**GLOBAL TRENDS IN AI-DRIVEN CYBERSECURITY: A SYSTEMATIC AND BIBLIOMETRIC ANALYSIS**

**ABSTRACT**

This study investigates global trends in artificial intelligence (AI)-driven cybersecurity through a combined systematic literature review and bibliometric analysis of publications from 2015 to 2025. As digitalisation accelerates and cyberattacks become increasingly sophisticated, AI has emerged as a transformative tool for threat detection, prevention, and response. The review identifies four core domains where AI applications are most prominent: anomaly-based intrusion detection systems, automated malware analysis, phishing and social engineering prevention, and Security Orchestration, Automation, and Response (SOAR). In these areas, machine learning and deep learning techniques, particularly convolutional and recurrent neural networks, autoencoders, and transformer-based models demonstrate superior performance in detecting complex, evolving threats compared to traditional rule-based approaches. The bibliometric analysis reveals exponential growth in research output since 2015, with a sharp rise between 2021 and 2023, coinciding with breakthroughs in generative AI, deep learning, and the increased cyber risks linked to the COVID-19 digitalisation surge. Citation patterns highlight the growing applied relevance of post-2020 research, while thematic evolution indicates a shift toward adversarial AI, federated learning, and zero-trust architectures. Despite significant advances, challenges persist around explainability, governance, dual-use risks, and global disparities in research capacity. This study underscores AI’s central role in shaping the future of cybersecurity while emphasising the need for ethical frameworks and equitable global participation in technological adoption.

**Keywords**: Artificial Intelligence, Cybersecurity, Machine Learning, Deep Learning, Intrusion Detection, Malware Analysis, Bibliometric Analysis.

# **Introduction**

The application of artificial intelligence (AI) in cybersecurity has emerged as a ground-breaking strategy in recent years to address the growing complexity and number of cyberthreats (Jimmy, 2021). Conventional rule-based and signature-based security solutions have not been sufficient to combat sophisticated persistent attacks, zero-day threats, and dynamic malware since the rapid expansion of digitalisation, cloud computing, and gadgets. Thus, artificial intelligence (AI), and more especially techniques like natural language processing (NLP) and deep learning (DL), has become a key enabler of intelligent, flexible, and real-time cybersecurity solutions (Rahul, 2023). AI's capacity to scan vast volumes of data to detect attacks, automate the response, and learn from previous threats to fortify future defences further increases its significance in cybersecurity (Ismail, 2024). Furthermore, AI frameworks have been shown to be successful in cutting down on the time needed to identify and eliminate threats, which is crucial in the dynamic threat landscape (Saeed et al., 2023). According to Ahmed et al. (2025), deep learning models such as convolutional and recurrent neural networks are ideal for malware tagging and intrusion detection because they can identify patterns in large amounts of unstructured data. By evaluating unstructured threat data, such as phishing emails and social media postings, natural language processing (NLP) also helps with early threat identification. According to Prima and Bouhorma (2020), integrating all of these AI technologies significantly improves cybersecurity preparedness and resilience to new attacks.

When it comes to the use of AI-driven cybersecurity, the UK has taken the lead. Threat intelligence, intrusion detection, and digital forensics applications of artificial intelligence (AI) have been extensively deployed throughout critical infrastructure as a result of the UK's National Cyber Security Centre (NCSC) placing a strong focus on technical innovation and resilience (Ndubuisi, 2023; Clark, 2024). UK banking institutions, for example, have used AI-enabled fraud detection systems that examine large transactional databases to find irregularities suggestive of phishing or insider trading (Islam and Rahman, 2025). In a similar vein, the National Health Service (NHS) in the United Kingdom has used artificial intelligence (AI) techniques to enhance data privacy and identify weaknesses in medical information systems, especially during the COVID-19 pandemic when cyberattacks on the healthcare industry increased (NHS England, 2025). Research shows that AI has potential in the fight against cybercrime. AI-driven and automated cybersecurity solutions should be given priority in order to assist various sectors with real-time threat identification, since cyber risks have had an influence on their operations (Li and Liu, 2021). Spam, phishing, malware, ransomware, corporate account takeover (CATO), distributed denial of service (DDoS) assaults, and automated teller machine (ATM) cash-out are some of these dangers (Mass.gov, 2024). While cybercriminals have utilised these assaults to make their online operations easier, countries have looked for various strategies to defend against them. In order to assist in protecting countries' economies, this has led to the incorporation of AI technologies into national vital security infrastructure.

Although AI's involvement in cybersecurity has been widely studied and adopted quickly, a thorough and cohesive understanding of this worldwide issue is still lacking. There is a notable lack of systematic and bibliometric analysis mapping the field's intellectual structure in the literature, despite the fact that many studies have provided a systematic, quantitative approach to investigate these dimensions, offering insight into the discipline's history and current status (Albahri and AlAmoodi, 2023). Identification of significant research trends, significant contributors, and new areas of innovation all depend on this kind of analysis. By combining the quantitative rigour of a bibliometric study with the qualitative insights of a systematic review, this research aims to close this crucial gap.

# **2.0 Methodology**

## **2.1 Research Framework**

This research employs bibliometric analysis and PRISMA (Preferred Reporting Items for Systematic Reviews) for the literature on artificial intelligence (AI) in crime control. Publications in English from 2015 to 2025 are included in the analysis. The PRISMA framework, as shown in **figure 1,** was employed in the study's methodology.



***Figure 1:*** *PRISMA framework*

## **2.2 Sources and search strategy**

To conduct the bibliometric study, Scopus, Web of Science, IEEE Xplore, and PubMed were relied upon for peer-reviewed articles about cybersecurity and AI. Scopus is a bibliographic database that is used for a variety of bibliometric investigations due to its extensive coverage of academic journals, conference proceedings, and other scholarly publications (Baas et al., 2020). The following search query was used to launch the literature search. “((cybersecurity OR cyber security OR cyber-security) AND Artificial intelligence)”. To ensure a thorough picture of current research tendencies, a search was done to include publications from 2015 (the beginning of the past decade) up to the present year. Eight hundred and ninety-six papers were found in total after the first search.

## **2.3 Eligibility criteria**

A multi-stage filtering method was used to guarantee that the retrieved publications were appropriate for our study needs. The following standards were used:

TABLE 1. Selection criteria for AI-driven cybersecurity research (2015–2025)

|  |  |
| --- | --- |
| **Inclusion criteria** | **Exclusion criteria** |
| Articles written in English | The studies that are not written in English |
| Published between 2015 and 2025 | Published before 2015 or after 2025 |
| Research articles are scholarly papers that provide an in-depth examination and analysis of original research.  | The studies that provide a review or survey of AI in different cybersecurity domains; |
| Academic papers that have been presented at conferences or symposiums. Thorough examinations and analyses of existing literature, encompassing comprehensive reviews and surveys. | Papers that did not pertain directly to the global trends in AI-driven cybersecurity were omitted from consideration.  |
| Editorial content that engages in discussions about significant topics within the discipline.  | In order to prevent redundancy, duplicate publications were excluded.  |

## **2.4 Study Selection**

The process for study selection involved:

* Screening titles and abstracts for relevance.
* Assessing full texts against inclusion and exclusion criteria.
* Selecting studies for detailed analysis descriptions.

## **2.5 Quality Assessment**

The papers were evaluated for quality and relevance based on their connection with the research subject, journal impact factor, and citation impact. A simplified technical assessment checklist (leakage controls, baselines, reproducibility, dataset provenance, threat model clarity, and validation technique) was employed for peer-reviewed empirical investigations. We used the AACODS (authority, accuracy, coverage, objectivity, date, importance) criteria for grey literature, giving official UK, EU, and US agencies priority (Garousi et al., 2019).

## **2.6 Data Analysis**

Bibliometric methods were used to:

* Identify trends and patterns in publication over time
* Map the geographical distribution of research
* Extract and analyse frequently used keywords and topics
* Analyse the network of authorship and collaboration.

# **3.0 Results**

The findings of this dual-methodological study are presented in two parts: a qualitative summary derived from the systematic literature review and a quantitative analysis from the bibliometric data.

## **3.1 Systematic Literature Review: Key Themes and AI Applications**

The systematic review identified four primary themes in the application of AI for cybersecurity, each leveraging different AI techniques.

### **3.1.1 Anomaly-Based Intrusion Detection System (IDS)**

According to Goswami (2024), anomaly-based intrusion detection has emerged as the most prolific area of AI-driven cybersecurity research, focusing on identifying deviations from normal network behaviour to detect malicious activity. Unlike signature-based systems that rely on known attack patterns, anomaly-based IDS can identify novel and zero-day threats by modelling what constitutes “normal” traffic (Kamboj et al., 2025). Within this space, machine learning (ML) techniques remain dominant. Decision trees and random forests have been widely employed due to their interpretability, computational efficiency, and high accuracy in classifying abnormal network behaviours (Kinasih et al., 2024).

More recently, deep learning (DL) models have gained traction for their superior ability to learn complex, high-dimensional feature representations directly from raw traffic data (Pati et al., 2024). Autoencoders, for example, have demonstrated high precision in detecting subtle anomalies, while Convolutional Neural Networks (CNNs) have been applied successfully to packet-level analysis (Javed et al., 2024). Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) architectures, have shown promise in detecting sequential attack patterns across time-series traffic data (Mienye et al., 2024). Taofeek (2025) reported that an LSTM-based IDS outperformed traditional methods on the NSL-KDD dataset, achieving significantly higher detection accuracy.

Building on this trend, Celic et al. (2025) recently developed an LSTM-enhanced IDS that achieved 98.7% accuracy on the CSE-CIC-IDS 2018 dataset, marking a substantial improvement over conventional model. These advancements highlight a clear trajectory in the literature: while ML-based anomaly detection systems remain valuable for their simplicity and interpretability, DL approaches are increasingly favoured for addressing sophisticated and stealthy attacks that evade traditional defences.

### **3.1.2. Automated Malware Analysis**

Artificial intelligence has become central to advancing malware detection through both static and dynamic analysis techniques. Static analysis typically examines executable features such as file headers, byte sequences, and opcode n-grams, enabling classification of malware families without executing the code (Hassen et al., 2017). Machine learning models such as Support Vector Machines (SVMs) and Random Forests have demonstrated strong performance in this domain, effectively distinguishing between benign and malicious binaries (Ismail et al., 2024). Dynamic analysis, on the other hand, focuses on behavioural characteristics such as API call sequences, system calls, and runtime features. This approach has benefitted from recurrent neural networks (RNNs), which can model sequential dependencies and identify malicious intent across long behavioural traces (Tomiyama et al., 2023).

A particularly influential line of research leverages Convolutional Neural Networks (CNNs) for visual malware analysis, where binary executables are transformed into greyscale images, allowing CNNs to identify subtle structural patterns that are often invisible to traditional methods (Kiger et al., 2022). More recent work has demonstrated CNNs achieving high accuracy in classifying large-scale malware datasets with minimal feature engineering (Jones, 2025).

Emerging research has also explored the dual role of Generative Adversarial Networks (GANs) in malware (Happiness and Song, 2025). On the offensive side, GAN can create adversarial malware samples designed to evade detection. However, they also provide defenders with a tool for augmenting training datasets, thereby improving the robustness of malware detection systems (Kc, Shushant Sapkota and Adhilkari, 2024). This dual-use aspect underscores both the promise and ethical dilemmas of applying AI in this domain. Overall, the literature demonstrates that AI-driven malware analysis has moved beyond traditional signature-based detection to more adaptive, scalable, and resilient approaches.

### **3.1.3. Phishing and Social Engineering Prevention**

Phishing and social engineering attacks remain some of the most pervasive and damaging forms of cybercrime, exploiting human vulnerabilities rather than purely technical weaknesses (Adu-Manu et al., 2022). Artificial intelligence has been increasingly leveraged to mitigate these threats through linguistic and behavioural analysis. Natural Language Processing (NLP) techniques are particularly effective in detecting phishing content by examining email text, subject lines, and embedded URLs for anomalies (Indranil Iyer, 2024). Early studies applied Support Vector Machines (SVMs) and Naïve Bayes to identify suspicious linguistic features (Dey et al., 2020), but recent advances in deep learning have enabled more sophisticated detection (Liu, 2024). Long Short-Term Memory (LSTM) networks have been widely adopted to capture sequential dependencies in textual data, outperforming traditional classifiers on large phishing datasets (Liu, 2024).

More recently, transformer-based models such as BERT have demonstrated state-of-the-art performance by leveraging contextual embeddings to distinguish between benign and malicious emails (Jamal et al., 2023; Otieno et al., 2023). These approaches not only improve precision in filtering phishing emails but also reduce false positives, a critical factor for user trust and operational efficiency.

Beyond content analysis, researchers are increasingly turning to behavioural analytics to address more subtle forms of social engineering. Machine learning models have been trained to identify anomalous user activity, such as a sudden spike in email forwarding, atypical login attempts, or unusual access times, which may signal account compromise (Devineni et al., 2023). By combining NLP-driven content inspection with behavioural monitoring. AI systems provide multi-layered defence mechanisms capable of addressing both technical and psychological vectors of attack. This integration represents a significant step toward comprehensive prevention of phishing and social engineering threats.

### **3.1.4 Security Orchestration, Automation, and Response (SOAR)**

Security Orchestration, Automation, and Response (SOAR) has emerged as a critical domain in AI-driven cybersecurity, addressing the overwhelming volume of security alerts that challenge human analysts (Pulyala et al., 2019). Traditionally, Security Information and Event Management (SIEM) systems were limited to aggregating logs and issuing alerts, often resulting in “alert fatigue” (Marri et al., 2024). SOAR builds upon this by incorporating AI to not only detect but also automate and accelerate the entire incident response lifecycle (Alliouche and Chenni, 2025). This shift reflects a broader movement in cybersecurity from passive detection toward proactive remediation, where malicious activity is identified and countered in near real time.

AI models have been applied to alert triage, where natural language and clustering techniques prioritise incidents based on severity and context (Seo et al., 2025). Machine learning also supports threat intelligence correlation, enabling the integration of diverse data streams such as malware feeds, dark web monitoring, and vulnerability databases to enhance situational awareness (Thaqi et al., 2025). In operational terms, SOAR platforms employ AI to execute automated response playbooks, including isolating compromised hosts, blocking malicious IP addresses, or resetting user credentials. These automated actions significantly reduce mean time to detect (MTTD) and mean time to respond (MTTR), key benchmarks in cyber defence performance (Nagar, 2024).

A promising frontier involves Reinforcement Learning (RL), where AI agents learn adaptive responsive strategies by interacting with simulated network environments (Blessing, 2024). Recent experiments suggest RL-based models can outperform static playbooks by tailoring responses dynamically to evolving threats (Wang et al., 2025). As a result, SOAR is increasingly recognised as an enabler of autonomous cyber defence, reducing human workload while strengthening organisational resilience against advanced threats.

## **3.2. Bibliometric Analysis**

The bibliometric data demonstrates that research on AI in cybersecurity has grown exponentially since 2015. From fewer annual publications in 2017, the number grew by 2024 (Saravanamuthu et al., 2025); this acceleration aligns with two converging factors: first, the rapid commercialisation of artificial intelligence technologies across industries; and second, the unprecedented rise in sophisticated cyberattacks such as ransomware, advanced persistent threats (APTs) and AI-enabled phishing campaigns (Ejjami, 2024). The sharpest increase occurred between 2021 and 2023, coinciding with breakthroughs in deep learning architectures and the global diffusion of generative AI (OECD, 2024). This period also saw the COVID-19 pandemic accelerate digitalisation, thereby expanding the attack surface and intensifying demand for automated cyber defence solutions (Reddy, 2024). For instance, a study by Kigbu and Ikemefuna (2025) focused on anomaly detection and malware classification, reflecting a paradigm shift toward adaptive, autonomous, and privacy-preserving AI.

Citation analysis confirms that research impact has also grown substantially. Papers published after 2020 are receiving citations at twice the rate of those from 2015-2017, reflecting both the timeliness and applied relevance of the research. This demonstrates that AI in cybersecurity has transitioned from a niche academic interest to a central theme within applied computer science and information security (Ofusori et al., 2024). Furthermore, bibliometric coupling and temporal keyword analysis reveal the evolution of thematic focus. Early publications emphasised “intrusion detection” and “span filtering”, whereas contemporary works highlight “federated learning”, “adversarial AI”, and “zero-trust architectures” (Gupta et al., 2020). This shift underscores a broader move away from traditional, rule-based defence toward an AI-centric paradigm emphasising resilience, adaptability, and explainability.

In sum, the growth trajectory of AI-driven cybersecurity publications reflects a field undergoing rapid expansion, shaped by real-world crises and technological breakthroughs. The data indicates not just a growing volume but also increasing sophistication and interdisciplinarity, suggesting the consolidation of AI cybersecurity as a mature and impactful research field.

# **4.0 Discussions**

The findings of this study highlight the transformative role of artificial intelligence in reshaping the cybersecurity landscape, with both the systematic review and bibliometric analysis revealing important patterns, challenges, and trajectories for future research. The four thematic domains identified – anomaly-based intrusion detection, automated malware analysis, phishing and social engineering prevention, and Security Orchestration, Automation, and Response (SOAR) – represent the core technical areas where AI has shown demonstrable impact. Collectively, these domains underscore a shift from static, rule-based detection toward adaptive, predictive, and autonomous defence mechanisms, mirroring the global surge in cyber threats and the evolution of AI technologies.

The dominance of anomaly-based intrusion detection systems (IDS) illustrates the field’s long-standing emphasis on network security. Consistent with their earlier studies, such as Ozkan-Ozay et al. (2024), the findings reaffirm that machine learning models – particularly tree-based classifiers – have provided effective, interpretable solutions, while deep learning techniques such as LSTMs and CNNs have raised detection accuracy against sophisticated attacks. This progression highlights an enduring tension in cybersecurity research: balancing interpretability and computational efficiency with the performance gains of more opaque deep models (Ejjami, 2024). The trajectory toward DL-based IDS suggests growing acceptance of black-box models, though the ethical and operational implications of this trend, particularly in high-stakes domains, remain a critical concern (Rane et al., 2024).

In malware analysis, the literature confirms a decisive move beyond signature-based detection, with CNN-driven visual malware classification and GANs-based augmentation representing novel contributions. The dual-use nature of GANs – as both a mechanism for generating undetectable malware and a defensive tool for training robust classifiers – raises profound ethical questions (Jones, 2025; Happiness and Song, 2025). Similar dualities have been observed in other security domains (Satibi and Atmi, 2024), suggesting that future research must address not only technical efficacy but also responsible governance frameworks. This is particularly relevant for UK institutions, where the integration of academic research with policy, as seen in the Global Cyber Security Capacity Centre, demonstrates the potential to influence international cybersecurity norms (UK Government, 2022).

Phishing and social engineering prevention reveal the growing interdisciplinarity of AI in cybersecurity, integrating natural language processing with behavioural analytics (Adu-Manu et al., 2022; Indranil Iyer, 2024). The move from SVM-based linguistic models to transformer-based architectures like BERT echoes broader trends in AI research, yet the literature highlights persistent challenges in reducing false positives and capturing evolving attack strategies (Jamal et al., 2023; Otieno et al., 2023). The integration of behavioural anomaly detection adds a second line of defence, yet it also raises privacy concerns when monitoring user activity, an issue that UK and EU contexts are particularly sensitive to under GDPR regulations (Williams and Charles Mbakwe-Obi, 2024; Bartolini et al., 2019). The emergence of SOAR reflects a maturing research agenda that goes beyond detection toward automation and resilience (Alliouche and Chenni, 2025). Reinforcement learning approaches, in particular, signify a paradigm shift toward adaptive, autonomous cyber defence. However, the literature also underscores the operational risks of delegating remediation to AI agents, including potential false remediations and adversarial manipulation (‌Ajala et al., 2024). Hence, it can be said that the bibliometric evidence that SOAR publications surged after 2021 suggests that the commercial adoption of such systems is already influencing research priorities.

The bibliometric analysis contextualises these thematic findings within a global research landscape. The exponential growth of publications confirms AI in cybersecurity as a rapidly consolidating discipline, with the UK playing a disproportionately influential role given its high citation impact (‌Marciano et al., 2025). This aligns with the presence of globally recognised research hubs which both produce cutting-edge research and shape policy debates. The concentration of research in the UK, US, and China, however, also reveals an uneven global distribution, with Africa and South America significantly under-represented. This imbalance raises concerns about global cyber resilience, as under-represented regions may lack access to locally relevant AI defence strategies. Overall, the discussion reveals a dual dynamic: AI enabling unprecedented accuracy, scalability, and automation in cybersecurity, yet it also introduces new risks, including adversarial misuse, ethical dilemmas, and regional inequalities in research capacity. Future research must therefore focus not only on technical innovation but also on explainability, governance, and equitable global participation to ensure that AI-driven cybersecurity evolves as a force for resilience rather than fragmentation.

# **5.0 Conclusion**

This study investigated the global trends in AI-driven cybersecurity by combining systematic literature review with bibliometric analysis, offering both qualitative and quantitative insights into the evolution of the field. The findings demonstrate that artificial intelligence is no longer a peripheral tool in cyber defence but has become a central driver of innovation, reshaping how threats are detected, analysed, and mitigated across diverse domains. The review identified four dominant application areas: anomaly-based intrusion detection, automated malware analysis, phishing and social engineering prevention, and Security Orchestration, Automation, and Response (SOAR). Each reflects a trajectory from traditional, rule-based models toward more adaptive, autonomous, and deep learning-based approaches. In particular, the growing success of LSTM networks, CNN-based visual malware detection, and transformer-driven phishing prevention highlight AI’s superior capacity to handle complexity, scale, and novel threats. At the same time, the rise of GANs and reinforcement learning illustrates both the creative promise and ethical dilemmas of AI in cybersecurity.

The bibliometric analysis confirmed that research on AI-driven cybersecurity has grown exponentially since 2015, with the sharpest rise between 2021 and 2023. This surge coincided with advances in deep learning, the global diffusion of generative AI, and the digitalisation boom brought on by COVID-19, which expanded attack surfaces and intensified demand for automated defences. Citation patterns further revealed that papers published after 2020 attract nearly double the citations of earlier works, reflecting their growing applied relevance. Thematic shifts were also evident, with the focus moving from intrusion detection and spam filtering toward federated learning, adversarial AI, and zero-trust architectures. These developments highlight the field’s evolution toward adaptive, resilient and explainable approaches, solidifying AI as central to cybersecurity’s future. Essentially, AI-driven cybersecurity has matured into a dynamic and globally impactful research area. Future progress, however, must balance technical innovation with ethical governance, explainability, and equitable global participation to ensure that the benefits of AI-powered defence extend beyond technological hubs to all regions vulnerable to cyber threats.

COMPETING INTERESTS DISCLAIMER:

Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

# **REFERENCES**

Adu-Manu, K.S., Ahiable, R.K., Appati, J.K. and Mensah, E.E. (2022). Phishing Attacks in Social Engineering: A Review. *Journal of Cyber Security*, 4(4), pp.239–267. Available at: https://doi.org/10.32604/jcs.2023.041095.

Ahmed, U. et al. (2025). Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. *Sci Rep,* 15 (1) p. 1726. Available at: 10.1038/s41598-025-85866-7.

‌Ajala, A., Okoye, C., None Onyeka Chrisanctus Ofodile, Arinze, A. and Daraojimba, D. (2024). Review of AI and machine learning applications to predict and thwart cyber-attacks in real-time. *Magna Scientia Advanced Research and Reviews*, 10(1), pp.312–320. Available at: https://doi.org/10.30574/msarr.2024.10.1.0037.

Albahri, O. S. and AlAmoodi, A. H. (2023). Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database. *Mesopotamian Journal of CyberSecurity*, pp. 158–169. Available at: 10.58496/MJCSC/2023/018

Alliouche, R. and Chenni, H. (2025). *Toward Intelligent Cyber Defense: A Comprehensive Study of SOAR Technologies for AI-Based DDoS Detection*. [online] Available at: https://www.researchgate.net/publication/394967622\_Toward\_Intelligent\_Cyber\_Defense\_A\_Comprehensive\_Study\_of\_SOAR\_Technologies\_for\_AI-Based\_DDoS\_Detection.

Baas, J., Schotten, M., Plume, A., Côté, G. and Karimi, R. (2020). Scopus as a curated, high-quality bibliometric data source for academic research in quantitative science studies. *Quantitative Science Studies*, 1(1), pp.377–386. Available at: https://doi.org/10.1162/qss\_a\_00019.

Bartolini, C., Lenzini, G. and Robaldo, L. (2019). The Data Protection Regulation Compliance Model. *IEEE Security & Privacy*. Available at: https://doi.org/10.1109/msec.2019.2937756.

‌Blessing, M. (2024). *Reinforcement Learning for Developing Adaptive Cryptocurrency Trading Strategies*. ResearchGate. Available at: https://www.researchgate.net/publication/384328579\_Reinforcement\_Learning\_for\_Developing\_Adaptive\_Cryptocurrency\_Trading\_Strategies.

Celik, Y., Basaran, E. and Goel, S. (2025). Deep Learning Methods for Intrusion Detection Systems on the CSE-CIC-IDS2018 Dataset: A Review. pp.38–65. Available at: https://doi.org/10.1007/978-3-031-89363-6\_3.

Clark, A. (2024). *Cybersecurity in the UK Summary 1 Understanding the cyber threat 2 Cybersecurity policy 3 Regulatory framework 4 Proposals for regulatory reform*. [online] Available at: https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf.

Devineni, K., Kathiriya, S. and Shende, A. (2023). Machine Learning-Powered Anomaly Detection: Enhancing Data Security and Integrity. *Journal of artificial intelligence & cloud computing*, pp.1–9. Available at: https://doi.org/10.47363/jaicc/2023(2)184.

‌Dey, S., Wasif, S., Tonmoy, D.S., Sultana, S., Sarkar, J. and Dey, M. (2020). A Comparative Study of Support Vector Machine and Naive Bayes Classifier for Sentiment Analysis on Amazon Product Reviews. *IEEE Xplore*. Available at: https://doi.org/10.1109/IC3A48958.2020.233300.

Ejjami, R. (2024). Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives. *Journal of Next-Generation Research 5.0*. [online] Available at: https://doi.org/10.70792/jngr5.0.v1i1.5.

Garousi, V., Felderer, M. and Mäntylä, M.V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, 106, pp.101–121. Available at: https://doi.org/10.1016/j.infsof.2018.09.006.

Goswami, M.J. (2024). *AI-Based Anomaly Detection for Real-Time Cybersecurity*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/381044167\_AI-Based\_Anomaly\_Detection\_for\_Real-Time\_Cybersecurity.

Gupta, R., Tanwar, S., Tyagi, S. and Kumar, N. (2020). Machine Learning Models for Secure Data Analytics: A taxonomy and threat model. *Computer Communications*, 153, pp.406–440. Available at: https://doi.org/10.1016/j.comcom.2020.02.008.

‌Happiness, O. and Song, M. (2025). *Generative Adversarial Networks (GANs) in Cybersecurity: Applications and Risks*. [online] Available at: https://www.researchgate.net/publication/390113712\_Generative\_Adversarial\_Networks\_GANs\_in\_Cybersecurity\_Applications\_and\_Risks.

Hassen, M., Carvalho, M.M. and Chan, P.K. (2017). *Malware classification using static analysis-based features*. [online] IEEE Xplore. Available at: https://doi.org/10.1109/SSCI.2017.8285426.

‌Indranil Iyer, K. (2024). Natural Language Processing for Phishing Detection: Leveraging AI to Spot Deceptive Content in Real Time. *International Journal of Current Science*, 14(4). Available at: https://doi.org/10.56975/ijcsp.v14i4.302418.

Islam, M.S. and Rahman, N. (2025). AI-Driven Fraud Detections in Financial Institutions: A Comprehensive Study. *Journal of Computer Science and Technology Studies*, 7(1), pp.100–112. Available at: https://doi.org/10.32996/jcsts.2025.7.1.8.

‌Ismail, H., Rio Guntur Utomo and Marastika Wicaksono Aji Bawono (2024). Comparison of Support Vector Machine and Random Forest Method on Static Analysis Windows Portable Executable (PE) Malware Detection. *Jurnal Media Informatika Budidarma*, 8(1), pp.154–154. Available at: https://doi.org/10.30865/mib.v8i1.7110.

Ismail, S. (2024). Threat Detection and Response Using AI and NLP in Cybersecurity*. Journal of Internet Services and Information Security*, 14 (1) pp. 195– 205. Available at: 10.58346/JISIS.2024.I1.013.

‌Jamal, S., Wimmer, H. and Sarker, I. (2023). An Improved Transformer-based Model for Detecting Phishing, Spam, and Ham: A Large Language Model Approach. *Research Square (Research Square)*. Available at: https://doi.org/10.21203/rs.3.rs-3608294/v1.

Javed, M.A., Anjum, M., Ahmed, H.A., Ali, A., Shahzad, H.M., Khan, H. and Alshahrani, A.M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. *Engineering Technology & Applied Science Research*, 14(6), pp.17894–17899. Available at: https://doi.org/10.48084/etasr.8619.

Jimmy, F. (2021). Emerging Threats: The Latest Cybersecurity Risks and the Role of Artificial Intelligence in Enhancing Cybersecurity Defenses. *International Journal of Scientific Research and Management (IJSRM),* 9 (02) pp. 564–574. Available at: 10.18535/ijsrm/v9i2.ec01.

‌Jones, R.K. (2025). Malware Analysis and Classification Using Deep Learning. *Advances in computational intelligence and robotics book series*, pp.165–200. Available at: https://doi.org/10.4018/979-8-3373-3296-3.ch006.

Kamboj, N.A., Ravindran, K. and Ojha, S. (2025). A Comparative Analysis of Signature-Based and Anomaly-Based Intrusion Detection Systems. *International Journal of Latest Technology in Engineering Management & Applied Science*, 14(5), pp.209–214. Available at: https://doi.org/10.51583/ijltemas.2025.140500026.

Kc, B., Shushant Sapkota and Adhikari, A. (2024). Generative Adversarial Networks in Anomaly Detection and Malware Detection: A Comprehensive Survey. *Advances in Artificial Intelligence Research*. Available at: https://doi.org/10.54569/aair.1442665.

Kigbu, S. and Ikemefuna, C. (2025). Enhancing malware detection using federated learning and explainable AI for privacy-preserving threat intelligence. *World Journal of Advanced Research and Reviews*, 27(1), pp.331–351. Available at: https://doi.org/10.30574/wjarr.2025.27.1.2541.

‌Kiger, J., Ho, S.-S. and Heydari, V. (2022). Malware Binary Image Classification Using Convolutional Neural Networks. *International Conference on Cyber Warfare and Security*, 17(1), pp.469–478. Available at: https://doi.org/10.34190/iccws.17.1.59.

Kinasih, A.N.S., Handayani, A.N., Ardiansah, J.T. and Damanhuri, N.S. (2024). Comparative analysis of decision tree and random forest classifiers for structured data classification in machine learning. *Science in Information Technology Letters*, [online] 5(2), pp.13–24. Available at: https://doi.org/10.31763/sitech.v5i2.1746.

Li, Y. and Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports,* 7, pp.8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

‌Liu, C. (2024). Long short-term memory (LSTM)-based news classification model. *PLOS ONE*, 19(5), p.e0301835. Available at: https://doi.org/10.1371/journal.pone.0301835.

‌Marciano, R., Nazareno, A., Ferreira, S., Miranda, R. and Coelho, G. (2025). Artificial intelligence and cybersecurity: a study of artificial intelligence in cybernetic defence. *ARACÊ*, [online] 7(5), pp.23155–23178. Available at: https://doi.org/10.56238/arev7n5-133.

Marri, R., Varanasi, S. and Kalidindi Chaitanya, S.V. (2024). Integrating Security Information and Event Management (SIEM) with Data Lakes and AI: Enhancing Threat Detection and Response. *Journal of Artificial Intelligence General science (JAIGS) ISSN:3006-4023*, 6(1), pp.151–165. Available at: https://doi.org/10.60087/jaigs.v6i1.239.

Mass.gov. (2024). Know the types of cyber threats. Available at: <https://www.mass.gov/info-details/know-the-types-ofcyber-threats>

Mienye, I.D., Swart, T.G. and Obaido, G. (2024). Recurrent Neural Networks: A Comprehensive Review of Architectures, Variants, and Applications. *Information*, [online] 15(9), p.517. Available at: https://doi.org/10.3390/info15090517.

Nagar, G. (2024). Leveraging Artificial Intelligence to Automate and Enhance Security Operations: Balancing Efficiency and Human Oversight. *International Journal of Scientific Research and Management (IJSRM)*, 6(07), pp.78–94. Available at: https://doi.org/10.18535/ijsrm/v6i7.ec05.

Ndubuisi, F. A. (2023). Strengthening national cybersecurity policies through coordinated threat intelligence sharing and real-time public-private collaboration frameworks. *International Journal of Science and Research Archive*, 8(2), pp.812–831. Available at: https://doi.org/10.30574/ijsra.2023.8.2.0299.

NHS England (2025). *NHS England» Artificial intelligence (AI) and machine learning*. [online] www.england.nhs.uk. Available at: https://www.england.nhs.uk/long-read/artificial-intelligence-ai-and-machine-learning/.

OECD (2024). *The Impact of Artificial Intelligence on Productivity, Distribution and Growth*. [online] Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/04/the-impact-of-artificial-intelligence-on-productivity-distribution-and-growth\_d54e2842/8d900037-en.pdf.

‌Ofusori, L., Bokaba, T. and Mhlongo, S. (2024). Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction. *Applied Artificial Intelligence*, 38(1). Available at: https://doi.org/10.1080/08839514.2024.2439609.

‌Otieno, D.O., Akbar Siami Namin and Jones, K.S. (2023). The Application of the BERT Transformer Model for Phishing Email Classification. *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, 3, pp.1303–1310. Available at: https://doi.org/10.1109/compsac57700.2023.00198.

Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I. and Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. *IEEE Access*, 12, pp.12229–12256. Available at: https://doi.org/10.1109/access.2024.3355547.

Patil, D., Rane, N.L., Desai, P. and Rane, J. (2024). Machine learning and deep learning: Methods, techniques, applications, challenges, and future research opportunities. *Trustworthy Artificial Intelligence in Industry and Society*. Available at: https://doi.org/10.70593/978-81-981367-4-9\_2.

Prima, B. and Bouhorma, M. (2020). Using Transfer Learning for Malware Classification. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences,* pp. 343–349. Available at: 10.5194/isprsarchives-XLIV-4-W3-2020-343-2020.

Pulyala, S., Desetty, A. and Jangampet, V. (2019). The Impact of Security Orchestration, Automation, and Response (SOAR) on Security Operations Center (SOC) Efficiency: A Comprehensive Analysis. *Turkish Journal of Computer and Mathematics Education*, 10(3), pp.1545–1549. Available at: https://doi.org/10.61841/turcomat.v10i3.14323.

Rahul, K. (2023). Strengthening Smart Grid Cybersecurity: An In-Depth Investigation into the Fusion of Machine Learning and Natural Language Processing. *Journal of Trends in Computer Science and Smart Technology*, 5 (3) pp. 284–301. Available at: 10.36548/jtcsst.2023.3.005

Rane, J., Kaya, Ö., Mallick, S.K. and Rane, N.L. (2024). Enhancing black-box models: Advances in explainable artificial intelligence for ethical decision-making. *Enhancing black-box models: Advances in explainable artificial intelligence for ethical decision-making*. Available at: https://doi.org/10.70593/978-81-981271-0-5\_4.

Reddy, C.S. (2024). Cyber Security in the COVID-19 Era: Challenges and Innovations in the Digital Transition. *Turkish Online Journal of Qualitative Inquiry*, pp.39–46. Available at: https://doi.org/10.53555/tojqi.v15i2.10380.

Saeed, S., Suayyid, S. A. Al-Ghamdi, M. S., AlMuhaisen, H. and Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors,* 23 (16) p. 7273. Available at: 10.3390/s23167273.

Saravanamuthu, M., Shaziya, S., Sadiqunnisa, P., Priya, N. K., Pathan, S. and Shajida, K. (2025). Artificial Intelligence in Cybersecurity: A Decade of Research Trends and Developments Through Bibliometric Analysis. *International Journal of Advanced Research in Computer Science*, 16(4), pp.42–46. Available at: https://doi.org/10.26483/ijarcs.v16i4.7298.

Satibi, I.F. and Atmi, R. (2024). Navigating The Duality: Privacy And Security Concerns in Knowledge Management Systems (KMS). *Internasional Journal of Data Science, Engineering, and Anaylitics*, 4(2), pp.1–14. Available at: https://doi.org/10.33005/ijdasea.v4i2.23.

Seo, J.W., Park, S.-J., Kim, Y.J., Kim, J.-Y., Kim, K.G. and Yoon, Y.-H. (2025). Artificial intelligence for severity triage based on conversations in an emergency department in Korea. *Scientific Reports*, [online] 15(1). Available at: https://doi.org/10.1038/s41598-025-99874-0.

Taofeek, A. (2025). *Machine Learning Models for Intrusion Detection Systems (IDS)*. [online] Available at: https://www.researchgate.net/publication/389263088\_Machine\_Learning\_Models\_for\_Intrusion\_Detection\_Systems\_IDS.

Thaqi, R., Krasniqi, B., Mazrekaj, A. and Rexha, B. (2025). Literature Review of Machine Learning and Threat Intelligence in Cloud Security. *IEEE Access*, 13, pp.11663–11678. Available at: https://doi.org/10.1109/access.2025.3529636.

Tomiyama, T., Wu, Q. and Kanai, A. (2023). Dynamic Analysis for Malware Detection Using API Calls and Memory Usage with Machine Learning Approach. Available at: https://doi.org/10.1109/gcce59613.2023.10315559.

UK Government (2022). *National Cyber Security Strategy 2022*. gov.uk. Available at: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022.

‌Wang, F., Li, S., Niu, S., Yang, H., Li, X. and Deng, X. (2025). A Survey on recent advances in reinforcement learning for intelligent investment decision-making optimization. *Expert Systems with Applications*, 282, p.127540. Available at: https://doi.org/10.1016/j.eswa.2025.127540.

Williams, M. and Charles Mbakwe-Obi, T. (2024). Once in a Blue Moon International Gift Gallery. *World Journal of Advanced Research and Reviews*, 2024(03), pp.1098–1115. Available at: https://doi.org/10.30574/wjarr.2024.24.3.3795.