International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 10 Issue 1, Jan-Feb 2026 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Artificial Intelligence in Cybersecurity

Paul A. Adekunte[1], Matthew N. O. Sadiku[2], Janet O. Sadiku[3]

[1]International Institute of Professional Security, Lagos, Nigeria
[2]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[3]Juliana King University, Houston, TX, USA

ABSTRACT

Artificial intelligence (AI) in cybersecurity makes use of AI to revolutionize cybersecurity in enhancing threat detection, incident response, and vulnerability management. AI refers to computing systems that can perform tasks which normally require human intelligence – such as pattern recognition, learning from data, and decision-making. However, in cybersecurity, AI systems (especially machine learning and deep learning models) analyze massive data, detect threats, and respond faster than traditional rule-based systems. AI is transforming cybersecurity by enabling: 1. Faster, scalable threat detection, 2. Automated responses, and 3. Predictive threat intelligence. This as well introduces new challenges. This paper presents the usefulness, the various challenges cum solutions, and the benefits of AI in cybersecurity to humanity.

KEYWORDS: *Artificial Intelligence (AI), cybersecurity, Machine Learning (ML), Deep Learning (DL), ethical governance, Large Language Models (LLMs), adversarial attacks.*

How to cite this paper: Paul A. Adekunte | Matthew N. O. Sadiku | Janet O. Sadiku "Artificial Intelligence in Cybersecurity" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-10 | Issue-1, February 2026, pp.922-930, URL: www.ijtsrd.com/papers/ijtsrd100153.pdf

IJTSRD100153

INTRODUCTION

Artificial intelligence (AI) helps in transforming cybersecurity by enhancing threat detection, incident response, and vulnerability management, as shown in Figure 1. AI-powered systems analyze vast data to identify patterns and anomalies, detecting threats in real-time. It has key applications in the areas of threat detection and intelligence; phishing and social engineering prevention; network security and; incident response. Some of its benefits include improved detection accuracy, enhanced incident response, and reduced false positives. Challenges posed are: bias in training data, adversarial attacks, and explainability. AI in cybersecurity also enhances decision-making. By analyzing vast or large amounts of data, AI can identify patterns and correlations that humans can miss. These insights can inform strategic decisions, such as where to allocate resources or how to improve security protocols. The predictive capacities of AI also contribute to better decision-making.

By forecasting future threats and their potential impact, AI allows organizations to plan and prepare effectively. This proactive approach can significantly enhance an organization's resilience to cyber-attacks. As AI technology in cybersecurity continues to evolve, its potential for enhancing security measures will only grow, from automating routine tasks to predicting and preventing sophisticated attacks. A significant advantage of AI in cybersecurity is the ability to respond in real-time as opposed to traditional security which is time-consuming leading to slower response. AI systems can analyze and respond to threats as they occur, thereby significantly reducing the time between threat detection and response – thus organizations can minimize the damage caused by cyber-attacks, as shown in Figure 2. In other words, AI in cybersecurity refers to the use of machine learning (ML), deep learning (DL), and other related techniques (including large language models and generative models) to automate detection, analysis, response, and prediction of cyber threats – and, conversely, using AI by attackers to automate and improve offensive operations. This dual-use nature is central to the field [1-5].

HISTORY

Let us look at the structured history of artificial intelligence (AI) in cybersecurity showing how the technology evolved from basic rule-based tools into the advanced systems used today, as shown in Figure 3. The historical background to AI in cybersecurity is as stated below:

1. Foundations of AI (1950s-1980s)

Even though cybersecurity never yet existed as a formal field, however, early AI laid the foundation or groundwork via [6, 7]:

- 1950s – Alan Turing's work on machine intelligence (Turing Test) inspired automated reasoning.
- 1960s-1980s: There emerged Symbolic AI and Expert Systems, which enabled the rule-based automation that later influenced intrusion detection.

The early AI concepts are relevant to cybersecurity as it introduced pattern recognition and rule-based decision making it essential for later automated threat detection.

2. Early Automated Security & ML-Based Detection (1980s-1990s)

- 1980 (Anderson Report): This was the first major proposal for automated threat monitoring [8].
- 1987 (Dorothy Denning): She introduced the *intrusion detection model* using anomaly detection principles. This formed the first bridge between AI and cybersecurity [9].

The relevance is that the models made use of the early machine concepts (such as statistics, anomaly scoring) to identify unusual behavior on systems.

3. Machine Learning Expands (2000s)

- The growth of networks and malware drove interest in ML-based detection.
- Research focused on using classifiers (SVMs, decision trees, Bayesian models) to detect malware and network anomalies.
- Limitations: High false-positive rates, limited computing power, and lack of large datasets [10, 11].

The relevance was that these decades marked the first systematic attempts to apply AI techniques to real cybersecurity challenges.

4. Deep Learning and Behavior Analytics (2010s)

The 2010s witnessed the shift from signatures to behavior-based detection:

- 2010-2015: Machine learning during this period became mainstream in Intrusion Detection Systems (IDS).
- 2015-2018: Companies such as **Vectra AI, Darktrace,** and **Deep Instinct** introduced behavioral analytics and deep learning models for real-time detection and response.
- 2010s research revealed and emphasized unsupervised learning, clustering, and neural networks for threat classification [12-15].

The relevance of this is that AI has transitioned from research to commercial products capable of identifying unknown malware (zero-day or 0-day).

5. AI-Assisted Cyber Threat Intelligence (2020-2022)

- Defensive tools incorporated big-data analytics and automated threat hunting.
- Cloud security and endpoint detection and response (EDR/XDR) platforms adopted AI to triage security alerts.
- Early studies on AI-driven malware analysis and adversarial attacks on ML systems emerged [16-18].

The relevance of the above facts has made AI to become essential for large-scale cyber defense due to the volume of modern cyber threats.

WHAT AI DOES IN CYBERSECURITY

The core function of AI is to augment traditional cybersecurity by automating, scaling, and improving detection and response to threats that are too complex or fast for humans alone. This is achieved primarily through machine learning (ML), deep learning (DL), natural language processing (NLP), and anomaly detection techniques [19], as shown in Figures 4-7.

AI APPLICATIONS IN CYBERSECURITY AND CHALLENGES

It is a known fact that AI is revolutionizing cybersecurity, enhancing threat detection, incident response, and as well as vulnerability management. Some of the key applications, as shown in Figure 8 and challenges are as outlined below:

AI Applications in Cybersecurity

- Threat Detection and Intelligence: AI-powered systems analyze vast data to identify patterns and anomalies, detecting threats in real-time via learning pattern deviations – detecting attacks that can be missed by rule-based tools, e. g. network intrusion detection with >98% accuracy in detecting abnormal behavior. Also, behavioral analytics spots unusual logins, lateral movements, or data exfiltration.
- Phishing and Social Engineering Prevention: In this case, AI-driven tools recognize and block sophisticated phishing attempts.
- Network Security: AI-enhanced firewalls and intrusion detection systems monitor traffic and identify suspicious activities.

- Identity and Access Management (IAM): AI-powered IAM solutions detect and respond to unauthorized access attempts.
- Incident Response: AI automates incident response, reducing response times and minimizing damage [3, 18-21].

Challenges and Principal Risks

A look at the evolution of cyber threats shows that it has evolved far beyond the rudimentary viruses and worms of the past. As at today, modern cyberattacks leverage sophisticated techniques like AI-powered malware, social engineering, and zero-day exploits to breach defenses – such as Advanced Persistent Threats (APTs), use of deepfake technologies by hackers, and vulnerability of the Internet of Things (IoT) devices.

Some of the challenges and risks faced by AI in cybersecurity include the followings [22-28]:

- Bias in Training Data: AI models can inherit biases from training data, leading to flawed decisions, due to the generation of false alarms or misinterpretation of normal activity as malicious if training data is biased or incomplete.
- Adversarial Attacks & Model Poisoning: AI systems can be vulnerable to adversarial attacks, designed to evade detection. Attackers can tamper with training data or craft inputs that trick AI security models into misclassification. In other word, attackers can deliberately manipulate data inputs to confuse or bypass AI models (data poisoning).
- Explainability & Transparency: AI-driven decisions can be difficult to explain, making it challenging to understand and address threats. Many AI models are black boxes – meaning that their decisions are not easily interpretable by humans – which complicates incident analysis and regulatory compliance.
- Cybersecurity Risks/AI-Powered Attacks (Malicious use of AI/Offensive AI): AI models can be used to create sophisticated cyber threats, such as zero-day exploits, automated and scale attacks – including phishing, automated scanning, and malware creation. There is also the recent emergence of fully automated "vibe crime" attacks using agentic AI.
- False Positives & Blind Spots: Since AI isn't perfect, hence it can generate:
  - False positives (benign events flagged as threats)
  - False negatives (real threats missed)

This can overwhelm analysts or provide a false sense of security.

- Data Privacy & Security Issues: Cybercriminals may train datasets to inject poisoned data and compromise the integrity of the model. Differential Security (DS) and Federated Learning (FL) have been proposed to resolve privacy risks. The protection of large datasets containing sensitive user information are major concerns to comply with.
- Legal and Ethical Issues: The legal and ethical consequences of AI in cybersecurity continued to be complex and evolving. AI-enabled security software must follow regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). This enforces strict procedures on data collection, storage, and processing. There are also ethical concerns, like bias in AI and its use in mass surveillance. There is therefore the need to build AI that is clear about how it makes decisions.
- Talent Shortage: Skilled professionals who understand both cybersecurity and AI are in short supply, thereby slowing adoption and oversight.

Defenses, Mitigation and Operational Controls

The defenses, mitigation and operational controls of AI in cybersecurity can be carried out via:

1. **Technical controls:**

- Advanced training & robust models: This would involve the inclusion of adversarial examples at training time and use of model architectures known to be more robust where possible [29].
- Input validation & feature sanitization: Need to normalize inputs, strip suspicious content before model ingestion, and the use of layered detectors (static + dynamic) [30].
- Ensemble & layered detection: Combine signature rules, anomaly detection, and ML to reduce single-point failures [31].
- Model monitoring & drift detection: Need to continuously monitor model accuracy, data distribution shifts, and alert on unusual query patterns (to detect model extraction attempts) [32].
- Rate-limiting & query controls: Protect public model endpoints with throttling, authentication, and logging to mitigate extraction and abuse [33].
- Use of XAI carefully: Provide analysts with explainability for triage, but restrict detailed explanations in public APIs to avoid leakage [34].

2. **Process & governance:**

- AI Risk Management Frameworks: One should apply NIST AI RMF for governance, mapping AI risks to business impact and mitigation strategies [32].
- Secure development lifecycle (SDL) for models: Threat modeling for ML components, code reviews for model code, data governance and provenance checks, third-party model evaluation [35, 36].
- Red team/purple team ML testing: Need for routine adversarial testing (poisoning, evasion, extraction) to validate robustness [37].
- Human-in-the-loop and Security Operations Centre (SOC) integration: Route high risk/low confidence alerts to analysts; this keeps humans for final decisions on blocking or intrusive response actions [38].

The standards, frameworks, and guidance for AI in cybersecurity

With regards to the above, the underlisted facts are to be utilized:

1. NIST AI Risk Management Framework (AI RMF) – This is to serve as a foundational guidance for governance and lifecycle risk management for AI systems. It is an essential reading for program leaders [16, 32].
2. ENISA reports – They are to serve as practical cybersecurity controls specific to AI, plus a multilayer framework for securing AI systems. Useful for EU/UK/Global practitioners [17, 35].
3. MITRE ATLAS / ATT&CK extension for AI (ATLAS) – Catalogs attack specific to ML/AI systems and ties to defender mitigations (very useful for red/purple team design) [39].
4. CISA guidance on generative AI risks – For critical-infrastructure orgs and election security lens [40], as shown in Figure 9.

Tools, datasets, and research resources for AI in cybersecurity

These are required for:

1. Knowledge bases and mapping: MITRE ATT&CK (for attacker TTPs) and MITRE ATLAS (AI-specific attacks [41].
2. Dataset collections: Public malware corpora and labeled phishing datasets (used in many academic reviews) – reference to malware/malicious-URL datasets in malware detection literature [42].
3. Open-source defensive tooling: Model-monitoring libraries, adversarial example toolkits, SIEM/SOAR integrations, and toolchain [43].

Actionable checklist for security teams

Some of the actionable checklist for security teams include [29, 31, 33, 35]:

1. Inventory ML assets (models, datasets, endpoints) and Map criticality.
2. Apply NIST AI RMF & ENISA multilayer practices to those assets.
3. Add model monitoring & drift detection to pipelines; log model inputs and outputs for audit.
4. Run adversarial tests monthly (poisoning, evasion, extraction simulation).
5. Use emsemble detection (static + dynamic + ML) to reduce single-model failure.
6. Protect model endpoints with auth, rate-limits and anomaly detection; treat model access like a privileged service.
7. Keep a human-in-the-loop for high-impact decisions and continually train analysts on AI signals.

BENEFITS OF AI IN CYBERSECURITY

Some of the key benefits of AI in cybersecurity include:

1. Detecting threats in real-time – AI systems can analyze massive volumes of data (like network traffic, logs, and user activity) continuously and in real-time – detecting suspicious patterns or behavior immediately rather than waiting for human review. This helps organizations identify threats as they occur rather than after damage is done [44].
2. Enhanced accuracy and reduced false positives – Traditional systems often overwhelm security teams with alerts – many of which are benign. However, AI uses machine learning (ML) to distinguish real threats from harmless activity more precisely, reducing "false fatigue" and freeing analysts to focus on real risks [44, 45].
3. Proactive threat prediction – AI doesn't just react, but it can predict likely attack vectors by analyzing historical attack data and behavioral patterns. This means that organizations can reinforce defenses before threats materialize [44].
4. Automated Incidence Response – At the detection of a breach or malicious event, AI will automatically trigger predefined responses (e.g., isolate affected systems, block IP addresses, enforce patches) without waiting for manual intervention, which drastically cuts down response time [46].

5. Scalability without proportionally more staff – AI can monitor and protect vast amounts of endpoints (servers, devices, cloud resources) without requiring a corresponding increase in human analysts. This makes cybersecurity economically scalable for large and growing environments [46].
6. Advanced Malware, Phishing and Zero-day Threat Detection – Traditional antivirus relies on known signatures. AI leverages behavioral analysis and pattern recognition to detect malware and phishing campaigns – even new ("zero-day") threats that haven't been catalogued yet [47].
7. User & Entity Behavior Analytics – AI models establish baselines of normal behavior and flag deviations, helping detecting insider threats, compromised accounts, or malicious automation. This is key for identity-centric defense strategies [48].
8. Better Compliance & Data Protection – AI helps to enforce data governance and privacy standards by monitoring access to sensitive information and automating enforcement of policies such as encryption and access controls [44].
9. Reduced Operational Costs – By automating repetitive and resource-intensive tasks (like scanning logs or managing alerts), AI helps to reduce the manpower needed for routine security tasks, thereby lowering costs while enhancing protection [49].
10. Supports Human Security Teams – AI simply augments human expertise rather than replacing it. AI handles scale, speed, and pattern analysis, while human professionals focus on strategic decisions [50].

There are several types of artificial intelligence based on capabilities, functionalities, and technologies of which are [51]: Narrow AI (Weak AI), General AI (Strong AI), Superintelligent AI, Reactive Machines, Limited Memory, Theory Mind, Self-aware AI, Machine Learning, Deep Learning (a subset of ML), Natural Language Processing (NLP), Robotics, Computer Vision, Expert Systems. The various branches of AI include:

- Machine learning
- Deep learning
- Natural language processing
- Robotics, and
- Expert systems

CONCLUSION

Artificial intelligence (AI) as an indispensable modern cybersecurity enables more proactive, scalable, and intelligent defense. However, with all its benefits, AI in cybersecurity is inseparable from its risks (dual-use risks) as the same AI methods can be deployed by attackers to automate attacks, increasing scale and sophistication. Therefore, maximizing value while minimizing harm will depend on balanced strategies that integrate AI capabilities with robust human judgement, ethical guardrails, and ongoing adaptation to a rapidly evolving threat landscape. The future directions would require human-AI collaboration, regulatory frameworks, and explainable and trustworthy AI that are critical for sustainable cybersecurity. More information on artificial intelligence in cybersecurity can be found in the books in [52-61] and the following related journals:

International Journal of Artificial Intelligence and Cybersecurity (IJAIC)

International Journal of Cybersecurity and Artificial Intelligence (IJCSAI)

Cybersecurity & General Security Journals

Journal of Cybersecurity

Computers & Security

International Journal on Sematic Web and Information Systems

IT Journal Research and Development

International Journal of Computational and Experimental Science and Engineering

Journal of Engineering Research and Reports

Computing and Artificial Intelligence

REFERENCES

[1] S. Kenny, "The impact of AI analytics and cybersecurity," February 7, 2023, https://www.newsroom.axis.com/impact-of-ai-analytics-and-cybersecurity

[2] A. Sheps (January 4, 2024), "What is AI in cyber security?" https://www.aquasec.com/what-is-ai-in-cyber-security

[3] "AI use cases in cybersecurity: 6 Examples," https://www.legitsecurity.com/ai-use-cases-in-cybersecurity-6-examples

[4] "9 trends on AI security shaping the future of defense," July 23, 2025 https://www.auxis.com/9-trends-on-ai-security-shaping-the-future-of-defense

[5] T. Sowmya & E. A. Mary Anita (August 2023), "A comprehensive review of AI based intrusion detection system," *Measurement: Sensors,* vol. 28. https://www.sciencedirect.com/a-

comprehensive-review-of-ai-based-intrusion-detection-system

[6] A. M. Turing (1950), *Computing machinery and intelligence,* Mind, vol. 59, no. 236, pp. 433-460.

[7] S. Russell & P. Norvig (2021), *Artificial Intelligence: A Modern Approach (4th ed.),* Pearson Education.

[8] J. P. Anderson (1980), *Computer security threat monitoring and surveillance,* James P. Anderson Co.

[9] D. E. Denning (1987), *An intrusion-detection model,* IEEE Transactions on Software Engineering, vol. 13, no. 2, pp. 222-232.

[10] R. Sommer & V. Paxson (2010), "Outside the closed world: On using machine learning for network intrusion detection," *IEEE Symposium on Security and Privacy,* pp. 305-316.

[11] A. L. Buczak & E. Guven (2016), "A survey of data mining and machine learning methods for cybersecurity intrusion detection," *IEEE Communications Surveys & Tutorials,* vol. 18, no. 2, pp. 1153-1176.

[12] J. Saxe & K. Berlin (2015), "Deep neural network-based malware detection," *2015 IEEE Malicious and Unwanted Software Conference (MALCON).*

[13] A. Shalaginov et al. (2020), "AI-assisted malware analysis," arXiv:2009.11101.

[14] T. Raynel, "Vectra AI unveils enhance Cloud Detection Response for AWS," *SscurityBrief Asia.* Retrieved 2023-12-21.

[15] "Vectra AI," Wikipedia, the free encyclopedia, https://en.wikipedia.org/vectra-ai

[16] National Institute of Standards and Technology (NIST) (2023), *AI Risk Management Framework (AI RMF 1.0).*

[17] European Union Agency for Cybersecurity (ENISA) (2022), *Artificial Intelligence Cybersecurity Challenges*.

[18] J. Strasburg & R. Winkler (2024), "AI hackers are coming dangerously close to beating humans," *The Wall Street Journal.*

[19] "Cybersecurity and artificial intelligence: How AI is being used in cybersecurity to improve detection and response to cyber threats," (PDF), December 17, 2018, *Turkish Journal of Computer and Mathematics Education* (TURCOMAT), vol. 9, no. 3. https://www.turcomat.org/

[20] "AI in cybersecurity: Use cases, challenges, and best practices," October 10, 2025, https://www.cynet.com/ai-in-cybsecurity-use-cases-challenges-and-best-practices

[21] "AI in cybersecurity: How AI is changing threat defense," July 20, 2025 https://www.ischool.syracuse.edu/ai-in-cybersecurity-how-ai-is-changing-threat-defense

[22] "AI in cybersecurity: Staying ahead of emerging threats," https://www.intellinez.com/ai-in-cybersecurity-staying-ahead-of-emerging-threats

[23] S. Okdem & S. Okdem (2024), "Artificial intelligence in cybersecurity: A review and a case study," *Journal of Applied Sciences,* vol. 14, no. 22, pp 10487.

[24] K. Achuthan et al. (2024), "Advancing cybersecurity and privacy with artificial intelligence: current trends and research directions," https://www.pmc.ncbi.nlm.nih.gov/advancing-cybersecurity-and-privacy-with-artificial-intelligence-current-trends-and-future-research-directions

[25] "What are the risks and benefits of artificial intelligence (AI) in cybersecurity?" https://www.paloaltonetworks.in/what-are-the-risks-and-benefits-of-artificial-intelligence-in-cybersecurity

[26] "Trend Micro issues warning over rise of 'vibe crime' as cyber criminals turn to agentic AI to automate attacks," https://www.itpro.com/trend-micro-issues-warning-over-rise-of-vibe-crime-as-cyber-crimimals-turn-to-agentic-ai-to-automate-attacks

[27] C. Mendes & T. N. Rios (27 February 2023), "Explainable artificial intelligence and cybersecurity: A systematic literature review," (PDF), https://www.arxiv.org

[28] L. C. Ming (12 December 2025), "An AI agent spent 16 hours hacking Stanford's network. It outperformed human pros for much less than their 6-figure salaries," https://www.businessinsider.com

[29] S. Alkadi, S. Al-Ahmadi & M. M. Ben Ismail (2023), "Better safe than never: A survey on Adversarial Machine Learning Applications towards IoT environment," https://www.mdpi.com/better-safe-than-never-

a-survey-on-adversarial-machine-learning-applications-towards-iot-environment

[30] D. S. Adeyemi (2025), "AI-driven malware detection and classification: A systematic review of techniques and effectiveness," *European Journal of Computer Science and Information Technology,* vol. 13, no. 52, pp. 13-34.

[31] R. Kaur, D. Gabrijelcic & T. Klobucar (September, 2023), "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion,* vol. 97, https://www.sciencedirect.com/artificial-intelligence-for-cybersecurity-literature-review-and-future-research-directions

[32] "AI risk management framework 1 NIST," https://www.nist.gov/ai-risk-management-framework

[33] Reuters (December 10, 2025), "OpenAI warns new models pose 'high' cybersecurity risk," https://www.reuters.com/openai-warns-new-models-pose-high-cybersecurity-risk

[34] A. Sharma, S. Rani & M. Shabaz (December 2025), "A comprehensive review of explainable AI in cybersecurity: Decoding the black box," *ICT Express,* vol. 11, no. 6, pp. 1200-1219. https://www.sceincedirect.com

[35] "Multilayer Framework for good Cyber Security Practices (FAICP) for AI," https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai

[36] Microsoft, "What is the MITRE ATT&CK framework?" https://www.microsoft.com/what-is-mitre-att&ck-framework

[37] M. Thukkaram (October 2025), "An adversarial testing framework for multi-agent red-blue systems in automated software hardening," *International Journal of Scientific Research in Engineering and Management,* vol. 09, no. 10, pp. 1-9.

[38] N. Madhusudanan & R. Manickam (July 2023), "The role of the human-in-the-loop in dustrial digitalization and automation," In: "Design in the Era of Industry 4.0," vol. 1, pp. 1241-1250. https://www.researchgate.net

[39] "MITRE ATLAS: Insights into AI-based threats," https://www.packetlabs.net/mitre-atlas-insights-into-ai-based-threats

[40] America's Cyber Defense Agency, "Risk in focus: Generative AI and the 2024 Election Cycle," https://www.cisa.gov/risk-in-focus-generative-ai-and-the-2024-election-cycle

[41] Ir. C. Lim, "Best practices for mapping cyber threats using the MITRE ATT&CK framework," https://www.sgu.ac.id/best-practices-for-mapping-cyber-threats-using-the-mitre-att&ck-framework

[42] P. Mendes, E. Maia & I. Praca, "MeAJOR Corpus: A multi-source dataset for phishing Email detection," https://www.arxiv.org/meajor-corpus-a-multi-source-dataset-for-phishing-email-detection

[43] R. Krohn, "Considerations for your DevOps toolchain," https://www.atlassian.com/considerations-for-your-devops-toolchain

[44] A. Kunwar (March 10, 22025), "5 Benefits of implementing AI in cybersecurity," https://www.timesofai.com/5-benefits-of-implementing-ai-in-cybersecurity

[45] N. Hassan (07 February 2025), "The advantages and disadvantages of AI in cybersecurity," https://www.techtarget.com/the-advantages-and-disadvantages-of-ai-in-cybersecurity

[46] "Benefits of AI in cybersecurity: How artificial intelligence is transforming digital defense," June 18, 2025. https://www.transfotechacademy.com/benefits-of-ai-in-cybersecurity-how-artificial-intelligence-is-transforming-digital-defense

[47] "How AI improves cybersecurity: Techniques and use cases," https://www.oxfordcentre.uk/how-ai-improves-cybersecurity-techniques-and-use-cases

[48] D. Gupta & C. Brown (ed.) (July 05, 2023), "10 Benefits of using AI in cybersecurity practices," https://www.entrepreneur.com/10-benefits-of-using-ai-in-cybersecurity-practices

[49] Altamira Team (04 September 2023), "AI in cyber security: Benefits and use cases," https://www.altamira.ai/ai-in-cyber-security-benefits-and-use-cases

[50] S. Varalakshmi, "An AI-driven security approach to fortifying our digital ecosystem against cyber threats," *International Journal of Cyber Security* (IJCS), vol. 3, no. 2, July-December 2025, pp. 74-86.

[51] A. Kumar (August 20, 2025), "Types of AI explained," https://www.simplilearn.com/types-of-ai-explained

[52] V. Kulothungan (15 January 2025), "Securing the AI frontier: Urgent ethical and regulatory imperatives for AI-driven cybersecurity," (PDF), https://www.arxiv.org

[53] Executive Office of the President, "Preparing for the future of artificial intelligence," Obama White House Archives, 2016.

[54] UNESCO, "Recommendation on the ethics of artificial intelligence," 2021.

[55] M. Mitchell, "Artificial intelligence: A guide for thinking humans," Pelican, 2020.

[56] Symantec (2022), *Internet security threat report,* Broadcom Inc.

[57] B. Kolosnjaji et al., "Artificial intelligence for cybersecurity."

[58] F. Bergadano & G. Giacinto (eds.), "AI for cybersecurity: Robust models for authentication, threat and anomaly detection."

[59] S. Ajuwon et al. (2025-12-12), "AI-driven cybersecurity strategies for detecting threats and enhancing network resilience in critical infrastructure," *Journal of Engineering Research and Reports,* vol. 27, no. 12, pp. 327-347.

[60] Z. B. Akhtar & A. T. Rawol (2024), "Harnessing artificial intelligence (AI) for cybersecurity: Challenges, opportunities, risks, future directions," *Computing and Artificial Intelligence,* vol. 2, no. 2, 1485.

[61] D. Schatz, R. Bashroush & J. Wall, "Towards a more representative definition of cyber security," *The Journal of Digital Foresics, Security and Law,* vol. 12, no. 2, pp. 1558-7215, 2017.

Figure 1: Artificial intelligence
Source:
https://en.wikipedia.org/wiki/Artificial_intelligence

Figure 2. AI safety
Source: https://en.wikipedia.org/wiki/AI_safety

Figure 3. History of artificial intelligence
Source:
https://en.wikipedia.org/wiki/History_of_artificial_intelligence

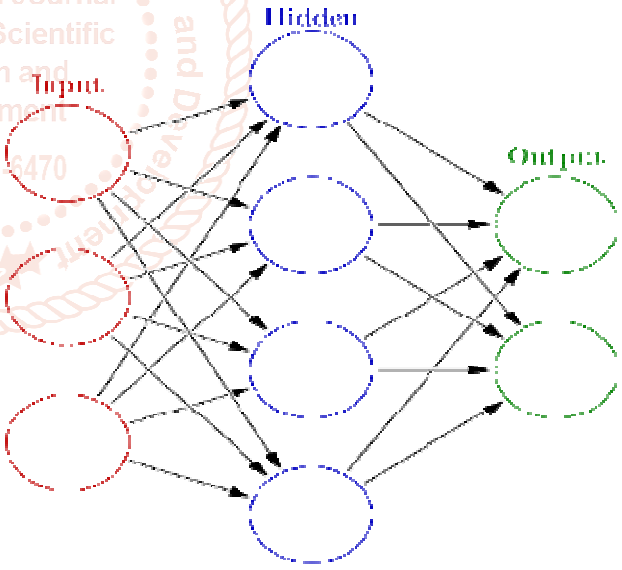

Figure 4. Neural network (Machine Learning)
Source:
https://en.wikipedia.org/wiki/Neural_network_(machine_learning)

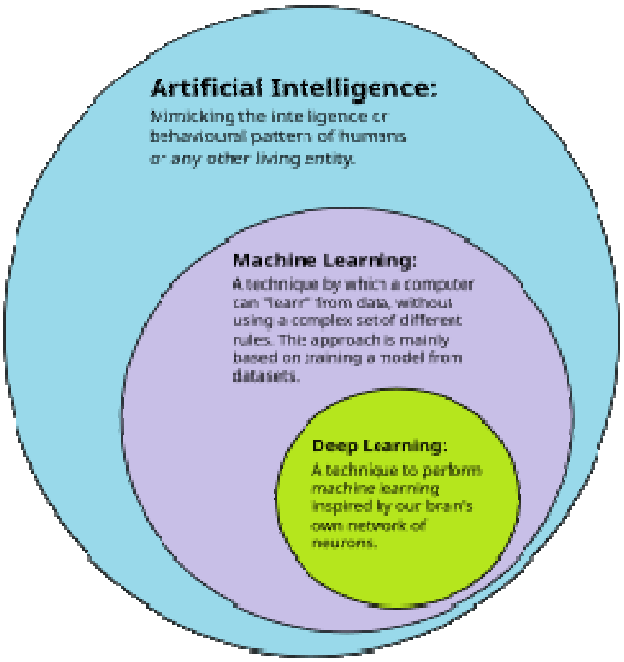

Figure 5. Deep Learning
Source:
https://en.wikipedia.org/wiki/Deep_learning

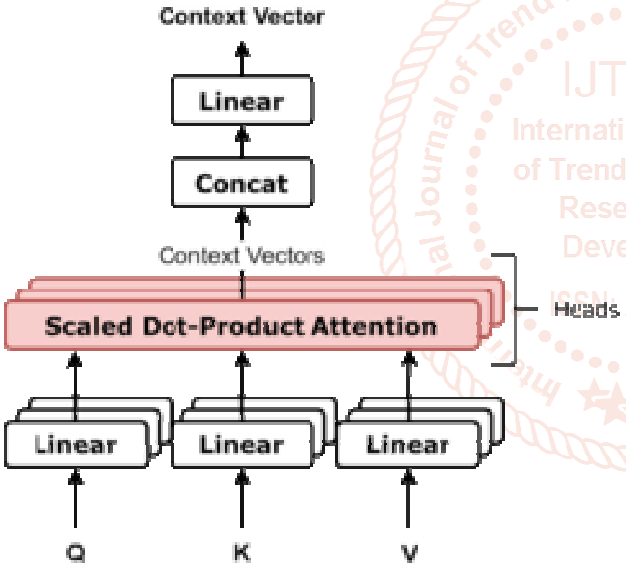

Figure 6. Transformer (Deep Learning)
Source:
https://en.wikipedia.org/wiki/Transformer_(deep_learning)

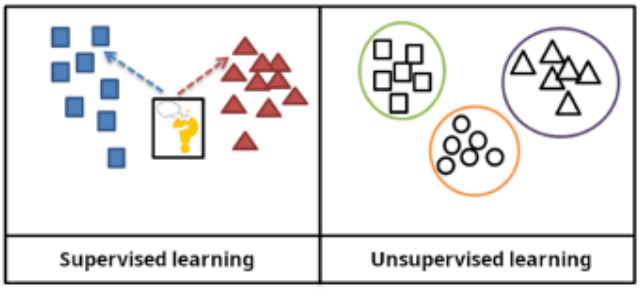

Figure 7: Artificial intelligence
Source:
https://en.wikipedia.org/wiki/Artificial_intelligence

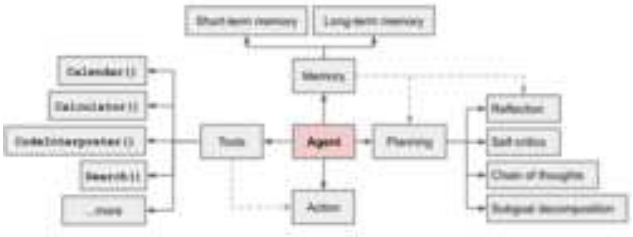

Figure 8: Applications of artificial intelligence
Source:
https://en.wikipedia.org/wiki/Applications_of_artificial_intelligence

Figure 9. Generative artificial intelligence
Source:
https://en.wikipedia.org/wiki/Generative_artificial_intelligence