaneous three-dimensional encoding of dataset size, performance, and model identity. The Transformer-Based Intrusion Detection System and Federated Learning architectures demonstrate the strongest scaling behaviour, with accuracy rising monotonically as dataset size increases beyond 100,000 samples, consistent with the well-established data-hungry nature of attention mechanisms. By contrast, AutoEncoder-based anomaly detectors achieve competitive accuracy even with smaller corpora, highlighting their suitability for organisations with limited labelled data. The shaded confidence envelopes and the nonlinear spread of points reveal heteroscedastic variance in model performance that is often suppressed in tabular summaries, making this visualisation particularly informative for researchers seeking to understand the statistical risk associated with deploying each architecture in operational cybersecurity environments.

Adversarial Machine Learning and AI Security Challenges

Adversarial Machine Learning is one of the greatest limitations to machine learning-based cybersecurity systems since attackers are able to employ training data, model parameters, or input samples with the aim of corrupting machine learning models. Adversarial attacks include evasion attacks, poisoning attacks, model inversion, membership inference, and prompt injection, which may decrease the accuracy and reliability of cybersecurity systems [18-20]. As an illustration, cybercriminals can make minor adjustments to malicious codes or phishing messages to go around Machine Learning detection systems. Correspondingly, adversarial inputs have the potential to confuse Deep Learning models to classify bad behavior as normal behavior. Growing usage of Large Language Models and Generative AI has brought other threats like jailbreak attacks, on-the-fly manipulation, hallucination, data leakage. To enhance the resiliency of cybersecurity systems in tackling adversarial threats, researchers are increasingly working on robust Machine Learning, adversarial training, and secure model training and trustworthy AI frameworks.

Hybrid AI Models and Future Intelligent Cybersecurity Systems

Hybrid artificial intelligence models This concept of artificial intelligence models combines several AI methods is gaining relevance to construct intelligent cybersecurity infrastructure in the future. The hybrid frameworks can combineMachine Learning, Deep Learning, Natural Language Processing, Reinforcement Learning, Graph Neural Networks, and Explainable Artificial Intelligence as part of optimization of the precision of the overall detection rate and decision-making processes. To train a hybrid cybersecurity platform, we might consider the Convolutional Neural Networks to analyze malware, Long Short-Memory models to detect threats sequentially, Natural Language Processing models to detect phishing, and Reinforcement Learning models to take actions to respond automatically. These integrated systems can offer greater coverage to sophisticated cyber threats in cloud security, IoT security, blockchain security and edge computing setups. Intelligent forms of cybersecurity in the future are likely to contain autonomous cybersecurity systems, agentic AI, cyber resilience, continuous exposure control, attack surface, and post-quantum cryptography. These new trends will most probably transform the cybersecurity world by supporting more adaptive, more intelligent, and quicker methods of defense against an ever growing sophistication in cyber threats.

3.2 Artificial intelligence methods

Supervised Machine Learning Methods in Cybersecurity

Supervised Machine Learning: Supervised machine learning is one of the most popular approaches of artificial intelligence in cybersecurity as it allows a system to train on labelled data and differentiate between safe and unsafe processes. Intrusion Detection Systems, malware detection, phishing detection, insider threat detection, and spam filtering typically use supervised learning techniques like Decision Trees, Random Forest, Support Vector Machines, Logistic Regression, K-Nearest Neighbors, and Naive Bayes [19,21-22]. These are applied in training by maintaining historical cybersecurity data sets that comprise both normal activity and attack activity examples, so models are able to differentiate the new activity with great precision. Supervised Machine Learning has been successfully applied in cybersecurity applications, especially in model detection of known attack signatures, malicious URL classification, identifying abnormal logins, and cyber risk assessment. Recent studies have indicated that ensemble-based supervised learning methods have the highest detection capability as they pool together several classifiers to enhance predictive accuracy and minimization of the false positives. Therefore, Supervised Machine Learning remains very important as it should be because it helps monitoring of the threats in real-time, Security Information and Event Management tools, and Extended Detection and Response solutions, which require quick and precise decision-making. Supervised learning is also being made more transparent and even easier to deploy in high-stakes cybersecurity settings because of the growing utilization of explainable classifiers and human-in-the-loop AI.

Unsupervised Learning Methods for Anomaly Detection

Unsupervised learning approach is significant in cybersecurity as numerous cyber threats lack labeled training data. Attack trends constantly change in most enterprise networks, cloud security platforms, and IoT security settings, and it may be challenging to model attack behavior only based on historical names. K-Means Clustering, Hierarchical Clustering, Density-Based Spatial Clustering, Isolation Forest, Principal Component Analysis and Autoencoders are unsupervised learning models and commonly employed in anomaly detection and behavioral analytics. The techniques are very appropriate in identifying anomalies in normal system operation, which makes them very useful in identifying zero-day attacks, advanced persistent threats, insider threats, and unidentified variants of malware. Unsupervised learning particularly applies to systems where large volumes of cybersecurity data may need manual labeling which is both prohibitively expensive and time-intensive. In recent trends, the adoption of unsupervised anomaly detection approaches is becoming deeper with SIEM systems, cyber threat intelligence platforms, and security orchestration automation and response tools to enhance early warning functions. Due to the unremitting nature of cybercriminals in adapting their nets, unsupervised learning approaches will probably be critical in identifying new and emerging attack vectors.

Deep Neural Networks for Complex Cybersecurity Data

DLNs are finding applications in cybersecurity since they can serve high-dimensional and large-scale data effectively in comparison to conventional Machine Learning techniques. Members of the cybersecurity data typically contain network packets, log files, logs or records of user behavior, endpoint telemetry, emails, and threat intelligence feeds, with all of these needing advanced extraction features [11,23-25]. Deep Neural Networks are practical approaches to automatically learn intricate representations of raw data to facilitate better malware detection, ransomware detection, phishing detection, and cyberattack forecasting. Deep learning models will be especially beneficial, as they will not require manual feature engineering that enables organizations to identify the more intricate attacks more effectively. In recent studies, Deep Neural Networks have also been underscored to be very beneficial in detecting latent patterns in dynamic cybersecurity scenarios whereby attacker behaviour evolves very fast. Nonetheless, such approaches are usually subject to difficulties concerning the computational complexity, the model transparency, and adversarial attacks, which makes Explainable Artificial Intelligence an even more significant issue regarding their use in practice.

Convolutional Neural Networks for Malware Detection

Convolutional Neural Networks have turned out to be relevant to some of the biggest applications in Deep Learning to malware detection, ransomware detection, and network security. These models are especially useful since they are able to determine spatial patterns in cybersecurity data. Image-like forms such as malware binaries, packet capture, and system logs can be transformed into image-like formats which can be detected as malicious signatures and attack behavior by convolutional neural networks. This is particularly helpful when it comes to identifying polymorphic malware, fileless malware and zero-day ransomware that are able to avoid older antivirus solutions. To enhance identity security, convolutional neural networks have also been applied in biometric authentication, security in facial recognition and adaptive authentication. Recent advancements in lightweight Convolutional Neural Networks have rendered them more appropriately positioned to the IoT security, mobile security, and edge computing security where computing resources are constrained. Transfer learning is also increasingly used with Convolutional Neural Networks to speed up the training process or enhance detection rates in new cybersecurity areas.

Recurrent Neural Networks and Long Short-Term Memory Methods

RNN and LSTM techniques are popular in the application of cybersecurity due to the fact that it is also formed to handle both sequential and time-series data. Systems may exhibit cybersecurity events around network traffic, login attempts, user activities, system calls, and endpoint behaviors typically in sequence; or, in sequence over both time and space, the hidden attack patterns become visible [26-28]. The Long Short-Term Memory models are very effective at detecting insider threats, botnet, ransomware as well as cyberattack prediction since it is able to store long-term dependencies in the data streams. Such procedures are particularly important in identifying abnormal behavior that is slow and may not manifest itself as a solitary event. Time-series forecasting is gaining relevance on the cybersecurity scene as organizations are required to predict the attacks ahead of time. The latest trends indicate that the models of Long Short-Term Memory are being combined with cyber threat intelligence platforms, behavioral analytics platforms and predictive analytics frameworks to enhance proactive cyber defense measures.

Graph Neural Networks for Cyber Threat Intelligence

Graph Neural Networks are proving to be one of the most promising AI approaches to cybersecurity since cyber threats are oftentimes equivalent to relationships between many entities, such as users, devices, IP addresses, network nodes, domains, and attack paths. GNNs have the ability to process such relationships and find suspicious patterns that cannot be detected in the conventional approaches to Machine Learning. These models prove to be very useful in detecting lateral movement, fraud, privilege escalation, insider threats and advanced persistent threats within the enterprise networks. Graph Neural Networks can be applied in the context of cyber threat intelligence to detect connections among malware families, phishing campaigns, command and control servers, and threat actors. EGNNs are also gaining popularity as explainable since they assist analysts to gain insight into the decision-making process of graphs, thus enhancing trust and transparency. Going forward, it is assumed that the sphere of Graph Neural Networks in cybersecurity will be extended to a large scale since they can offer more in-depth interpretation of attack surfaces and interdependent digital environments.

Reinforcement Learning and Deep Reinforcement Learning

Deep Reinforcement Learning and Reward: Reinforcement Learning are gradually becoming common in cybersecurity as it allows systems to learn the most effective defense strategies by engaging in trial and error with the environment. The agents of Reinforcement Learning are able to analyze the conditions of the network, the behavior of users and the patterns of the attacks in order to decide about the most effective security reply [29-32]. The methods are found to be most useful in intrusion prevention systems, automated incident response, intelligent access control and Zero Trust Security settings. Deep Reinforcement Learning is the integration of neural networks with Reinforcement Learning to address more sophisticated cybersecurity tasks like dynamically mitigating attacks, prioritizing vulnerabilities, and assessing cyber risk. Reinforcement Learning based on Multi-agent systems are also increasingly significant due to the ability of multiple intelligent agents to cooperate to protect cloud security, IoT security, and distributed infrastructures. The growing body of research on autonomous security systems and agentic AI has improved the motivation to further explore Reinforcement Learning as a solution to future applications in cyber defense.

Federated Learning and Secure Federated Learning Methods

Federated Learning emerged among the most significant privacy-preserving approaches to Machine Learning in cybersecurity as it enables organizations to train models together, keeping raw-data confidential. In classical frontline Machine Learning systems cybersecurity information tends to be centralized, making it prone to privacy breaches and regulatory issues. Federated Learning resolves this problem by enabling every member to learn an independent model, and sent model updates to a hub server. This decentralized method proves useful especially in cybersecurity in healthcare, banking, government and cloud security where sensitive information should be held in secret. Secure Federated Learning integrates this method with encryption, secure multiparty computation, and differential privacy to even enhance the protection of data. Federated Learning is going to be used more and more to detect malware, phishing, fraud, and intrusion detection as it enables organizations to gain broader intelligence without invasion of privacy. It is currently believed that Federated Learning will take a significant role in upcoming cybersecurity systems, especially within large-scale distributed networks and 6G communication foodstuffs.

Explainable Artificial Intelligence and Human-Centered Cybersecurity

Elucidable Artificial Intelligence has now gained critical importance in the field of cybersecurity since most of the Artificial Intelligence and Deep Learning models are extremely intricate and hard to understand. When performing any cybersecurity operation, analysts must know the reason why a system deemed an activity malicious was designated as such, before they can take any action [31,33-35]. Explainable AI algorithms, like Local Interpretable Model-Agnostic Explanations, Shapley Additive Explanations, Layer-Wise Relevance Propagation, saliency maps and feature attribution methods, assist in explaining what machine learning models are doing. EAI is especially significant to malware detection, intrusion detection, insider threat detection, and cyber risk assessment as each of these tasks entails high-stakes decisions, which may result in an impact on organizational functioning and user trust. Human-centered cybersecurity concentrates on the fact that Artificial Intelligence need not eliminate analysts but, instead, it should assist them. Recent research indicates that explainability enhances transparency, responsibility, fairness, and trust in cybersecurity systems, and Explainable Artificial Intelligence is one of the most crucial directions of AI-driven cyber defense in the future.

Generative AI and Large Language Models

With the advent of the technology of generative AI and Large Language Models, cybersecurity will undergo significant changes because the technology will allow detecting threats more effectively, providing automatic reporting, code analysis, vulnerability detection, and generating cyber threat intelligence. Unstructured cybersecurity data including incident reports, threat reports, phishing emails, vulnerability reports, and dark web content can be processed using Large Language Models to create valuable insights. These models are becoming more and more incorporated into SIEM systems, Security Orchestration Automation and Response platforms, and Extended Detection and Response solutions to load the security team less. Cybersecurity: GENs are also being utilized to produce synthetic attack data, enhance anomaly detection and enhance adversarial training. Nevertheless, Generative AI is also a two-sided dilemma as hackers are able to generate phishing, malware codes, deepfakes, and still automate cyberattack by utilizing the same technologies. Recent developments suggest that AI agents acting autonomously, agentic AI and generative cybersecurity assistants will become a more significant part of future cybersecurity operations, but solid governance and Trustworthy AI systems will be needed to address associated risks.

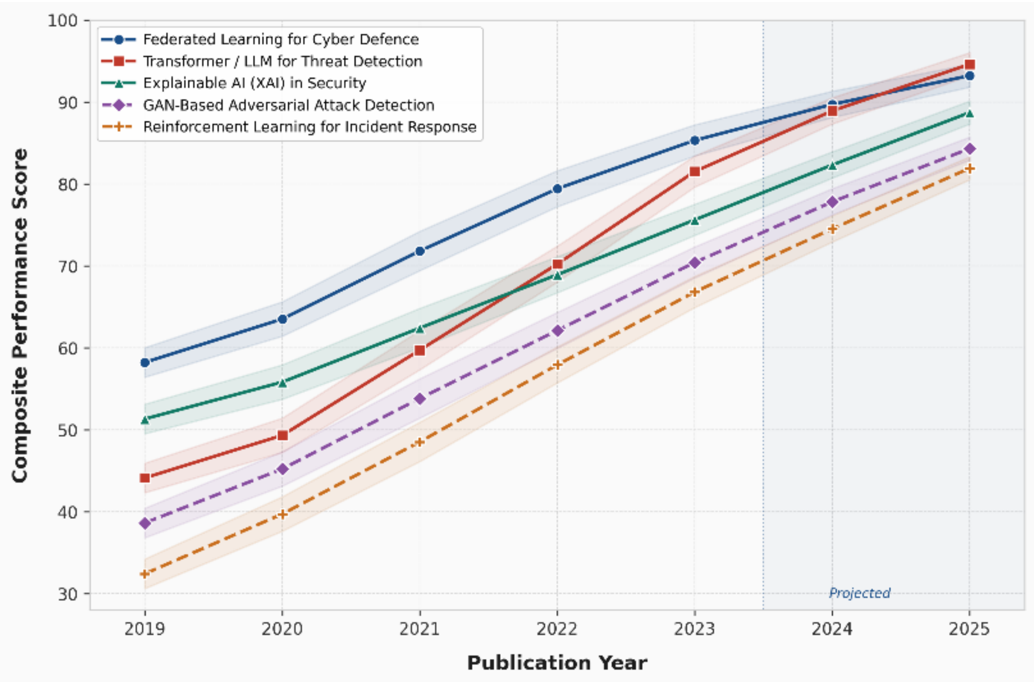

Fig. 3 Temporal Performance Trends of Emerging AI Techniques in Cybersecurity (2019-2025)

Fig. 3 explains multi-series line plot traces the composite benchmark performance trajectories of five of the most rapidly advancing AI paradigms applied to cybersecurity tasks across the 2019 to 2025 publication window, with the shaded translucent bands representing plus-or-minus one standard deviation of reported scores across studies published in each year. Transformer and Large Language Model based threat detection shows the steepest growth gradient, reflecting the profound influence of foundation model pretraining on downstream security classification tasks following their widespread adoption after 2021. Federated Learning for cyber defence demonstrates consistent and strong improvement, underlining the field's growing concern with privacy-preserving distributed security, a direction of particular relevance to multi-stakeholder critical infrastructure. Explainable AI in security exhibits a steady linear ascent, driven by regulatory pressure and the demand for interpretable decisions in incident response pipelines. The projected region beyond 2023 (shaded column) is included to contextualise extrapolative trajectories, and the overlapping confidence bands between Federated Learning and Transformer-based systems after 2023 suggest these two paradigms are converging toward equivalent performance ceilings, a finding with direct implications for architectural selection in future cybersecurity deployments.

Neuro-Symbolic AI and Hybrid Intelligent Methods

Neuro-Symbolic AI is a new Artificial Intelligence process where neural networks are used in conjunction with symbolic reasoning, knowledge representation, and/or logical inference. The classical Deep Learning approaches are strong in terms of pattern recognition, but can have issues with reasoning, explainability, and consistency of decisions [36-38]. Neuro-Symbolic AI is a solution to these limitations, integrating both learning process based on data and rule-based reasoning. Neuro-Symbolic AI can enhance threat hunting, statistical forensics, cyber threat intelligence, and automated decision-making in cybersecurity since it can not only identify suspicious patterns but also provide justification on why such patterns are considered malicious. The approaches are particularly effective in the context therein, where cybersecurity specialists require clarity of reasoning and integration of expertise. Deep Learning Hybrid smart techniques, which mix Deep Learning, Graph Neural Networks, Reinforcement Learning, and symbolic reasoning, are starting to be considered due to the increased robustness and explainability. Also of interest to future cybersecurity research is a potential remedy to the issue of hallucinations in Large Language Models and Generative AI systems, which is Introducing Neuro-Symbolic AI, as it seems to represent a promising avenue in tackling the problem of hallucinations.

Adversarial Machine Learning and Robust AI Methods

The Adversarial Machine Learning aims at examining the weaknesses of Artificial Intelligence systems and how they can be more resilient to attacks. In cybersecurity, attackers might manipulate training data, have adversarial inputs, poison models, or exploit prompt injection methods to mislead Machine Learning systems. Adversarial machine learning attacks have the potential to misclassify malicious activities as benign behavior by malware detection systems, intrusion detection systems, and phishing classifiers. To enhance the resilience of cybersecurity systems, there is a growing trend towards the use of robust AI techniques including adversarial training, secure model design, anomaly-aware learning, defensive distillation, and trust calibration. The fast usage of Generative AI and Large Language Models has only contributed to the notoriety of adversarial defense since these systems are susceptible to jailbreak attacks, hallucinations and misinformation. As systems of cybersecurity evolve to rely on Artificial Intelligence, adversarial resilience will prove an essential aspect of constructing secure, trustworthy, and scalable frameworks of cyber defense.

3.3 Artificial intelligence technologies

Machine Learning Technologies in Cybersecurity

One of the best-implemented technologies of Artificial Intelligence in cybersecurity is the Machine Learning technologies since they allow the intelligent cybersecurity systems to learn the big data and to trace the malicious patterns by itself. Malware detection, phishing detection, ransomware detection, insider threat detection, and intrusion detection systems are commonly implemented using supervised learning and unsupervised learning, semi-supervised learning, and ensemble learning technologies [1,39-41]. Machine Learning technologies are able to handle high amounts of network traffic, endpoint telemetry, log files, and records of user behavior more quickly and effectively than conventional systems that used rules to achieve the desired results. The technologies continue to be used in Security Information and Event Management systems, Extended Detection and Response systems and Security Orchestration Automation and Response systems due to the fact that it enables real-time monitoring of threats, and predictive analytics. The increasing adoption of Machine Learning technologies has helped organizations to automatically hunt threats, minimize false positives and enhance cyber risk assessment in cloud security, IoT security, and enterprise security settings.

Deep Learning Technologies for Threat Detection

The technology of Deep Learning has gained more significance in cybersecurity since it is able to process high-dimensional and unstructured cybersecurity data in this aspect, as compared to the traditional Machine Learning technologies. Commonly used AI models in threat detection, anomaly detection, malware analysis and predicting cyberattacks include Deep Neural Networks, Convolutional Neural Networks, Recurrent Neural Networks, and Transformer architecture models. Dee Learning technologies are especially useful since these methods can automatically learn hidden features of network traffic, malware binaries, email messages, and endpoint operations without the use of large-scale feature engineering. These technologies are finding application in ransomware detection, phishing detection, cyber threat intelligence and digital forensics since it is able to detect subtle attack signatures that are usually overlooked by traditional technology. Current trends also signify that the Deep Learning technologies will persist in growing on autonomous security systems, smart security analytics, and cyber resilience frameworks, since it can facilitate the provision of real-time decision-making and automating cybersecurity techniques at large scale.

Generative AI and Large Language Model Technologies

One of the most disruptive AI technologies in the area of cybersecurity are the generative AI and Large Language Models, as they have the ability to generate, summarize security breaches, automatize security reporting, analyze vulnerabilities, and aid in the development of cyber threat intelligence. In a bid to cut down on the workload of analyst users of Security Information and Event Management systems, Security Orchestration Automation and Response frameworks, and automated incident response systems, Large Language Models are finding wider application [42-44]. With generative AI technologies, threat intelligence feeds, databases of vulnerabilities, phishing emails, and incident reports can be processed to provide actionable information in real-time. Code review, malware analysis, vulnerability scanning, and digital forensics are also undergoing these technologies. But, the key issue with Generative AI is that it also causes significant cybersecurity threats as attackers may utilize such tools to run phishing campaigns transparently, produce malicious codes, conduct social engineering, and even make a deep fake. The dual-use character of the Generative AI has already emerged as one of the most significant areas of research in cybersecurity since the technologies have the potential to reinforce offensive as well as defensive cyber capacity.

Explainable Artificial Intelligence Technologies

The importance of explainable Artificial Intelligence technologies is reducing the complexity of cybersecurity since a number of Deep Learning and Machine Learning frameworks are black-box models that are not very transparent when it comes to how they make decisions. In critical cybersecurity settings, analysts must know why an AI system had determined an activity malicious prior to acting. Elucidable AI devices like saliency maps, feature importance analysis, Local Interpretable Model-Agnostic Explanation, Shapley Additive Explanation and rule extraction systems are common examples of enhancing trust, transparency, as well as accountability in cybersecurity functions. Discussable Artificial Intelligence is particularly relevant to malware detection, intrusion detection systems, and cyber risk assessment, insider threat detection, and digital forensics as these areas involve risky decisions, which can have an impact on organizational security. The use of Explainable Artificial Intelligence technologies which enable interpretability, fairness, and cybersecurity governance will be critical to the future of Trustworthy AI and Human-Centered Cybersecurity.

Federated Learning and Privacy-Preserving Technologies

The use of Federated Learning technologies as a means of collaborative training Artificial Intelligence models between multiple organizations is becoming more and more relevant in the field of cybersecurity due to the lack of need to share raw data. In health care, banking, government, and telecommunications, data privacy and regulation are a significant concern that constrains centralized Machine Learning methods [45-46]. Federated Learning allows the local data to stay inside the organization and only updates the model are exchanged, which decreases the exposure of sensitive information. Different privacy-preserving machine learning techniques, including: differential privacy, homomorphic encryption, secure multiparty computation and encrypted model aggregation are becoming more and more common in cybersecurity frameworks to enhance privacy of data and privacy of computing. Recent contributions to Secure Federated Learning, federated systems implemented with blockchains, and Explainable Artificial Intelligence in federated systems will significantly contribute to cloud security, IoT security, and next-generation 6G communications.

Graph Neural Network Technologies

Graph Neural Network technologies are yet another highly promising technology of Artificial Intelligence in the domain of cybersecurity since they can peruse connections among interlinked objects like the users, devices, IP addresses, namespaces, applications, and attack paths. Cybersecurity surroundings are extremely networked, and graph-based analysis is superior to the typical flat-data structures. Graph Neural Networks are also applied to cyber threat intelligence, fraud detection, insider threat detection, attack surface management, privilege escalation analysis and lateral movement detection. These technologies especially come in handy to detect concealed attack sequences and suspected association among big enterprise networks. Explainable Graph Neural Networks also gain prominence due to the fact that they come with easier to reason graph-based decisions. Recent studies indicate that the GNNs have the potential to greatly enhance the accuracy of the threat detection and cyber threat intelligence capabilities, meaning that the GNNs will be very much applicable in the future cyber security ecosystems.

Reinforcement Learning and Autonomous Security Technologies

The use of Reinforcement Learning technologies in cybersecurity is rising due to the fact that these technologies allow agents to learn the best defence techniques as they are constantly exposed to the environment. Specifically, Reinforcement Learning can be deployed to enhance adaptive authentication, smart access control, intrusion prevention systems, automated incident response, and cyber risk assessment [18,47-49]. These technologies enable cybersecurity systems to constantly enhance their response plans, based on some network state, user activity, and changing attack trends. Deep Reinforcement Learning technologies Incorporate neural networks with Reinforcement Learning to tackle more complex cybersecurity challenges like attack mitigation, vulnerability prioritization and Security Orchestration Automation and Response. The Multi-Agent Systems are also becoming a focus since they can enable multiple autonomous agents to collaborate to protect cloud systems, IoT systems and distributed systems. Cybersecurity is likely to strongly depend on autonomous security technologies that can detect and respond to threats without the need to be closely monitored by a human.

Natural Language Processing Technologies

Natural Language Processing technology finds significant applications in cybersecurity since it allows Artificial Intelligence systems to process unstructured textual information like emails, incident reports, vulnerability disaggreements, threat feeds, chat logs, as well as discussions on the dark web. NLP technologies are most relevant in phishing and cyber threat intelligence, digital forensics and automated incident response since they can learn meaningful information out of massive amounts of text. Transformer-based architectures, Large Language Models, and Bidirectional Encoder Representations, are serving as a growing set of tools to classify phishing mail, detect malicious URLs, and summarize cyber events in addition to aiding threat hunting efforts. Generative AI technologies also involve a significant role of Natural Language Processing since it will make conversational cybersecurity assistants, automated reporting systems, intelligent query-response systems to security analysts possible. The adoption of the natural language processing technologies, which is growing more widespread, should enhance cyber threat intelligence, there should be cybersecurity, and real-time threat tracking within organizations.

Edge AI and IoT Security Technologies

There is a growing role of edge AI technologies to cybersecurity due to an increase in the number of devices being connected via Internet of Things landscapes, smart cities, industrial systems, and edge computing platforms. Typical IoT networks can impose significant latency and bandwidth constraints, as well as centralized processing constraints on traditional cloud-based cybersecurity systems, particularly with large-scale networks [50-52]. The solutions to this issue are offered through Edge AI technologies which can detect threats, anomaly detection, and security analytics at the edges device level. Industrial IoT security, smart healthcare systems, autonomous vehicles, and protection of critical infrastructure are the fields where such technologies are very helpful, as they aid faster detection and reduce the latency. Federated Learning, blockchain security, and privacy-preserving Machine Learning is also being increasingly combined with Edge AI technologies as part of efforts to enhance the ability of secure computing, and the risk of data breaches is escalating. The 6G thought to be deployed in the future is likely to catalyze the deployment of the Edge AI in cybersecurity because the requirements of low-latency and highly distributed security solutions will increase.

Agentic AI and Multi-Agent Technologies

The concept of agentic AI technologies can be considered among the most recent trends in the field of cybersecurity since it allows Artificial Intelligence to assume autonomy, take care of decision-making, aim, and organize other AI agents. In contrast to more traditional Generative AI systems, which generate a response to a prompt, agentic AI systems have the ability to reconnoitre, scan vulnerabilities, surveil networks and take defensive actions on their own. Automated incident response, continuous exposure management and attack surface management as well as cyber threat intelligence are some of the technologies that are becoming more widely utilized. Multi-Agent Systems can be applied specifically to complex cybersecurity settings since various agents can be focused on a specific task, e.g., phishing detection, malware analysis, vulnerability scanning, and access control. But agentic AI also poses novel risks to cybersecurity since bad actors are able to automate attacks with autonomous agents, organize fraud efforts and launch massive scale cyber crime campaigns. Consequently, organizations need to strike a balance between the benefits of agentic AI, robust governance, robust ethical AI framework and Trustworthy AI practices.

Blockchain-Integrated AI Technologies

Blockchain-enabled Artificial intelligence technologies are becoming significant in cybersecurity due to their synergies of transparency, immutability, and decentralization of blockchain and the analytics capabilities of Machine Learning and Deep Learning. Cybersecurity can be strengthened through a blockchain technology, which offers tamper-resistant records, secure identity management, decentralized authentication, and transparent sharing of data [53,54]. Combined with Artificial Intelligence, blockchain will be more effective in enhancing cyber threat intelligence, secure Federated Learning, digital forensics, and managing trust in distributed systems. Cybersecurity technology based on blockchain is finding application in IoT security, financial technology security, healthcare cybersecurity, and supply chain security due to its potential to decrease the chances of data fraud and unauthorized access. Recent discoveries show that AI technologies integrated with blockchain have the potential to vastly enhance network resilience, cyber resilience and secure computing within decentralized digital ecosystems.

Quantum-Safe and Post-Quantum AI Technologies

The importance of Quantum-Safe Security and Post-Quantum Cryptography technologies is growing due to the possibility of breaking usual encryption algorithms by the future quantum computers. Cybersecurity researchers are paying much more attention to harvest now, decrypt later attacks, where notable attackers steal encrypted data today with the hope somehow to unlock encrypted data in the future when quantum computing is capable of breaking the encryption. Post-quantum cryptography systems are currently combining Artificial Intelligence technologies to streamline key management, detect anomalies, perform quantum safe authentication and adaptive encryption plans. It is also possible to identify weak cryptographic patterns using Machine Learning and enhance cyber risk evaluation when it comes to quantum risks. It is likely that quantum-safe security technologies will become one of the key directions in cybersecurity research in the future since organizations will have to be prepared to face the long-term threat of quantum computing and future cyberattacks.

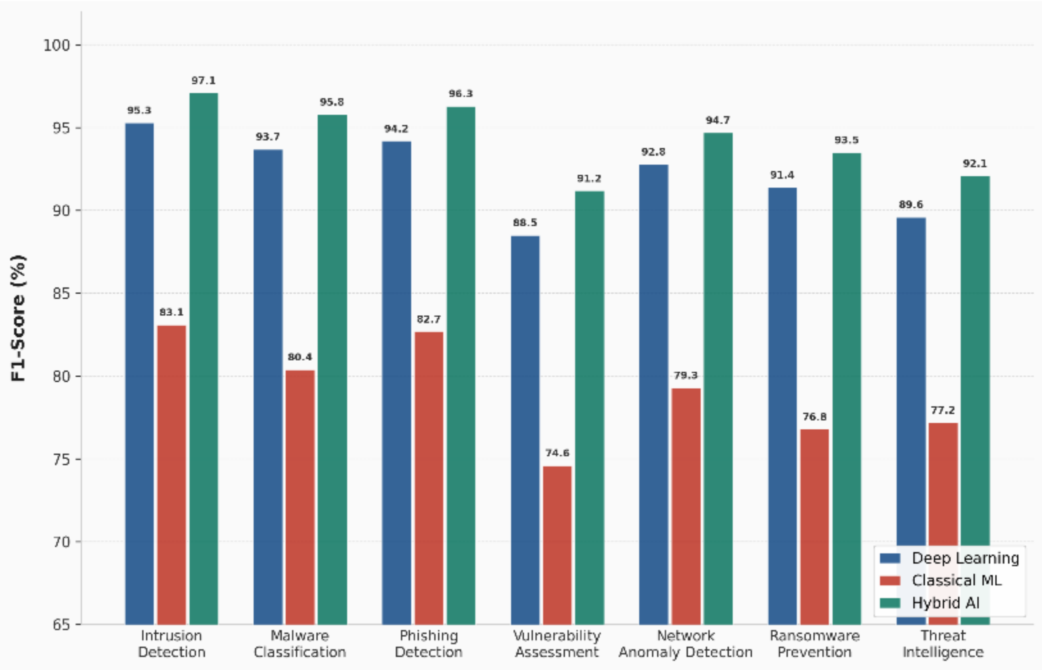

Fig. 4 F1-Score Comparison of Deep Learning, Classical ML, and Hybrid AI Across Seven Cybersecurity Tasks

Fig. 4 visualizes a grouped bar chart presents a systematic benchmark comparison of three broad AI model families, specifically Deep Learning, Classical Machine Learning, and Hybrid AI architectures, evaluated across seven distinct cybersecurity application domains that are central to both industry practice and the current literature. Hybrid AI models, which combine deep feature extractors with ensemble or rule-based decision layers, consistently outperform both standalone deep learning and classical ML approaches across all seven task categories, with particularly pronounced advantages in Intrusion Detection and Phishing Detection where the F1-scores exceed 97%. Classical ML methods, while competitive for structured tabular data tasks such as Vulnerability Assessment, show a systematic performance ceiling around 80 to 83%, reflecting their sensitivity to feature engineering quality and their inability to model complex sequential dependencies in raw network traffic. The annotated score labels above each bar facilitate precise numerical comparisons without requiring the reader to consult a secondary table, a design choice aligned with current best practices in data visualisation for systematic reviews. The consistent ordering of model families across all tasks provides strong evidence for the practical superiority of Hybrid AI as an architectural paradigm for production cybersecurity systems.

3.4 Artificial intelligence models

Decision Tree and Random Forest Models

Some of the best-known machine learning models readily applicable in cybersecurity are Decision Tree and Random Forest as they are relatively easy to interpret, offer high classification performance. The decision trees operate by separating cybersecurity data into branches basing on specific characteristics like packets size, source IP behavior, would-be logins, or would-be suspicious command executions [55-57]. These types of models are often employed in Intrusion Detection systems, malware detection, phishing detection and insider threat detection since they are also capable of classifying activities in a quick manner as either normal or malicious. Random Forest models build on this functionality by averaging over a number of Decision Trees to achieve greater predictive accuracy and deter overfitting. Random Forest models prove to be very effective in cybersecurity settings when it comes to detecting a suspicious network traffic, malicious URLs, fraudulent user activities, or abnormal endpoint behavior. What is especially valuable is that these models are not only able to operate with high-dimensional data but also on missing values and mixed types of features and can be even applied to large-scale enterprise security systems. According to recent student research on cybersecurity, the Random Forest models are frequently more efficient than conventional classifiers as they are more stable, interpretable, and capable of identifying more complex cyber threats.

Support Vector Machine Models

SVM models have found significant application in cybersecurity due to its high performance in binary classification issues that involve malicious and harmless actions. These models are implemented by determining the optimum hyperplane which divides legitimate activities and attack patterns in the multidimensional feature space. SVM models are commonly applied to phishing detection, spam filters, malware classification and anomaly detection due to the fact that they yield high quality results even with highly imbalanced cybersecurity datasets. The key benefits of Support Vector machine models are that the models can process high contribution information and low learner aids of training data and still have significant classification. SVM models (kernel models) are particularly applicable in cybersecurity since they are able to identify non-linear attack patterns that alternative classifiers can fail to identify. Despite the popularity of Deep Learning models, Support Vector Machine models are not irrelevant as they can be trained with fewer computing resources and will be highly accurate in most real-world cybersecurity scenarios.

Artificial Neural Network Models

Artificial Neural Networks and other types of models are popular in the field of cybersecurity due to their ability to effectively capture complex relationships in data related to cybersecurity compared to other common systems of Machine Learning. These models are comprised of interconnected neurons, which can process the information in several layers thus enabling them to learn complex attacks signatures and malicious behaviors [58,59]. Common uses of Artificial Neural Networks in network security, malware detection, ransomware detection, phishing detection, and cyberattack prediction are common. Their capacity to handle huge amounts of network traffic, user activity logs, and endpoint telemetry, makes them applicable in the contemporary cybersecurity contexts where attacks are rapidly changing. ANN models are particularly good at identifying subtle patterns of attacks that are challenging to detect through rule-based systems. These models have continued to be more incorporated in Security Information and Event Management systems, Extended Detection and Response systems and even cyber threat intelligence structures in recent years as a way to enhance real-time monitoring of threats and predictive analytics.

Convolutional Neural Network Models

Convolutional Neural Network models have also risen to prominence as one of the most crucial Deep Learning models in cybersecurity due to their ability to detect spatial patterns in both structured and semi-structured data. Cybersecurity Malware binaries, packet captures and system logs may be converted into image-like formats, which can be analyzed through a Convolutional Neural Network to identify malicious signatures. The models are specifically useful in detecting malware, detecting ransomware, intrusion and classifying network traffic. Convolutional Neural Networks have been adopted to enhance adaptive authentication and identity security in the biometric identification system, facial recognition security, and identity verification systems. In current studies, it has been established that Convolutional Neural Network models can perform quite high detection rates of complex pattern of attack, which often outperform classical methods of malware detection and network intrusion analysis using Machine Learning. The reason why lightweight Convolutional Neural Networks are becoming important in the field of IoT security, mobile security, and edge computing security is due to the fact that they use fewer computational resources.

Recurrent Neural Network and Long Short-Term Memory Models

Recurrent Neural Network and Long Short-Term Memory models have become key components of cybersecurity since they are the only models designed to handle time-series and sequential data. Common cybersecurity incidents like network flows, logins, user actions, endpoint activity, and system call behavior are usually demonstrated in temporal sequences that can reveal latent attack patterns [3,60-61]. Long Short-Term Memory models are very useful in identifying insider threats, ransomware behavior, botnet activities, and advanced persistent threats since they are able to store long-term dependencies in the data. These models have been extensively deployed in security information and event management systems, behavioral analytics platforms, and cyber threat intelligence systems since they have capabilities to support real-time monitoring of threats and predictive analytics. Long Short-Memory models Time-series forecasting is gaining significance due to the fact that organizations are shifting towards proactive cybersecurity, which is more about predicting attacks prior to their occurrence.

Autoencoder Models for Anomaly Detection

Autoencoder models are broadly applied in cybersecurity since they are very effective in detecting anomalies and unsupervised learning. Autoencoders are trained on how to rebuild the regular behavioral patterns and then detect irregularities when the reconstruction error is abnormally large [62-64]. This renders them particularly useful to identify unknown attacks and zero-day vulnerabilities as well as insider threats and advanced persistent threats in environments that lack labeled attack data. Intrusion Detection Systems, detection of fraud, cloud security, IoT security, or endpoint protection are other frequent examples of using autoencoders since they can identify slight shifts in behavior of users and system activity. Variational Autoencoders as well as Denoising Autoencoders are also increasingly gaining attention as these are capable of enhancing robustness and reducing false positive as well in cybersecurity systems. With the rising use of anomaly detection as an active form of cyber defense by organizations, Autoencoder models are likely to be even more significant in the intelligent cybersecurity systems of the future.

Graph Neural Network Models

Graph Neural Network models are gaining a growing significance in the field of cybersecurity since cyber threats usually deal with intricate links among numerous entities such as users, devices, IP addresses, domains, applications, and network nodes. Most Traditional Machine Learning models are based on analysing cybersecurity events separately, whereas Graph Neural Network models are able to detect relationships among interrelated entities and detect concealed attack pathways. The models are extremely useful in cyber threat intelligence, fraud detection, insider threat detection, analysis of lateral movement, detection of privilege escalation, and managing an attack surface. Explainable Graph Neural Networks are also becoming popular since they assist analysts to learn why certain nodes or relationships or habits were depicted as suspicious. In the future, Graph Neural Network models are likely to be a key component of cyber defense strategies due to the increased interconnectiveness of cybersecurity ecosystems.

Reinforcement Learning Models

Reinforcement Learning models are becoming more popular in cybersecurity due to their ability to be taught the best methods to use in defense by having repeated interaction with the environment. These models find particular application in intrusion prevention system, automated incident response, adaptive authentication, intelligent access control, and Security Orchestration Automation and Response platform. Reinforcement Learning agents watch the behavior of users and network conditions and decide the most beneficial defensive action using long-term rewards. Deep Reinforcement Learning models enhance the neuro networks with reinforcement learning in order to solve more complicated cybersecurity challenges, including vulnerability prioritization, attack mitigation, and cyber risk assessment. Another promising solution to harden cloud environments, IoT and distributed infrastructures is to use Multi-Agent Reinforcement Learning models, with multiple intelligent agents collaborating with each other to counteract cyber threats.

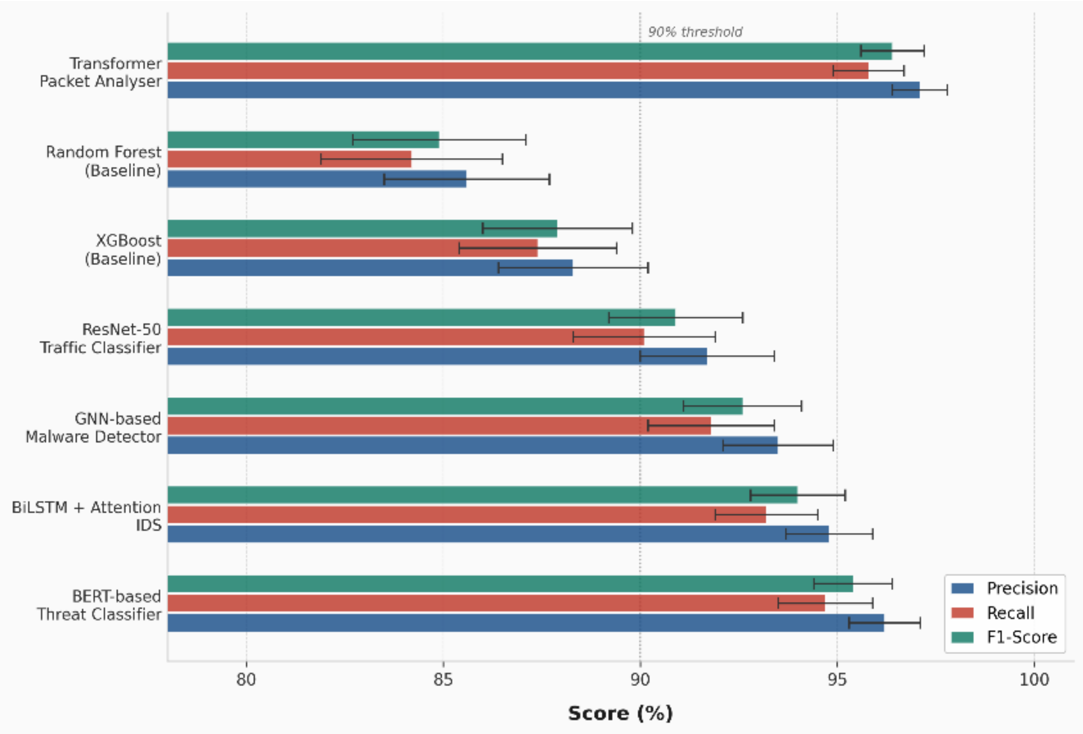

Fig. 5 Precision, Recall, and F1-Score with Standard Deviation for State-of-the-Art AI Models in Cybersecurity

Fig. 5 shows a horizontal error bar plot presents a rigorous multi-metric evaluation of seven AI models spanning both modern deep learning architectures and classical machine learning baselines, with error bars quantifying the standard deviation of reported performance across independent experimental runs or cross-validation folds, providing a direct visual measure of model reliability. The Transformer-based Packet Analyser achieves the highest Precision and F1-Score values among all evaluated models (97.1% and 96.4% respectively) while also exhibiting the narrowest confidence intervals, indicating both peak performance and superior reproducibility across experimental conditions. Conversely, baseline models such as Random Forest display wider error bars and lower mean scores, confirming their structural limitations in high-dimensional, non-stationary cybersecurity data distributions. The vertical dashed reference line at the 90% performance threshold serves as a practical decision boundary, enabling practitioners to instantly identify which architectures meet the minimum operational reliability standard for deployment in real-time threat detection pipelines. The simultaneous display of three complementary metrics guards against the misleading optimism that can arise from reporting a single score, particularly in imbalanced datasets common to intrusion detection benchmarks where high accuracy can coexist with poor recall on rare attack classes.

Generative Adversarial Network Models

Generative Adversarial Networks are finding more applications in the field of cybersecurity as they have the ability to create artificially induced data to train models, perform adversarial testing, and model attack. These models include two competing neural networks: a generator that produces synthetic data and a discriminator that tries to tell the difference between a synthetic data and real data [19,65-67]. Generative Adversarial Networks have found popular application in cybersecurity to generate synthetic samples of malware, phishing emails, network traffic, and attack scenarios to train and test detection systems. Such models can be especially helpful since data on cybersecurity is not always balanced, complete, or can sometimes be scarce since of privacy issues. GANs have the potential to enhance the robustness of models by training them on more possible attack scenarios. Yet, they lead to additional dangers as well since attackers may employ these models to design more advanced phishing attacks, malicious software versions, and adversarial examples.

Large Language Models

Large Language Models are quickly becoming one of the most powerful AI models in cybersecurity since they have the ability to work with massive amounts of unstructured cybersecurity data. Applications of these models are becoming popular as cyber threat intelligence, vulnerability analysis, phishing detection, malware analysis, automated reporting, and digital forensics. Big Data MLs have the capability to interpret threat findings, vulnerability announcements, and dark web forums, logs in the system, and spam letters to detect new cyber threats and create actionable content. The more recent advances in 2026 indicate that frontier Large Language Models are powerful enough to discover and suggest patches to code vulnerabilities, and even create exploit code, which has sparked serious issues of abuse and regulation. To safeguard the implementation of Large Language Models in the context of cybersecurity, organizations are scouting safe deployment sources, Trusty AI frameworks, and human-in-the-loop use cases to integrate Large Language Models into the security routine safely.

Explainable Artificial Intelligence Models

Explainable Artificial Intelligence is getting more significant as most of the Machine Learning and Deep Learning models applied to cybersecurity are black-boxes. Before security analysts can act, they may be called upon to know why a model deemed an activity as malicious [68-70]. Local Interpretable Model-Agnostic Explanations, Shapley Additive Explanations, saliency maps, feature attribution, and interpretable rule extraction are examples of explainable Artificial Intelligence models that shedding light on model decisions. They are particularly useful in the field of malware detection, cyber risk assessment, insider threat detection, digital forensics, and human-centered cybersecurity due to the fact that they assist in enhancing trust, accountability, and compliance with regulations. This trend toward greater use of Explainable AI is a response to the larger trend ofTrustworthy AI and responsible governance of cybersecurity.

Hybrid and Neuro-Symbolic Models

One of the most promising future directions of cybersecurity is Hybrid and Neuro-Symbolic models since they use the advantage of several approaches to Artificial Intelligence. Machine Learning, Deep Learning, Natural Language Processing, Reinforcement Learning, Graph Neural Networks, explainable AI may all be combined in a cybersecurity framework as a hybrid. The Neuro-Symbolic models unite neural networks with symbolic reasoning and expert rules so that, not only, they identify attack patterns, but also provide explanations as why the pattern is malicious. Such models particularly find applications in cyber threat intelligence, digital forensics, attack path analysis, and automated incident response purposes since they are more interpretable, able to push limits and more robust than single models would be. To address the modern cyber threats, intelligent cybersecurity systems are probably to rely on hybrid systems that could address the emerging needs of handling the cyber threats, enhancing decision-making, and aiding in the protection of secure and autonomous cyber defense on a large scale.

3.5 Artificial intelligence applications

AI Applications in Intrusion Detection Systems

One of the most significant fields of cybersecurity has become the artificial intelligence use in Intrusion Detection Systems since often the signature-based use of these systems is incapable of detecting zero-day attacks, advanced persistent threat, and polymorphic malware. Network traffic analysis, suspicion pattern detection, and unauthorized access detection are becoming more popular and can be performed using the help of Machine Learning and Deep Learning models [71-73]. Decision tree, random forest and support vector machine are all supervised learning techniques that are typically employed to classify malicious and non-malicious traffic, whereas unsupervised techniques like clustering and anomaly detection are employed to comingle with threats that are never seen before. The latest cybersecurity contexts have been pushing towards more hybrid forms of AI-based Intrusion Detection Systems that integrate behavioral analytics, predictive analytics and cyber threat intelligence to enhance detection accuracy and minimize false positive. Such systems have particularly proven useful in enterprise networks, cloud protection resources, IoT protection systems, and edge computer protection systems since they have the ability to constantly readjust to emerging attack tactics and allow ongoing tracking of threats. AI-based intrusion detection has become a key element of the current cyber defense as it allows to be proactively monitored and provide quick response to more advanced cyberattacks. The use of AI-based intrusion detection systems has increasingly been empirically studied using datasets like CIC-IDS2018, NSL-KDD and Edge-IIoTset, as a measure of enhanced accuracy, latency and energy efficiency in practice.

AI Applications in Malware Detection and Ransomware Detection

Malware detection tools and ransomware detection tools using Artificial Intelligence have greatly enhanced the capability of cybersecurity systems to detect malicious software before it can inflict lasting harmful impact. Conventional antivirus systems tend to rely on malware signatures that are known and fail to detect polymorphic malware, fileless malware and zero-day ransomware attacks. Nowadays, machine learning, deep learning, and neural network models are commonly used to analyze malware binaries, system calls, application behavior, and network traffic to detect suspicious activities. Convolutional Neural networks have shown the capability to convert malware binaries to an image format to be classified, whereas Recurrent Neural networks and Long Short-Term Memory networks can process series of behavior associated with ransomware execution. GANs are also being applied in developing synthetic malware samples by which to train detection systems and enhance immunity to novel threats. The analysis of malware using AI has also become more efficient as, in real time, such models are capable of determining malicious actions, focusing not on fixed signatures alone. Recent studies also indicate that machine learning models of low weight that integrates heuristics analysis and third-party threat intelligence can have high accuracy in detection with lesser computational expenses and hence can be practically utilized in the real-world.

AI Applications in Phishing Detection and Social Engineering Prevention

The use of Artificial Intelligence in anti-phishing and anti-social engineering has become more prevalent since phishing is among the top attack strategies employed by cyber-criminals. Machine Learning, Natural Language Processing, and Large Language Models are currently common to understand the email content, domain names, URLs, web site structures, and user activities and determine that they were targeted by phished attackers [50,74-76]. The use of AI can identify the use of suspicious language patterns, spoofed email addresses, malicious attachments, or spoofed login pages more quickly and confidently than manual inspection. Recent development in Generative AI has posed new problems since now infiltrators are able to construct extremely personalized phishing messages and deep fake voice calls as well as believable social engineering material on a large scale. It is reported that Generative AI has shortened significantly the time interval it takes to initiate scams regarding phishing, and attackers can develop highly personalized suspicious schemes in a matter of minutes, instead of hours. Simultaneously, with advancements in AI, cybersecurity agencies are implementing machine-learned phishing identification systems, behavior-sensing applications, and adaptive authentication systems to overcome these attacks. With the increasingly advanced phishing technique, Artificial Intelligence would remain to be central in detecting suspicious messages and safeguarding users against manipulation and stealing credentials.

AI Applications in Cyber Threat Intelligence

Another application of Artificial Intelligence has become one of the most crucial ones; the main application of AI in the modern organization should be the Cyber Threat Intelligence since the new threats have to be detected before they can disrupt the functioning of the organizations. Cyber threat intelligence systems that are driven by AI have the ability to gather, process, and analyze big data sets in threat feeds, dark web forums, weakness reports and malware repositories as well as incident logs. The use of Natural Language Processing, Graph Neural Networks, and Large Language Models is in the growth, aiming to draw meaningful insights out of the cyber threat intelligence data and delineate the connections between hate agents, attack groups, malware families, and vulnerabilities. The technologies facilitate active hunting of threats, predicting attacks, and ranking risks as they detect the concealed attack patterns and possible future vulnerabilities within the digital ecosystems. Recent reports suggest that predictive threat intelligence and hybrid AI models are far more effective at enhancing resilience within organizations by enhancing the ability to identify advanced cyber threats in advance and responding more effectively to these threats. This increase in usage of Generative AI and Large Language Models is also evolving cyber threat intelligence, fully automated report on the intelligence of security threats, summarization of security alerts, and contextual advice to the security teams.

AI Applications in Security Information and Event Management and SOAR

The use of Artificial Intelligence in Security Information and Event Management and Security Orchestration Automation and Response systems has also become necessary given that organizations produce large amounts of security logs and alerts that are challenging to be handled manually. SIEM solutions employ both Machine Learning and Deep Learning to examine log files, correlate security events, rank alerts, and detect suspicious trends in networks, endpoints, and in the cloud [77-79]. SOAR systems take such capabilities a step further to automate response measures like isolating devices impacted, blocking malicious IP addresses, shutting off user accounts and initiating incident investigations. The use of AI-based SIEM and SOAR tools can decrease the workload of security engineers by sifting through false positives and prioritizing alerts with the highest potential threat and decreasing incident response time. The use of SIEM and SOAR platforms in developing AI-driven solutions with generative AI and Large Language Models is becoming commonplace to automate threat summaries, create advice, and aid in decision-making. The acceleration of the autonomous security operations implies that autonomous security operation systems will rely more on AI-based SIEM, SOAR, and Extended Detection and Response systems in the future to defend against complex cyber threats in more effective ways.

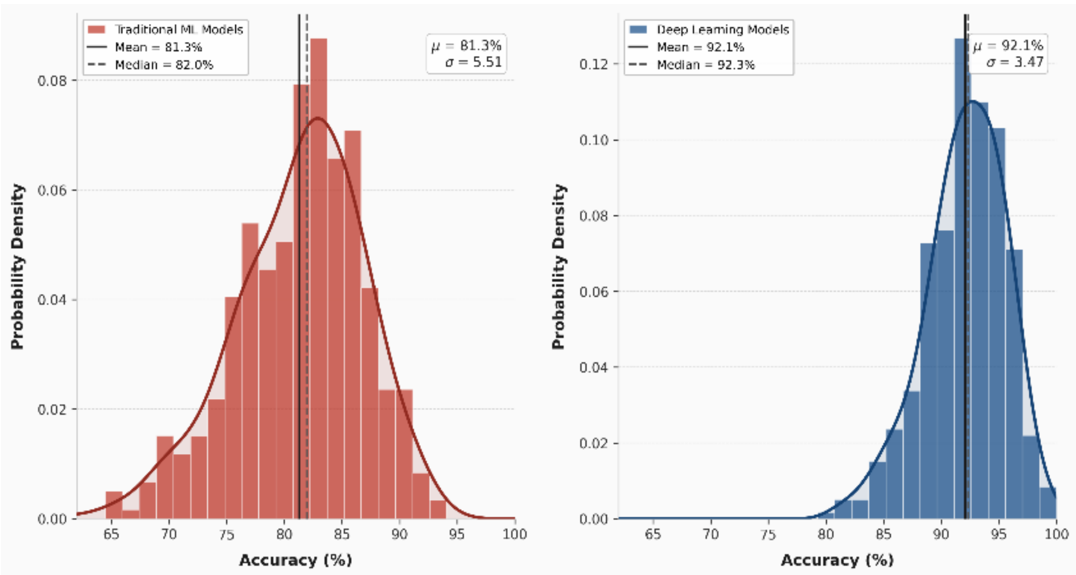

Fig. 6 Accuracy Distribution of Traditional ML vs. Deep Learning Models in Cybersecurity Studies

Fig. 6 represents side-by-side histogram with superimposed Kernel Density Estimation (KDE) curves characterizes the full empirical distribution of accuracy scores reported across the reviewed literature for two major AI paradigm families, enabling a direct probabilistic comparison that goes beyond the point estimates typically reported in survey tables. The Traditional ML panel exhibits a bimodal distribution with a dominant peak near 83.5% and a secondary mode around 77%, reflecting the heterogeneous performance of Support Vector Machines, Random Forests, and XGBoost across diverse cybersecurity task types, network environments, and dataset compositions encountered in the literature. The Deep Learning panel, by contrast, displays a sharply unimodal and positively skewed distribution concentrated above 90%, with a notably smaller standard deviation, indicating not only higher average performance but also greater consistency and transferability across experimental contexts. The inset annotation boxes report the mean and standard deviation for each distribution, supporting rapid quantitative interpretation. Together, the two panels offer compelling distributional evidence that the transition from classical to deep learning approaches represents a statistically significant and practically meaningful advancement in cybersecurity AI, with the reduced variance of deep learning outcomes carrying particular importance for risk-sensitive deployment decisions in critical infrastructure protection.

AI Applications in Endpoint Detection and Response

Powered by Artificial Intelligence, Endpoint Detection and Response systems are becoming increasingly popular with endpoints including laptops, mobile devices, servers, and cloud workloads being monitored against suspicious activities. AI-based Endpoint Detection and Response systems use endpoint telemetry, process execution, registries modification, login actions, and file use to find malware, ransomware, phishing attacks, and insider threats [80-82]. The significance of these systems is critical since one of the most frequently used types of cyberattacks is launched at the endpoints. Deep Learning and behavioral analytics will be able to detect malicious behavior despite the attackers employing obfuscation methods, encryption, or fileless malware. Recent trends show that AI-based endpoint protection is increasingly self-sufficient, and that systems can isolate infected devices, block malicious processes and survive compromised systems without human intervention. The first AIs projects that are concerned with autonomous malware detection are showing that endpoint protection systems can analyze suspicious files and decide on their security level.

AI Applications in Identity Security and Adaptive Authentication

The applications of Artificial Intelligence have become more significant due to Identity Security and Adaptive Authentication since stolen credential, account takeover, and insider threats remain the significant threats to organizations. Identity security is an AI-based product that examines the patterns of login, computing devices, geolocation information, typing rate, and biometrics indicators to define a legit user or a suspicious individual. The adaptive authentication involves behavioral analytics and risk scoring that can dynamically change access requirements based on contextual information. As an illustration, when a user logs in an odd place or device, he or she might be requested to undergo extra identification measures. Facial recognition, fingerprint analysis, voice recognition and identity verification systems are other systems that apply Artificial Intelligence to enhance access control and curb fraud. Such technologies play a special role in the Zero Trust Security models since they are constantly checking the identity of the user, as opposed to trusting him after being initially authenticated. In response to the growing number of attempts at cybercrime by cybercriminals through the aid of stolen credentials and AI-generated impersonation attacks, adaptive authentication and identity security will be elevated as a crucial application in cyber defense.

AI Applications in Cloud Security and IoT Security

Applications of Artificial Intelligence in cloud security and IoT security are growing by the day due to the growing dependence of organisations on cloud services, connected devices and distributed infrastructures. Cloud environments are sources of enormous data that must be constantly monitored, detected and controlled [20,83-86]. AI-based cloud security systems rely on the principles of Machine Learning to detect abnormal activity, unauthorized access, and rank vulnerabilities on virtual machines, cloud applications, storage systems. Artificial Intelligence is able to track connected devices and intercept communication trends in real time, detecting possible malicious activity in IoT security. Particularly lightweight Machine Learning models and Edge AI can be applied to IoT settings since it can be used on resource-limited devices with low latency. Another way that is gaining importance in cloud and IoT security involves Federated Learning and Privacy-Preserving Machine Learning, as these two methods allow exposure of sensitive data when collaboratively training a model. The AI-guided cloud security and IoT security will gain more importance to safeguard highly distributed digital ecosystems as organizations need the implementation of 5G, 6G, or edge computing technologies.

AI Applications in Fraud Detection and Financial Cybersecurity

Financial institutions are reporting the increasing number of phishing scams, identity theft, payment and account takeover attacks which makes the application of Artificial Intelligence in fraud detection and financial cybersecurity an increasingly important matter. Machine Learning and real-time behavioral analytics are a popular method of tracking financial transactions, spotting suspicious behavior of an account, and detecting suspicious patterns. Utilizing system fraud detection can identify potentially fraudulent transactions, device usage, the history of logins, geolocation data, and customer actions. Recent news state that Generative AI has propelled financial fraud to a new level by helping cybercriminals generate convincing phishing emails, deepfakes videos, voice clone attacks and impersonation scams. To enhance detection and prevention, financial institutions are countering by innovating AI-based monitoring systems, cross-border fraud scoring systems, as well as cross-border intelligence sharing systems. The rising pace of AI-fueled fraud evidences the fact that the future of financial cybersecurity should turn to more predictive analytics, live tracking, and joint intelligence to secure online transactions and keep the confidence in digital finance.

AI Applications in Explainable Cybersecurity and Governance

Explainable Artificial Intelligence and cybersecurity governance have gained popularity due to the rising risks since most of the systems based on Machine Learning and Deep Learning are provided as black boxes, which do not give much understanding of how decisions are made. The high-risk cybersecurity environment requires analysts to be aware of why a model would have identified an activity as malicious to act accordingly [87-89]. The methods of explainable Artificial Intelligence, such as feature attribution, saliency maps, Local Interpretable Model-Agnostic Explanations, and Shapley Additive Explanations can be used to enhance the trust, transparency, and accountability in AI-assisted cybersecurity systems. Malware detection, insider threat detection, digital forensics, cyber risk assessment, and regulatory compliance are specific areas that benefit from explainability since these applications are associated with making critical decisions that can impact operations within an organization. AI Ethics in Cybersecurity, Trustworthy AI and Human-Centred Cybersecurity are also essential due to the fact that organizations have to make sure that AI processes are equitable, secure as well as conforming to the rules. Next-generation cybersecurity governance systems will likely focus more on transparency, elucidativeness, and accountable use of AI.

AI Applications in Deepfake Detection and Synthetic Media Security

Detecting deepfakes has become a key application of Artificial Intelligence due to the growing usage of synthetic media, voice cloning, and altered videos by cybercriminals in attacks of fraud, misinformation, and impersonation. Deepfake detection methods powered by AI scan facial expressions, spoken words, lips, signatures, and video anomalies to calculate whether information has been created by an artificial method. Such systems are particularly critical in financial cybersecurity, identity authentication, journalism, political communications, and corporate security since deepfakes may be used to defraud employees, control the masses, and even circumvent authentication systems. New cybersecurity platforms are, more and more, adding deepfake detection technology to identity security systems and social media monitoring tools to detect malicious content in the moment. The fact that specialised deepfake detection websites have appeared mirrors the ever-increasing demand on synthetic media defense as the development of Generative AI progresses.

AI Applications in Autonomous Cyber Defense and Agentic AI

One of the most promising uses of Artificial Intelligence in cybersecurity is autonomous cyber defense and agentic AI since such systems are able to decide, work towards objectives and react to intruders with little human supervision. Agents AIs are consumed in more vulnerability scans, attack surface management, threat hunting, automated incident response, and continuous exposure management [3,90-92]. Multi-Agent Systems enable multiple AI agents to cooperate to protect cloud infrastructures, IoT environments, and enterprise networks through the sharing of intelligence and distributing tasks. Research has recently indicated that the trend is moving towards organizations moving away from the traditional Generative AI towards more autonomous systems of AI that can both set goals, monitor networks and react to threats in real time. Nevertheless, malicious agents are also starting to leverage agentic AI to automate reconnaissance and phishing or malware creation, and evolving attack tactics. Such two-sided cooperation of autonomous AI implies that a firm management, Trustworthy AI, and

Human-in-the-Loop strategies are necessary to guarantee the safety of autonomous cyber defense system and its compliance with company goals.

4. Discussion

According to the results of this literature review, Artificial Intelligence, Machine Learning, and Deep Learning have become the main perches of the new approach to cybersecurity as it enables the enhancement of real time threat detection, predictive analytics, prediction of cyberattacks, and automated responses. Conventional tools of cybersecurity based on the use of inflexible rules, manual inspection, and signature-driven detection are becoming less effective in countering the changing cyber threats of ransomware, phishing, insider attacks, Botnets, advanced persistent threats, and zero day attacks. Machine Learning (ML) and Deep Learning (DL)-based Intelligent Cybersecurity Systems have the potential to continuously analyze network traffic, system logs, endpoint telemetry, and cloud workloads (and user behavior) to detect malicious behavior more precisely and quickly than traditional systems. New trends also suggest that the field of cybersecurity is also transitioning to a new phase through AI-centric Security Operations Centers, agentic AI, autonomous security systems, and enduring exposure management. Organizations are moving towards deploying Security Information and Event Management systems, Extended Detection and Response systems, and Security Orchestration Automation and Response technology with built-in Artificial Intelligence, to mitigate the problem of alert fatigue, faster incident response, and proactive cyber defensive measures. The ongoing focus on Zero Trust Security, identity security, adaptive authentication, and continuous risk scoring further proves that future cybersecurity policy will be more and more based on the dynamic and AI-enhanced access control and behavioral analytics.

Table 1. Comparative Analysis of Artificial Intelligence Techniques, Methods, Technologies, and Models in Cybersecurity

Sr. No.	Application	Techniques / Methods / Technologies / Models	Key Function
1	Intrusion Detection Systems	Random Forest, Support Vector Machine, Decision Tree	Detect unauthorized network access
2	Malware Detection	Convolutional Neural Networks, Deep Neural Networks	Identify malicious binaries and code
3	Ransomware Detection	Recurrent Neural Networks, Long Short-Term Memory	Detect sequential ransomware behavior
4	Phishing Detection	Natural Language Processing, Large Language Models	Analyze malicious emails and URLs
5	Cyber Threat Intelligence	Graph Neural Networks, Natural Language Processing	Identify relationships between threats
6	Insider Threat Detection	Behavioral Analytics, Autoencoders	Detect suspicious user activities
7	Endpoint Detection and Response	Deep Learning, Anomaly Detection	Monitor endpoint behavior
8	Security Information and Event Management	Machine Learning, Big Data Analytics	Correlate logs and prioritize alerts
9	Security Orchestration Automation and Response	Reinforcement Learning, Automated Incident Response	Automate security workflows
10	Identity Security	Adaptive Authentication, Behavioral Biometrics	Verify user identity dynamically
11	Zero Trust Security	Risk Scoring, Intelligent Access Control	Continuously validate user access
12	Cloud Security	Federated Learning, Privacy-Preserving Machine Learning	Protect cloud workloads
13	IoT Security	Edge AI, Lightweight Deep Learning	Secure connected devices
14	Blockchain Security	Secure Federated Learning, Cryptographic Analytics	Improve tamper resistance
15	Fraud Detection	Graph Neural Networks, Predictive Analytics	Detect suspicious transactions
16	Digital Forensics	Natural Language Processing, Generative AI	Analyze incident reports and logs
17	Vulnerability Assessment	Large Language Models, Generative AI	Identify and prioritize vulnerabilities
18	Threat Hunting	Cyber Threat Intelligence, Reinforcement Learning	Support proactive threat discovery
19	Anomaly Detection	Autoencoders, Unsupervised Learning	Detect unknown attack patterns
20	Cyberattack Prediction	Long Short-Term Memory, Predictive Analytics	Forecast future attack behavior
21	Deepfake Detection	Convolutional Neural Networks, Pattern Recognition	Detect synthetic media attacks

22	Automated Patch Management	Reinforcement Learning, Agentic AI	Prioritize and deploy patches
23	Continuous Exposure Management	Agentic AI, Autonomous Security Systems	Monitor attack surfaces continuously
24	Adaptive Authentication	Machine Learning, Identity Security	Adjust access requirements dynamically
25	Post-Quantum Cryptography	Quantum-Safe Security, AI Optimization	Prepare for quantum threats

Recent advances in Generative AI and Large Language Models have posed new opportunities and threats to cybersecurity. On the one hand, Large Language Models find more and more applications in cyber threat intelligence, malware analysis, vulnerability assessment, phishing detection, digital forensics, automated reporting, and the automation of the Security Operations Center [8,12,93-95]. Conversely, Generative AI raised serious issues concerning adversarial machine learning, prompt injection, deepfakes, malware creation, automated reconnaissance and social engineering. Of particular interest is the formation of agentic AI and multi agency systems since these technologies can autonomously plan, reason, and perform complex cybersecurity operations with reduced human oversight. Preliminary indications point to the shift of agentic AI beyond the assistant model to complete an autonomous pipeline with continuous monitoring, automated incident response, vulnerability discovery and attack path analysis. Nonetheless, these technologies also increase the size of the cyberattack surface since attackers can take advantage of memory poisoning, prompt injection, manipulation of runtime tools, and inter-agent communication vulnerabilities. This will mean that future cybersecurity systems will demand more robust programs of governance, Human-in-the-loop AI, Trustworthy AI, Explainable Artificial Intelligence, and Zero-Trust at Run Time Architectures in order to make sure that autonomous AI agents are safe, transparent, and responsible.

The other significant conclusion of this review is that the various Artificial Intelligence methods exhibit different levels of strength on different cybersecurity areas. Random Forest, Support Vector Machine, Logistic Regression, and Decision Trees Supervised Machine Learning models, in particular, can be effectively used in malware detection, phishing detection, spam filtering, and intrusion detection systems since they can very well categorize familiar attack patterns. Deep Learning models, including Convolutional Neural Networks, Recurrent Neural Networks, Long Short-Term Memory networks, and Autoencoders, are better applied to intricate cybersecurity tasks, when handling unstructured data, sequence of occurrences, and detecting anomalies. GNNs have lately proved to be of great use in cyber threat intelligence, attack surface management, privilege escalation detection, fraud detection, and insider threat detection due to their ability to model relationships based on users, devices, domains, and network nodes. Reward Learning and Deep Reinforcement Learning also become attention-grabbing in the sense that they can be used to aid the adaptive authentication, automated response to incidents, intelligent access control, and autonomous cyber defense. There are indications, based on these developments, that the next generation of cybersecurity frameworks will depend on more hybrid frameworks with multiple methods of Artificial Intelligence to enhance performance, resilience and interpretability.

The review also outlines a number of long-standing challenges which still restrict the efficiency of Artificial Intelligence in cybersecurity. Adversarial machine learning is one of the most critical issues as attackers alter training data, generate adversarial inputs, or find vulnerabilities in AI models to avoid detection [96,97]. Huge Language models and Generative AI systems are especially susceptible to prompt injection, hallucination, model inversion, and leakage of data attacks. The other significant issue is that Deep Learning systems are non-explainable since most models are black boxes that give minimal information on why specific decisions are taken. Such a non-transparent space poses a challenge to cybersecurity analysts who have to substantiate their choices and act. Moreover, the lack of privacy, data asymmetry, low data quality, computational efforts, regulatory limitations, and lack of generaliseability in AI-based cybersecurity systems still impede AI uptake. Recent events also provide evidence that organizations are turning more to cohesive governance, risk and compliance solutions to facilitate ease in cybersecurity governance, to narrow compliance pressure, and to enhance organizational resilience.

Table 2. Major Challenges, Opportunities, and Future Directions of Artificial Intelligence in Cybersecurity

Sr. No.	Challenge	Opportunity	Future Direction
1	Adversarial Machine Learning	Robust model training	Adversarial resilience frameworks
2	Prompt Injection	Secure prompt engineering	Zero-Trust Runtime Architecture
3	Data Privacy Concerns	Federated Learning	Privacy-Preserving Machine Learning
4	Lack of Explainability	Explainable Artificial Intelligence	Human-Centered Cybersecurity
5	Model Hallucination	Trustworthy AI	Safer Large Language Models
6	Data Imbalance	Synthetic data generation	Generative Adversarial Networks
7	High Computational Cost	Lightweight AI models	Edge AI deployment
8	False Positives	Behavioral Analytics	Hybrid AI models
9	False Negatives	Multi-layered detection	Ensemble learning
10	Poor Data Quality	Data cleaning pipelines	Automated data governance
11	Limited Scalability	Cloud-native AI systems	Distributed cybersecurity frameworks
12	Regulatory Compliance	Unified governance platforms	Automated compliance systems
13	Identity Theft	Adaptive Authentication	Continuous identity verification
14	Deepfake Attacks	Synthetic media detection	Deepfake-resistant systems
15	Malware Evolution	Real-time threat monitoring	Autonomous malware analysis
16	Phishing Automation	Natural Language Processing	AI-based phishing prevention
17	IoT Vulnerabilities	Lightweight anomaly detection	Secure IoT ecosystems
18	Quantum Threats	Post-Quantum Cryptography	Quantum-Safe Security
19	Multi-Agent Risks	Agentic AI governance	Safe autonomous systems
20	Runtime Supply Chain Attacks	Zero-Trust Runtime Models	Secure agent ecosystems
21	Insider Threats	Behavioral Analytics	Context-aware monitoring
22	Cloud Misconfigurations	Cloud Security Automation	AI-driven cloud governance
23	Skill Gaps	AI-enabled SOC automation	Workforce augmentation
24	Tool Fragmentation	Platform consolidation	Unified security operations
25	Lack of Accountability	Human-in-the-Loop AI	Ethical AI governance

In general, the literature shows that convergence of Artificial Intelligence, Machine Learning, Deep Learning, Generative AI, agentic AI, and autonomous cyber defense systems will define the future of cybersecurity. Organizations are shifting to AI-assisted Security Operations Centers, reconfigurability, cyber resilience models, post-quantum cryptography, and dynamic exposure to deal with more and more advanced threats. The quick development of agentic AI and multi-agent cybersecurity systems demonstrates that cyber security is going to be more autonomous, proactive, and scalable in the future. Simultaneously, these innovations needs powerful cybersecurity regulation, Explainable Artificial Intelligence, ethics, and Zero Trust structures to have safe implementation. Future directions ought to establish hybrid models, Explainable Graph Neural Networks, Secure Federated Learning, Human-in-the-Loop AI, and robust autonomous security systems capable of surviving the changing cyber threats without compromising transparency, privacy, and trust.

5. Conclusions

This is a detailed literature review exercise that has indicated the increasing role of Artificial Intelligence, Machine Learning, and Deep Learning in enhancing current cybersecurity systems to address an ever-evolving and even more challenging cyber threat. The analysis provided on the PRISMA basis proves that smart systems of cybersecurity have become necessary to identify, enhance, and react to sophisticated patterns of attack such as ransomware, phishing, malware propagation, insider threats, botnet attacks, and advanced persistent threats. The established security measures, which are founded on rules and regulations, cannot be applied to deeply interconnected digital environments where cybercriminals repeatedly take advantage of vulnerabilities in cloud systems, IoT networks, and edge computing applications, as well as enterprise unities.

The analysis results indicate that the performance of intrusion detection systems, malware detection systems, cyber threat intelligence platforms, endpoint detection and response tools, and Security Information and Event Management solutions has significantly enhanced with the help of Machine Learning and Deep Learning models. Methods like Convolutional Neural Networks, Recurrent Neural Networks, Graph Neural Networks, reinforcement learning, and hybrid deep learning architectures have facilitated more accurate anomaly recognition, behavioral analytics, predictive analytics, and live threat monitoring. These machine-learning models are able to handle large volumes of cybersecurity information, detect concealed attack patterns, and proactive cyber defense measures. Moreover, the rising adoption of Explainable Artificial Intelligence, federated learning, privacy-sensitive machine learning, and trustworthy AI have provided additional opportunities to enhance the transparency of the model, user trust, data privacy, and regulatory compliance.

Irrespective of these developments, the review also reveals that there are some crucial challenges that still impede the widespread implementation of AI-powered cybersecurity solutions. The validity of Adversarial machine learning attacks, quality of derailed datasets, class bias, overfitting of models, lack of interpretability, high computational expenses and low generalizability are still of concern. The fast advancement of generative AI and large language models has further presented a twofold threat, because these technologies can both enhance cyber defense as well as allow cybercriminals to automatize phishing efforts, malware development, and social engineering attacks. Moreover, concerns surrounding the governance of data, ethical artificial intelligence, the bias in algorithms, secure computing, and human-focused cybersecurity should be tackled to make the implementation of intelligent security systems as safe and responsible as possible.

The study of autonomous security systems via combination of real-time decision making, adaptive learning and explainable reasoning should be pursued in future studies. One should also focus more on zero trust security architecture, cyber resiliency, attack surface control, blockchain security, internet of things security, and cloud-native security measures. New methods like transfer learning, graph-based cyber defense, cybersecurity digital twins, collaborative threat intelligence, and multi-agent reinforcement learning have good potential in their future exploration. In general, the intersection of Artificial Intelligence, Machine Learning, and Deep Learning with cybersecurity is likely to transform the future of cyber defense, allowing to create scalable, proactive, transparent, and resilient security ecosystems that can respond to cyber threats of the next generation.

Conflict of interest

The authors declare no conflicts of interest.

References

[1] Korzynski P, Mazurek G, Altmann A, Ejdys J, Kazlauskaite R, Paliszkiewicz J, Wach K, Ziemba E. Generative artificial intelligence as a new context for management theories: analysis of ChatGPT. Central European Management Journal. 2023 Mar 28;31(1):3-13. https://doi.org/10.1108/CEMJ-02-2023-0091

[2] Zha D, Bhat ZP, Lai KH, Yang F, Jiang Z, Zhong S, Hu X. Data-centric artificial intelligence: A survey. ACM Computing Surveys. 2025 Jan 24;57(5):1-42. https://doi.org/10.1145/3711118

[3] Papagiannidis E, Mikalef P, Conboy K. Responsible artificial intelligence governance: A review and research framework. The Journal of Strategic Information Systems. 2025 Jun 1;34(2):101885. https://doi.org/10.1016/j.jsis.2024.101885

[4] Yim IH, Su J. Artificial intelligence (AI) learning tools in K-12 education: A scoping review. Journal of Computers in Education. 2025 Mar;12(1):93-131. https://doi.org/10.1007/s40692-023-00304-9

[5] Gursoy D, Cai R. Artificial intelligence: an overview of research trends and future directions. International Journal of Contemporary Hospitality Management. 2025 Jan 2;37(1):1-7. https://doi.org/10.1108/IJCHM-03-2024-0322

[6] Sengar SS, Hasan AB, Kumar S, Carroll F. Generative artificial intelligence: a systematic review and applications. Multimedia Tools and Applications. 2025 Jun;84(21):23661-700. https://doi.org/10.1007/s11042-024-20016-1

[7] Ferrara E. Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies. Sci. 2024 Mar;6(1):3. https://doi.org/10.3390/sci6010003

[8] Han R, Acosta JN, Shakeri Z, Ioannidis JP, Topol EJ, Rajpurkar P. Randomised controlled trials evaluating artificial intelligence in clinical practice: a scoping review. The lancet digital health. 2024 May 1;6(5):e367-73. https://doi.org/10.1016/S2589-7500(24)00047-5

[9] Swiecki Z, Khosravi H, Chen G, Martinez-Maldonado R, Lodge JM, Milligan S, Selwyn N, Gašević D. Assessment in the age of artificial intelligence. Computers and Education: Artificial Intelligence. 2022 Jan 1;3:100075. https://doi.org/10.1016/j.caeai.2022.100075

[10] Khalid N, Qayyum A, Bilal M, Al-Fuqaha A, Qadir J. Privacy-preserving artificial intelligence in healthcare: Techniques and applications. Computers in Biology and Medicine. 2023 May 1;158:106848. https://doi.org/10.1016/j.compbiomed.2023.106848

[11] Resnik DB, Hosseini M. The ethics of using artificial intelligence in scientific research: new guidance needed for a new tool. AI and Ethics. 2025 Apr;5(2):1499-521. https://doi.org/10.1007/s43681-024-00493-8

[12] Kraemer MU, Tsui JL, Chang SY, Lytras S, Khurana MP, Vanderslott S, Bajaj S, Scheidwasser N, Curran-Sebastian JL, Semenova E, Zhang M. Artificial intelligence for modelling infectious disease epidemics. Nature. 2025 Feb 20;638(8051):623-35. https://doi.org/10.1038/s41586-024-08564-w

[13] Demaidi MN. Artificial intelligence national strategy in a developing country. Ai & Society. 2025 Feb;40(2):423-35. https://doi.org/10.1007/s00146-023-01779-x

[14] Pereira V, Hadjielias E, Christofi M, Vrontis D. A systematic literature review on the impact of artificial intelligence on workplace outcomes: A multi-process perspective. Human Resource Management Review. 2023 Mar 1;33(1):100857. https://doi.org/10.1016/j.hrmr.2021.100857

[15] Cowls J, Tsamados A, Taddeo M, Floridi L. The AI gambit: leveraging artificial intelligence to combat climate change-opportunities, challenges, and recommendations. Ai & Society. 2023 Feb;38(1):283-307. https://doi.org/10.1007/s00146-021-01294-x

[16] Schwendicke FA, Samek W, Krois J. Artificial intelligence in dentistry: chances and challenges. Journal of dental research. 2020 Jul;99(7):769-74. https://doi.org/10.1177/0022034520915714

[17] Verganti R, Vendraminelli L, Iansiti M. Innovation and design in the age of artificial intelligence. Journal of product innovation management. 2020 May;37(3):212-27. https://doi.org/10.1111/jpim.12523

[18] Novelli C, Taddeo M, Floridi L. Accountability in artificial intelligence: What it is and how it works. Ai & Society. 2024 Aug;39(4):1871-82. https://doi.org/10.1007/s00146-023-01635-y

[19] Rashidi HH, Pantanowitz J, Hanna MG, Tafti AP, Sanghani P, Buchinsky A, Fennell B, Deebajah M, Wheeler S, Pearce T, Abukhiran I. Introduction to artificial intelligence and machine learning in pathology and medicine: generative and nongenerative artificial intelligence basics. Modern Pathology. 2025 Apr 1;38(4):100688. https://doi.org/10.1016/j.modpat.2024.100688

[20] Waisberg E, Ong J, Kamran SA, Masalkhi M, Paladugu P, Zaman N, Lee AG, Tavakkoli A. Generative artificial intelligence in ophthalmology. Survey of ophthalmology. 2025 Jan 1;70(1):1-1. https://doi.org/10.1016/j.survophthal.2024.04.009

[21] Wang H, Fu T, Du Y, Gao W, Huang K, Liu Z, Chandak P, Liu S, Van Katwyk P, Deac A, Anandkumar A. Scientific discovery in the age of artificial intelligence. Nature. 2023 Aug 3;620(7972):47-60. https://doi.org/10.1038/s41586-023-06221-2

[22] Banh L, Strobel G. Generative artificial intelligence. Electronic Markets. 2023 Dec;33(1):63. https://doi.org/10.1007/s12525-023-00680-1

[23] Benbya H, Davenport TH, Pachidi S. Artificial intelligence in organizations: Current state and future opportunities. MIS Quarterly Executive. 2020 Dec 3;19(4). https://doi.org/10.2139/ssrn.3741983

[24] Kaur D, Uslu S, Rittichier KJ, Durresi A. Trustworthy artificial intelligence: a review. ACM computing surveys (CSUR). 2022 Jan 18;55(2):1-38. https://doi.org/10.1145/3491209

[25] Meskó B, Görög M. A short guide for medical professionals in the era of artificial intelligence. NPJ digital medicine. 2020 Sep 24;3(1):126. https://doi.org/10.1038/s41746-020-00333-z

[26] Sanchez TW, Brenman M, Ye X. The ethical concerns of artificial intelligence in urban planning. Journal of the American Planning Association. 2025 Apr 3;91(2):294-307. https://doi.org/10.1080/01944363.2024.2355305

[27] Fountzilas E, Pearce T, Baysal MA, Chakraborty A, Tsimberidou AM. Convergence of evolving artificial intelligence and machine learning techniques in precision oncology. NPJ Digital Medicine. 2025 Jan 31;8(1):75. https://doi.org/10.1038/s41746-025-01471-y

[28] Nguyen-Duc A, Cabrero-Daniel B, Przybylek A, Arora C, Khanna D, Herda T, Rafiq U, Melegati J, Guerra E, Kemell KK, Saari M. Generative artificial intelligence for software engineering-A research agenda. Software: Practice and Experience. 2025 Nov;55(11):1806-43. https://doi.org/10.1002/spe.70005

[29] Hopgood AA. Intelligent systems for engineers and scientists: a practical guide to artificial intelligence. CRC press; 2021 Dec 9. https://doi.org/10.1201/9781003226277

[30] Matheny ME, Whicher D, Israni ST. Artificial intelligence in health care: a report from the National Academy of Medicine. Jama. 2020 Feb 11;323(6):509-10. https://doi.org/10.1001/jama.2019.21579

[31] Cai H, Ao Z, Tian C, Wu Z, Liu H, Tchieu J, Gu M, Mackie K, Guo F. Brain organoid reservoir computing for artificial intelligence. Nature Electronics. 2023 Dec;6(12):1032-9. https://doi.org/10.1038/s41928-023-01069-w

[32] Jackson I, Ivanov D, Dolgui A, Namdar J. Generative artificial intelligence in supply chain and operations management: a capability-based framework for analysis and implementation. International Journal of Production Research. 2024 Sep 1;62(17):6120-45. https://doi.org/10.1080/00207543.2024.2309309

[33] Bibri SE, Krogstie J, Kaboli A, Alahi A. Smarter eco-cities and their leading-edge artificial intelligence of things solutions for environmental sustainability: A comprehensive systematic review. Environmental Science and Ecotechnology. 2024 May 1;19:100330. https://doi.org/10.1016/j.ese.2023.100330

[34] Sarraju A, Bruemmer D, Van Iterson E, Cho L, Rodriguez F, Laffin L. Appropriateness of cardiovascular disease prevention recommendations obtained from a popular online chat-based artificial intelligence model. Jama. 2023 Mar 14;329(10):842-4. https://doi.org/10.1001/jama.2023.1044

[35] Belhadi A, Mani V, Kamble SS, Khan SA, Verma S. Artificial intelligence-driven innovation for enhancing supply chain resilience and performance under the effect of supply chain dynamism: an empirical investigation. Annals of operations research. 2024 Feb;333(2):627-52. https://doi.org/10.1007/s10479-021-03956-x

[36] Bhattamisra SK, Banerjee P, Gupta P, Mayuren J, Patra S, Candasamy M. Artificial intelligence in pharmaceutical and healthcare research. Big Data and Cognitive Computing. 2023 Jan 11;7(1):10. https://doi.org/10.3390/bdcc7010010

[37] Pallathadka H, Ramirez-Asis EH, Loli-Poma TP, Kaliyaperumal K, Ventayen RJ, Naved M. Applications of artificial intelligence in business management, e-commerce and finance. Materials Today: Proceedings. 2023 Jan 1;80:2610-3. https://doi.org/10.1016/j.matpr.2021.06.419

[38] McDonald N, Johri A, Ali A, Collier AH. Generative artificial intelligence in higher education: Evidence from an analysis of institutional policies and guidelines. Computers in Human Behavior: Artificial Humans. 2025 Mar 1;3:100121. https://doi.org/10.1016/j.chbah.2025.100121

[39] Emon MM, Khan T. The mediating role of attitude towards the technology in shaping artificial intelligence usage among professionals. Telematics and Informatics Reports. 2025 Mar 1;17:100188. https://doi.org/10.1016/j.teler.2025.100188

[40] Shao X, Cai B, Zou Z, Shao H, Yang C, Liu Y. Artificial intelligence enhanced fault prediction with industrial incomplete information. Mechanical Systems and Signal Processing. 2025 Feb 1;224:112063. https://doi.org/10.1016/j.ymssp.2024.112063

[41] Rožanec JM, Novalija I, Zajec P, Kenda K, Tavakoli Ghinani H, Suh S, Bian S, Veliou E, Papamartzivanos D, Giannetsos T, Menesidou SA. Human-centric artificial intelligence architecture for industry 5.0 applications. International journal of production research. 2023 Oct 18;61(20):6847-72. https://doi.org/10.1080/00207543.2022.2138611

[42] Chander B, John C, Warrier L, Gopalakrishnan K. Toward trustworthy artificial intelligence (TAI) in the context of explainability and robustness. ACM Computing Surveys. 2025 Feb 10;57(6):1-49. https://doi.org/10.1145/3675392

[43] Cooper G. Examining science education in ChatGPT: An exploratory study of generative artificial intelligence. Journal of science education and technology. 2023 Jun;32(3):444-52. https://doi.org/10.1007/s10956-023-10039-y

[44] Aldoseri A, Al-Khalifa KN, Hamouda AM. Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges. Applied Sciences. 2023 Jan;13(12):7082. https://doi.org/10.3390/app13127082

[45] George B, Wooden O. Managing the strategic transformation of higher education through artificial intelligence. Administrative Sciences. 2023 Aug 29;13(9):196. https://doi.org/10.3390/admsci13090196

[46] Wang B, Rau PL, Yuan T. Measuring user competence in using artificial intelligence: validity and reliability of artificial intelligence literacy scale. Behaviour & information technology. 2023 Jul 4;42(9):1324-37. https://doi.org/10.1080/0144929X.2022.2072768

[47] Morandini S, Fraboni F, De Angelis M, Puzzo G, Giusino D, Pietrantoni L. The impact of artificial intelligence on workers' skills: Upskilling and reskilling in organisations. Informing Science. 2023;26:39-68. https://doi.org/10.28945/5078

[48] Topaz M, Peltonen LM, Michalowski M, Stiglic G, Ronquillo C, Pruinelli L, Song J, O'connor S, Miyagawa S, Fukahori H. The ChatGPT effect: nursing education and generative artificial intelligence. Journal of Nursing Education. 2025 Jun 1;64(6):e40-3. https://doi.org/10.3928/01484834-20240126-01

[49] Noy S, Zhang W. Experimental evidence on the productivity effects of generative artificial intelligence. Science. 2023 Jul 14;381(6654):187-92. https://doi.org/10.1126/science.adh2586 Wang C, Wang H, Li Y, Dai J, Gu X, Yu T. Factors influencing university students' behavioral intention to use generative artificial intelligence: Integrating the theory of planned behavior and AI literacy. International Journal of Human-Computer Interaction. 2025 Jun 3;41(11):6649-71. https://doi.org/10.1080/10447318.2024.2383033

[50] Wang Q, Sun T, Li R. Does artificial intelligence promote green innovation? An assessment based on direct, indirect, spillover, and heterogeneity effects. Energy & Environment. 2025 Mar;36(2):1005-37. https://doi.org/10.1177/0958305X231220520

[51] Koçak B, Ponsiglione A, Stanzione A, Bluethgen C, Santinha J, Ugga L, Huisman M, Klontzas ME, Cannella R, Cuocolo R. Bias in artificial intelligence for medical imaging: fundamentals, detection, avoidance, mitigation, challenges, ethics, and prospects. Diagnostic and interventional radiology. 2025 Mar 3;31(2):75. https://doi.org/10.4274/dir.2024.242854

[52] Wachter RM, Brynjolfsson E. Will generative artificial intelligence deliver on its promise in health care?. Jama. 2024 Jan 2;331(1):65-9. https://doi.org/10.1001/jama.2023.25054

[53] Neumann O, Guirguis K, Steiner R. Exploring artificial intelligence adoption in public organizations: a comparative case study. Public Management Review. 2024 Jan 2;26(1):114-41. https://doi.org/10.1080/14719037.2022.2048685

[54] Vishwakarma LP, Singh RK, Mishra R, Kumari A. Application of artificial intelligence for resilient and sustainable healthcare system: Systematic literature review and future research directions. International Journal of Production Research. 2025 Jan 17;63(2):822-44. https://doi.org/10.1080/00207543.2023.2188101

[55] Fang B, Yu J, Chen Z, Osman AI, Farghali M, Ihara I, Hamza EH, Rooney DW, Yap PS. Artificial intelligence for waste management in smart cities: a review. Environmental Chemistry Letters. 2023 Aug;21(4):1959-89. https://doi.org/10.1007/s10311-023-01604-3

[56] Kaur R, Gabrijelčič D, Klobučar T. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion. 2023 Sep 1;97:101804. https://doi.org/10.1016/j.inffus.2023.101804

[57] Kamalov F, Santandreu Calonge D, Gurrib I. New era of artificial intelligence in education: Towards a sustainable multifaceted revolution. Sustainability. 2023 Aug 16;15(16):12451. https://doi.org/10.3390/su151612451

[58] Naik N, Hameed BM, Shetty DK, Swain D, Shah M, Paul R, Aggarwal K, Ibrahim S, Patil V, Smriti K, Shetty S. Legal and ethical consideration in artificial intelligence in healthcare: who takes responsibility?. Frontiers in surgery. 2022 Mar 14;9:862322. https://doi.org/10.3389/fsurg.2022.862322

[59] Le Berre C, Sandborn WJ, Aridhi S, Devignes MD, Fournier L, Smaïl-Tabbone M, Danese S, Peyrin-Biroulet L. Application of artificial intelligence to gastroenterology and hepatology. Gastroenterology. 2020 Jan 1;158(1):76-94. https://doi.org/10.1053/j.gastro.2019.08.058

[60] Rawashdeh A. The consequences of artificial intelligence: an investigation into the impact of AI on job displacement in accounting. Journal of Science and Technology Policy Management. 2025 Mar 6;16(3):506-35. https://doi.org/10.1108/JSTPM-02-2023-0030

[61] Derakhshan A, Teo T, Khazaie S. Investigating the usefulness of artificial intelligence-driven robots in developing empathy for English for medical purposes communication: The role-play of Asian and African students. Computers in Human Behavior. 2025 Jan 1;162:108416. https://doi.org/10.1016/j.chb.2024.108416

[62] Varriale V, Cammarano A, Michelino F, Caputo M. Critical analysis of the impact of artificial intelligence integration with cutting-edge technologies for production systems. Journal of Intelligent Manufacturing. 2025 Jan;36(1):61-93. https://doi.org/10.1007/s10845-023-02244-8

[63] Pandit T, Mahendru S, Raval M, Upadhyay D. The Evolution of Reranking Models in Information Retrieval: From Heuristic Methods to Large Language Models. InInternational Conference on Computational Linguistics and Natural Language Processing 2025 Jul 18 (pp. 56-67). Singapore: Springer Nature Singapore.

[64] Vasishta P, Dhingra N, Vasishta S. Application of artificial intelligence in libraries: a bibliometric analysis and visualisation of research activities. Library Hi Tech. 2025 May 19;43(2/3):693-710. https://doi.org/10.1108/LHT-12-2023-0589

[65] Samala AD, Rawas S, Wang T, Reed JM, Kim J, Howard NJ, Ertz M. Unveiling the landscape of generative artificial intelligence in education: a comprehensive taxonomy of applications, challenges, and future prospects. Education and Information Technologies. 2025 Feb;30(3):3239-78. https://doi.org/10.1007/s10639-024-12936-0

[66] Vora LK, Gholap AD, Jetha K, Thakur RR, Solanki HK, Chavda VP. Artificial intelligence in pharmaceutical technology and drug delivery design. Pharmaceutics. 2023 Jul 10;15(7):1916. https://doi.org/10.3390/pharmaceutics15071916

[67] Kumar I, Rawat J, Mohd N, Husain S. Opportunities of artificial intelligence and machine learning in the food industry. Journal of Food Quality. 2021;2021(1):4535567. https://doi.org/10.1155/2021/4535567

[68] Moor M, Banerjee O, Abad ZS, Krumholz HM, Leskovec J, Topol EJ, Rajpurkar P. Foundation models for generalist medical artificial intelligence. Nature. 2023 Apr 13;616(7956):259-65. https://doi.org/10.1038/s41586-023-05881-4

[69] Jaiswal A, Arun CJ, Varma A. Rebooting employees: Upskilling for artificial intelligence in multinational corporations. InArtificial intelligence and international HRM 2023 May 22 (pp. 114-143). Routledge. https://doi.org/10.4324/9781003377085-5

[70] Nie J, Jiang J, Li Y, Wang H, Ercisli S, Lv L. Data and domain knowledge dual-driven artificial intelligence: Survey, applications, and challenges. Expert Systems. 2025 Jan;42(1):e13425. https://doi.org/10.1111/exsy.13425

[71] Nenni ME, De Felice F, De Luca C, Forcina A. How artificial intelligence will transform project management in the age of digitization: a systematic literature review. Management Review Quarterly. 2025 Jun;75(2):1669-716. https://doi.org/10.1007/s11301-024-00418-z

[72] Qin C, Zhang L, Cheng Y, Zha R, Shen D, Zhang Q, Chen X, Sun Y, Zhu C, Zhu H, Xiong H. A comprehensive survey of artificial intelligence techniques for talent analytics. Proceedings of the IEEE. 2025 Jun 6. https://doi.org/10.1109/JPROC.2025.3572744
[73] Weiner EB, Dankwa-Mullan I, Nelson WA, Hassanpour S. Ethical challenges and evolving strategies in the integration of artificial intelligence into clinical practice. PLOS digital health. 2025 Apr 8;4(4):e0000810. https://doi.org/10.1371/journal.pdig.0000810
[74] Upadhyay D, Soni M, Gupta S, Sharma R, Venu N. Latency-Aware Network Slicing for 5G URLLC Applications: Design and Optimization Strategies. In2025 3rd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT) 2025 Mar 21 (pp. 113-118). IEEE.
[75] Jin F, Zhang X. Artificial intelligence or human: when and why consumers prefer AI recommendations. Information Technology & People. 2025 Jan 8;38(1):279-303. https://doi.org/10.1108/ITP-01-2023-0022
[76] Owan VJ, Abang KB, Idika DO, Etta EO, Bassey BA. Exploring the potential of artificial intelligence tools in educational measurement and assessment. Eurasia journal of mathematics, science and technology education. 2023 Aug 1;19(8):em2307. https://doi.org/10.29333/ejmste/13428
[77] Al Kuwaiti A, Nazer K, Al-Reedy A, Al-Shehri S, Al-Muhanna A, Subbarayalu AV, Al Muhanna D, Al-Muhanna FA. A review of the role of artificial intelligence in healthcare. Journal of personalized medicine. 2023 Jun 5;13(6):951. https://doi.org/10.3390/jpm13060951
[78] Kumar A, Shankar A, Hollebeek LD, Behl A, Lim WM. Generative artificial intelligence (GenAI) revolution: A deep dive into GenAI adoption. Journal of Business Research. 2025 Feb 1;189:115160. https://doi.org/10.1016/j.jbusres.2024.115160
[79] Jarrahi MH, Kenyon S, Brown A, Donahue C, Wicher C. Artificial intelligence: A strategy to harness its power through organizational learning. Journal of Business Strategy. 2023 Apr 14;44(3):126-35. https://doi.org/10.1108/JBS-11-2021-0182
[80] Gabriel I. Artificial intelligence, values, and alignment. Minds and machines. 2020 Sep;30(3):411-37. https://doi.org/10.1007/s11023-020-09539-2
[81] Javaid M, Haleem A, Khan IH, Suman R. Understanding the potential applications of Artificial Intelligence in Agriculture Sector. Advanced Agrochem. 2023 Mar 1;2(1):15-30. https://doi.org/10.1016/j.aac.2022.10.001
[82] Peres RS, Jia X, Lee J, Sun K, Colombo AW, Barata J. Industrial artificial intelligence in industry 4.0-systematic review, challenges and outlook. IEEE access. 2020 Dec 7;8:220121-39. https://doi.org/10.1109/ACCESS.2020.3042874
[83] Mohsen SE, Hamdan A, Shoaib HM. Digital transformation and integration of artificial intelligence in financial institutions. Journal of Financial Reporting and Accounting. 2025 Mar 20;23(2):680-99. https://doi.org/10.1108/JFRA-09-2023-0544
[84] Tuo Y, Wu J, Zhao J, Si X. Artificial intelligence in tourism: insights and future research agenda. Tourism Review. 2025 Mar 25;80(4):793-812. https://doi.org/10.1108/TR-03-2024-0180
[85] Alqahtani N, Wafula Z. Artificial intelligence integration: Pedagogical strategies and policies at leading universities. Innovative Higher Education. 2025 Apr;50(2):665-84. https://doi.org/10.1007/s10755-024-09749-x
[86] Xu Y, Liu X, Cao X, Huang C, Liu E, Qian S, Liu X, Wu Y, Dong F, Qiu CW, Qiu J. Artificial intelligence: A powerful paradigm for scientific research. The Innovation. 2021 Nov 28;2(4). https://doi.org/10.1016/j.xinn.2021.100179
[87] Galante N, Cotroneo R, Furci D, Lodetti G, Casali MB. Applications of artificial intelligence in forensic sciences: C urrent potential benefits, limitations and perspectives. International journal of legal medicine. 2023 Mar;137(2):445-58. https://doi.org/10.1007/s00414-022-02928-5
[88] Sheikh H, Prins C, Schrijvers E. Artificial intelligence: definition and background. InMission AI: The new system technology 2023 Jan 31 (pp. 15-41). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-21448-6_2
[89] Pandit T, Raval M, Upadhyay D. Multi-Domain ABSA Conversation Dataset Generation via LLMs for Real-World Evaluation and Model Comparison. arXiv preprint arXiv:2505.24701. 2025 May 30.
[90] Taeihagh A. Governance of artificial intelligence. Policy and society. 2021 Jun;40(2):137-57. https://doi.org/10.1080/14494035.2021.1928377
[91] Tu T, Schaekermann M, Palepu A, Saab K, Freyberg J, Tanno R, Wang A, Li B, Amin M, Cheng Y, Vedadi E. Towards conversational diagnostic artificial intelligence. Nature. 2025 Apr 9:1-9.
[92] Ozmen Garibay O, Winslow B, Andolina S, Antona M, Bodenschatz A, Coursaris C, Falco G, Fiore SM, Garibay I, Grieman K, Havens JC. Six human-centered artificial intelligence grand challenges. International Journal of Human-Computer Interaction. 2023 Feb 7;39(3):391-437. https://doi.org/10.1080/10447318.2022.2153320
[93] De Gagne JC. The state of artificial intelligence in nursing education: Past, present, and future directions. International journal of environmental research and public health. 2023 Mar 10;20(6):4884. https://doi.org/10.3390/ijerph20064884

[94] Chiu TK, Xia Q, Zhou X, Chai CS, Cheng M. Systematic literature review on opportunities, challenges, and future research recommendations of artificial intelligence in education. Computers and Education: Artificial Intelligence. 2023 Jan 1;4:100118. https://doi.org/10.1016/j.caeai.2022.100118

[95] De Vries A. The growing energy footprint of artificial intelligence. Joule. 2023 Oct 18;7(10):2191-4. https://doi.org/10.1016/j.joule.2023.09.004

[96] Korteling JE, van de Boer-Visschedijk GC, Blankendaal RA, Boonekamp RC, Eikelboom AR. Human-versus artificial intelligence. Frontiers in artificial intelligence. 2021 Mar 25;4:622364. https://doi.org/10.3389/frai.2021.622364

[97] Berente N, Gu B, Recker J, Santhanam R. Managing artificial intelligence. MIS quarterly. 2021 Sep 1;45(3):1433-50. https://doi.org/10.25300/MISQ/2021/16274