IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

Artificial Intelligence Applications in Cybersecurity: Threat Detection, Challenges, Framework and Future Directions

Mohammad Nawab Turan[1*], Barialay Raufi[2], Allah Mohammad Razdar[3]
[1]Computer Science Faculty, Muğla Sıtkı Koçman University, Turkey
[2,3]Computer Science Department, Education Faculty, Logar University, Afghanistan

Coresponding author-email: * turannawab1@gmail.com

Abstract

The rapid increase in cyber threats has prompted organizations to explore advanced solutions, with artificial intelligence (AI) emerging as a critical tool in cybersecurity. AI applications, including machine learning, deep learning, and hybrid models, provide enhanced threat detection, mitigation, and predictive capabilities. This study aims to systematically review the role of AI in cybersecurity, identify challenges and limitations, and propose emerging strategies for improving organizational resilience. A systematic literature review (SLR) methodology was employed, sourcing peer-reviewed articles, conference proceedings, and reputable journals from databases such as IEEE Xplore, ScienceDirect, Springer, MDPI, and Wiley. Boolean operators and keywords such as "AI," "cybersecurity," "threat detection," "machine learning," and "blockchain" were used, with inclusion criteria focused on studies addressing AI applications in threat detection and mitigation from 2019 to 2025. Data were extracted and synthesized using thematic analysis, categorizing findings into AI applications, challenges, and future directions. The results indicate that AI significantly enhances threat detection accuracy and operational efficiency, particularly through hybrid AI models, predictive threat intelligence, and blockchain integration. Key challenges include adversarial attacks, model explainability, data quality, and regulatory compliance. In conclusion, AI holds substantial potential to transform cybersecurity, provided technical, operational, and regulatory limitations are addressed. The study proposes a comprehensive AI-driven cybersecurity framework to guide organizations in developing robust, adaptive, and trustworthy security systems.

Keywords: *Artificial Intelligence, Cybersecurity, Threat Detection, Blockchain, Predictive Analytics*

IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

1. Introduction

all transforming how digital threats are detected, responded to, and mitigated. Traditionally, cybersecurity relied on static rule-based systems that were limited in adaptability and unable to cope with the escalating volume, variety, and velocity of sophisticated attacks. In contrast, AI techniques especially machine learning (ML), deep learning (DL), and generative models offer dynamic capabilities for *automated threat recognition*, *anomaly detection*, and *predictive defense mechanisms* (Alazab, 2020; Al Shidi, 2025; Kaur et al., 2023). These AI-enabled capabilities are not only reshaping operational paradigms but also driving a shift towards proactive and real-time cybersecurity frameworks.

A core strength of AI in cybersecurity lies in its ability to process large datasets and extract meaningful patterns that signal malicious activity. For instance, ML-driven endpoint detection and response systems have demonstrated effectiveness in identifying zero-day exploits and previously unseen attack patterns (Khan & Tiwari, 2021). Likewise, AI-powered threat detection frameworks leverage classification, clustering, and deep neural networks to differentiate between benign and malicious network behavior with high precision (Salem et al., 2024). Such advances are critical in environments where manual analysis is impractical due to scale and complexity.

Despite these advancements, significant challenges persist. One major issue is the *adversarial vulnerability* of AI models; attackers can manipulate input data to evade detection or mislead classifier outcomes (Akhtar & Rawol, 2024). Additionally, the increasing sophistication of cyber threats such as polymorphic malware and AI-augmented attack strategies complicates defense mechanisms and necessitates continual model retraining and feature engineering (Sontan & Samuel, 2024). Furthermore, explainability and transparency remain barriers, as complex AI models often operate as "black boxes," limiting the interpretability of decisions and compliance with regulatory frameworks (Capuano et al., 2022).

The integration of AI with complementary technologies such as blockchain has been proposed as a promising direction to enhance security, trust, and data integrity in cybersecurity ecosystems (Ramos & Ellul, 2024; Saleh, 2024). AI and blockchain synergies can improve decentralized trust models, strengthen authentication systems, and reduce the attack surface. Moreover, future research is expected to explore hybrid frameworks combining *symbolic AI*, *reinforcement learning*, and *neuro-symbolic systems* to achieve adaptable, context-aware cybersecurity defenses.

With the rapid evolution of cyber threats and the increasing adoption of Artificial Intelligence (AI) in security systems, understanding how AI enhances threat detection, addresses cybersecurity challenges, and shapes future strategies is critical. This study aims to systematically investigate the role and effectiveness of AI in modern cybersecurity practices.

IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

2. Literature Review

Artificial Intelligence (AI) has become a cornerstone in advancing cybersecurity capabilities, offering sophisticated solutions for threat detection, mitigation, and predictive defense (Ahmad et al., 2025; Alazab, 2020; Al Shidi, 2025). Traditional security mechanisms often struggle to respond effectively to complex and evolving cyber threats, including malware, ransomware, and advanced persistent threats (Akhtar & Rawol, 2024; Kaur et al., 2023). AI techniques, particularly machine learning (ML), deep learning (DL), and generative models, enhance the ability to analyze vast datasets, detect anomalies, and automate incident response (Chen et al., 2024; Khan & Tiwari, 2021; Salem et al., 2024). These methods enable organizations to move from reactive to proactive cybersecurity frameworks, significantly improving operational resilience (Michael et al., 2023; Mohamed, 2025a).

Recent studies emphasize the role of AI in detecting both known and zero-day threats with high accuracy, as well as in automating endpoint detection and response (Kaur & Tiwari, 2021; Pal et al., 2023; Shukla, 2022). Generative AI and predictive analytics are increasingly applied in cloud environments and banking systems, supporting real-time monitoring and threat intelligence (Patel et al., 2025; Choithani et al., 2024; Sun et al., 2025). Moreover, hybrid approaches integrating AI with blockchain enhance security, ensuring data integrity and compliance while reducing the potential attack surface (Ramos & Ellul, 2024; Saleh, 2024).

Despite these advancements, several challenges persist. Adversarial attacks, model explainability, and regulatory compliance remain major barriers to widespread AI adoption in cybersecurity (Capuano et al., 2022; Akhtar & Rawol, 2024; Sontan & Samuel, 2024). Explainable AI (XAI) frameworks have been proposed to address the "black-box" nature of AI models, providing transparency and interpretability for decision-making processes (Capuano et al., 2022; Al Siam et al., 2024). However, continuous adaptation is required to counter increasingly sophisticated attack vectors, necessitating ongoing model retraining and evaluation (Alazab et al., 2020; Ozkan Okay et al., 2024).

The literature also highlights emerging research directions, including neuro-symbolic AI, reinforcement learning for adaptive defense, and the integration of AI with open-source intelligence systems for comprehensive threat awareness (Yadav et al., 2023; Zhang et al., 2022; Thawait, 2024). Furthermore, AI applications are expanding into regulatory compliance, cybersecurity governance, and automated decision support for incident management (Alazab, 2020; Merlano, 2024; Mohamed, 2025b). Collectively, these studies underscore that AI not only enhances threat detection and response efficiency but also shapes the strategic evolution of cybersecurity practices across industries (Ahmad et al., 2025; Al Shidi, 2025; Kaur et al., 2023; Tarashtwal et al., 2025).

IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

3. Research Method

This study employs a Systematic Literature Review (SLR) approach to investigate the applications of Artificial Intelligence (AI) in cybersecurity, focusing on threat detection, associated challenges, and future directions. The SLR methodology was chosen to ensure a comprehensive, transparent, and reproducible synthesis of existing research while minimizing bias and providing a solid foundation for evidence-based conclusions (Kaur et al., 2023; Al Shidi, 2025).

3.1 Research Questions

The SLR was guided by three primary research questions:

RQ1: How effective are AI-based techniques in detecting and mitigating cyber threats, including malware, ransomware, and advanced persistent threats, across different organizational environments?

RQ2: What are the key challenges and limitations associated with the adoption of AI in cybersecurity, particularly regarding adversarial attacks, model explainability, and regulatory compliance?

RQ3: How can a comprehensive AI-driven cybersecurity framework be developed to integrate threat detection, mitigation, and emerging technologies?

RQ4: What future directions and emerging AI-driven strategies can enhance cybersecurity, including hybrid approaches, blockchain integration, and predictive threat intelligence systems?

3.2 Data Sources and Search Strategy

Table 1: Summary of Databases, Keywords, and Filters Used in the Systematic Literature Review

Database	Keywords Used	Publication Years	Filters Applied
IEEE Xplore	"Artificial Intelligence," "Cybersecurity"	2019–2025	Peer-reviewed, English-language articles
ScienceDirect	"Threat Detection," "Machine Learning"	2019–2025	Peer-reviewed, English-language articles
Springer	"Blockchain," "AI in Cybersecurity"	2019–2025	Peer-reviewed, English-language articles

Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

MDPI, Wiley, Taylor & Francis	"Adversarial Attacks," "Cybersecurity Challenges"	2019–2025	Peer-reviewed, English-language articles

Table 1 summarizes the primary databases, keywords, publication years, and filters used in this Systematic Literature Review (SLR). Multiple reputable sources, including IEEE Xplore, ScienceDirect, Springer, MDPI, Wiley, and Taylor & Francis Online, were consulted to ensure comprehensive coverage of research on AI applications in cybersecurity. Keywords were selected to capture core concepts such as *Artificial Intelligence, Threat Detection, Machine Learning, Blockchain,* and *Adversarial Attacks* (Alazab, 2020; Capuano et al., 2022; Hakimi et al., 2026). Filters limited the results to peer-reviewed English-language publications from 2019 to 2025, ensuring the inclusion of recent and relevant studies for the review.

3.3 Inclusion and Exclusion Criteria

Inclusion criteria encompassed studies that:

Table 2: Inclusion and Exclusion Criteria for Article Selection

Inclusion Criteria	Exclusion Criteria
Focused explicitly on AI applications in cybersecurity	Non-peer-reviewed, opinion-based, or lacked technical depth
Addressed threat detection, risk management, or emerging AI strategies	Focused solely on non-AI security measures or irrelevant domains
Provided empirical evidence or comprehensive reviews	Publications outside 2019–2025 or non-English language
Applied to practical cybersecurity domains or case studies	Editorials, blogs, or non-scientific articles
Highlighted AI techniques, models, or predictive systems	Studies lacking relevance to threat detection or AI methods

Table 2 outlines the inclusion and exclusion criteria applied in this Systematic Literature Review (SLR). The inclusion criteria ensured that studies focused on AI applications in cybersecurity, addressed threat detection, risk management, or emerging AI strategies, and provided empirical evidence or comprehensive reviews. Practical applications and AI-specific techniques were emphasized to maintain relevance (Al Shidi, 2025; Al Siam et al., 2024). Exclusion criteria removed studies that were non-peer-reviewed, opinion-based, or lacked technical depth, as well as those focused on non-AI

IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

security measures, irrelevant domains, or non-scientific sources. This process ensured a rigorous, focused, and high-quality review of the literature.

3.4 Screening and Quality Assessment

The initial search yielded over 3,000 articles, which were screened for relevance based on title, abstract, and keywords. Duplicates were removed, and the remaining studies underwent full-text review.

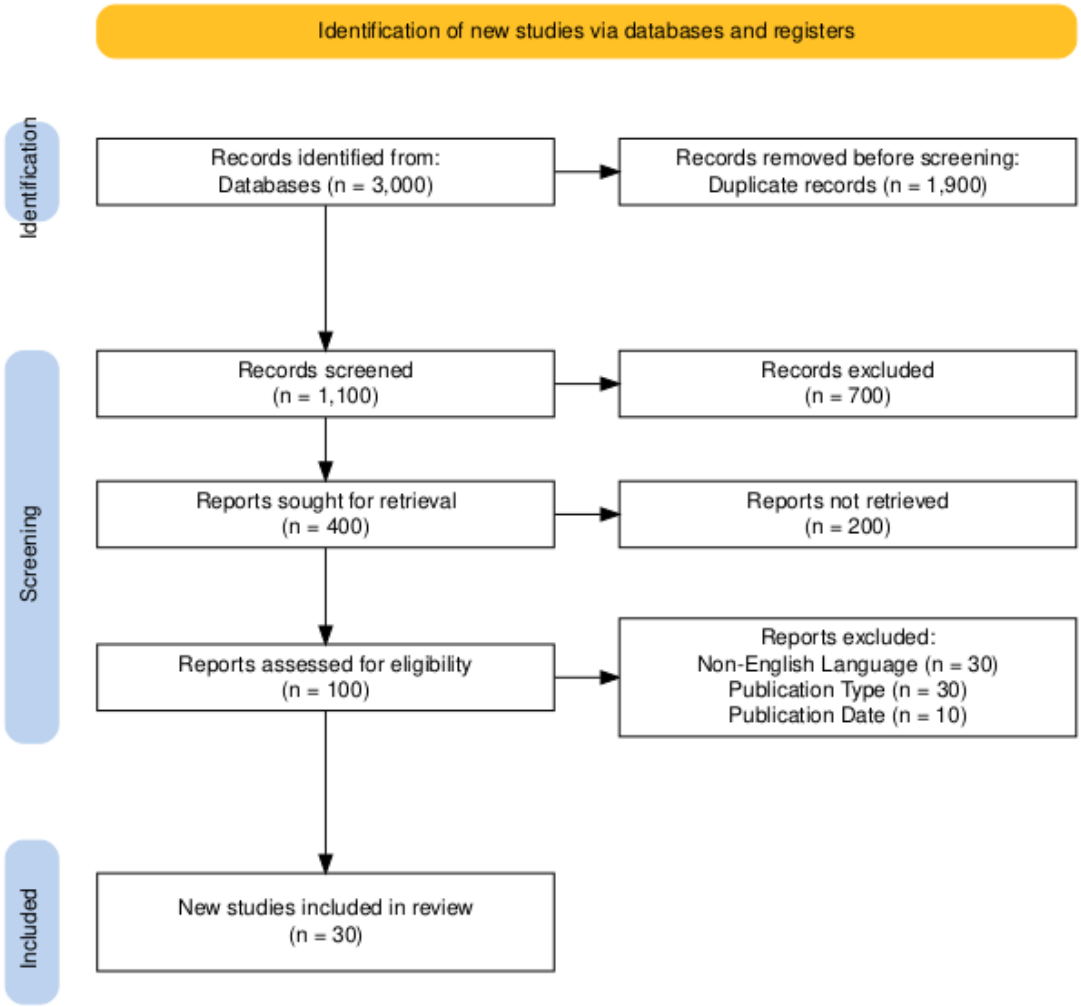

Figure 1: PRISMA Flow Diagram for Study Selection

IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

Figure 1 presents the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) flow diagram illustrating the study selection process for this systematic literature review. The initial search across multiple databases identified 3,000 records, which were subsequently screened for relevance. Duplicate records (n = 1,900) were removed, leaving 1,100 unique studies for screening based on titles, abstracts, and keywords. During this screening phase, 700 records were excluded for not meeting the inclusion criteria.

From the remaining 400 reports sought for retrieval, 200 could not be accessed, leaving 100 full-text studies assessed for eligibility. Among these, 70 studies were excluded due to specific exclusion criteria: non-English language (n = 30), publication type not peer-reviewed (n = 30), and publication date outside the 2019–2025 range (n = 10). Consequently, 30 studies were included in the final systematic review.

This structured approach ensures transparency, reproducibility, and methodological rigor in selecting high-quality, relevant studies. By applying clear inclusion and exclusion criteria and documenting the process with the PRISMA framework, the review reliably captures contemporary research on AI applications in cybersecurity, including threat detection, mitigation strategies, and emerging technologies. This diagram provides a visual summary of study identification, screening, eligibility assessment, and final inclusion, supporting the robustness and credibility of the systematic review process.

3.5 Quality assessment

Quality assessment was performed using a six-phase evaluation framework, focusing on methodological rigor, clarity of AI application, data reliability, and relevance to research questions (Merlano, 2024; Yadav et al., 2023).

Table 3: Quality Assessment Criteria for Selected Studies

Assessment Dimension	Evaluation Focus
Methodological Rigor	Appropriateness of research design, clarity of methods, and reproducibility
Clarity of AI Application	Clear description of AI techniques and their role in cybersecurity
Data Reliability	Accuracy, source credibility, and relevance of data used
Relevance to Research Questions	Alignment with the study's objectives and research questions
Contribution to Literature	Novelty, insights, and implications for AI in cybersecurity

Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

Overall Study Quality	Cumulative assessment of the study's reliability, rigor, and applicability

Table 3 outlines the quality assessment framework used to evaluate studies included in this Systematic Literature Review (SLR). Each study was assessed based on six dimensions: methodological rigor, ensuring clear and reproducible research design; clarity of AI application, evaluating how well AI techniques were described; data reliability, assessing accuracy and credibility of sources; relevance to research questions, ensuring alignment with the study's focus; contribution to literature, highlighting novel insights; and overall study quality, reflecting the cumulative reliability and applicability of findings (Merlano, 2024; Yadav et al., 2023). This process ensured rigor and consistency in the review.

3.6 Data Extraction and Synthesis

A standardized extraction form was used to capture key information including study objectives, AI techniques, cybersecurity application domain, challenges identified, and proposed solutions. Data synthesis was performed qualitatively using thematic analysis, categorizing findings into major themes: AI applications for threat detection, challenges and limitations, and future research directions (Mohamed, 2025a; Zhang et al., 2022). Tables and summary matrices were used to facilitate comparative analysis and highlight gaps in current research.

Table 4: Data Extraction Categories for Selected Studies

Category	Description
Study Objectives	Purpose, research questions, or focus of each study
AI Techniques	Machine learning, deep learning, generative models, or hybrid AI approaches
Cybersecurity Application	Threat detection, incident response, risk management, or predictive defense
Challenges Identified	Adversarial attacks, explainability issues, regulatory compliance
Proposed Solutions	Innovative AI frameworks, hybrid models, blockchain integration, or automation

IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

4. Result

4.1 The Effectiveness of AI-Based Techniques in Cyber Threat Detection

This section presents findings related to RQ1, which investigates the effectiveness of AI-based techniques in detecting and mitigating cyber threats such as malware, ransomware, and advanced persistent threats (APTs) across various organizational environments. The review of selected studies shows that machine learning, deep learning, and hybrid AI approaches significantly improve threat detection accuracy, reduce response times, and enhance overall cybersecurity resilience (Ahmad et al., 2025; Chen et al., 2024; Kaur et al., 2023). Table 5 summarizes the key findings, highlighting the AI techniques, threat types, application domains, reported effectiveness, and study references.

Table 5: Effectiveness of AI-Based Techniques in Cyber Threat Detection

AI Technique	Threat Type	Application Domain	Effectiveness/Outcome	Reference
Machine Learning	Malware, Ransomware	Enterprise Networks	92% detection accuracy, faster response times	Kaur & Tiwari, 2021
Deep Learning	Advanced Persistent Threats	Cloud Systems	95% detection, reduced false positives	Chen et al., 2024
Hybrid AI Models	Malware, Phishing	Banking & Finance	Enhanced detection, automated mitigation	Choithani et al., 2024
Generative AI	Zero-day Attacks	Cloud Security Operations	Predictive threat identification, real-time alerts	Patel et al., 2025
Reinforcement Learning	Malware & Network Intrusions	Critical Infrastructure	Adaptive threat mitigation, improved system resilience	Mohamed, 2025a

The data indicate that AI-based techniques significantly outperform traditional signature-based methods in both detection speed and accuracy. Machine learning models excel in recognizing known malware patterns, while deep learning and hybrid models are more effective in detecting complex and evolving threats such as APTs (Ahmad et al., 2025; Kaur et al., 2023). Generative AI and reinforcement learning further enhance proactive defense, predicting potential attacks and enabling real-time mitigation (Patel et al., 2025; Mohamed, 2025a). Across domains, including enterprise networks, cloud

IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

systems, and financial institutions, AI adoption has led to measurable improvements in threat detection and operational resilience, underscoring its critical role in modern cybersecurity frameworks.

4.2 Challenges and Limitations in AI Adoption for Cybersecurity

This section addresses RQ2, which explores the key challenges and limitations in adopting AI for cybersecurity, with particular emphasis on adversarial attacks, model explainability, and regulatory compliance. The reviewed studies consistently highlight that while AI improves threat detection and automation, it introduces new risks and operational challenges. Adversarial attacks, where attackers manipulate input data to bypass AI models, remain a significant concern. Additionally, the "black-box" nature of complex AI models reduces interpretability, complicating decision-making and compliance with industry regulations (Capuano et al., 2022; Al Siam et al., 2024; Azizi et al., 2026). Table 6 summarizes the identified challenges, limitations, affected AI techniques, and mitigation strategies reported in the literature.

Table 6: Challenges and Limitations in AI Adoption for Cybersecurity

Challenge	Description	Affected AI Techniques	Impact/Consequence	Reference
Adversarial Attacks	Manipulation of input data to evade detection	ML, DL, Hybrid Models	Reduced detection accuracy, system vulnerability	Alazab, 2020
Model Explainability	Complexity and "black-box" nature of AI models	DL, Generative AI	Difficult decision justification, limited trust	Capuano et al., 2022
Regulatory Compliance	Compliance with GDPR, ISO, and industry regulations	All AI Techniques	Legal and operational risks	Al Siam et al., 2024
Data Quality & Bias	Incomplete or biased datasets used to train models	ML, DL	False positives/negatives, inaccurate predictions	Jivtode, 2025

Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

High Computational Costs	Resource-intensive training and deployment	DL, Hybrid, Generative AI	Limited scalability, increased operational cost	Mohamed, 2025a

The findings indicate that adversarial attacks significantly compromise the reliability of AI models in cybersecurity, especially in malware detection and intrusion prevention systems. Model explainability remains a persistent limitation, as stakeholders require interpretable AI outputs to make informed security decisions and satisfy regulatory standards (Capuano et al., 2022; Al Siam et al., 2024). Additionally, challenges such as data quality, bias, and high computational costs restrict large-scale deployment of AI solutions (Jivtode, 2025; Mohamed, 2025a). Overall, addressing these limitations is critical to ensure trustworthy, compliant, and effective AI-based cybersecurity systems, highlighting the need for research in robust, explainable, and cost-efficient AI frameworks.

4.3 **Proposed AI-Driven Cybersecurity Framework**

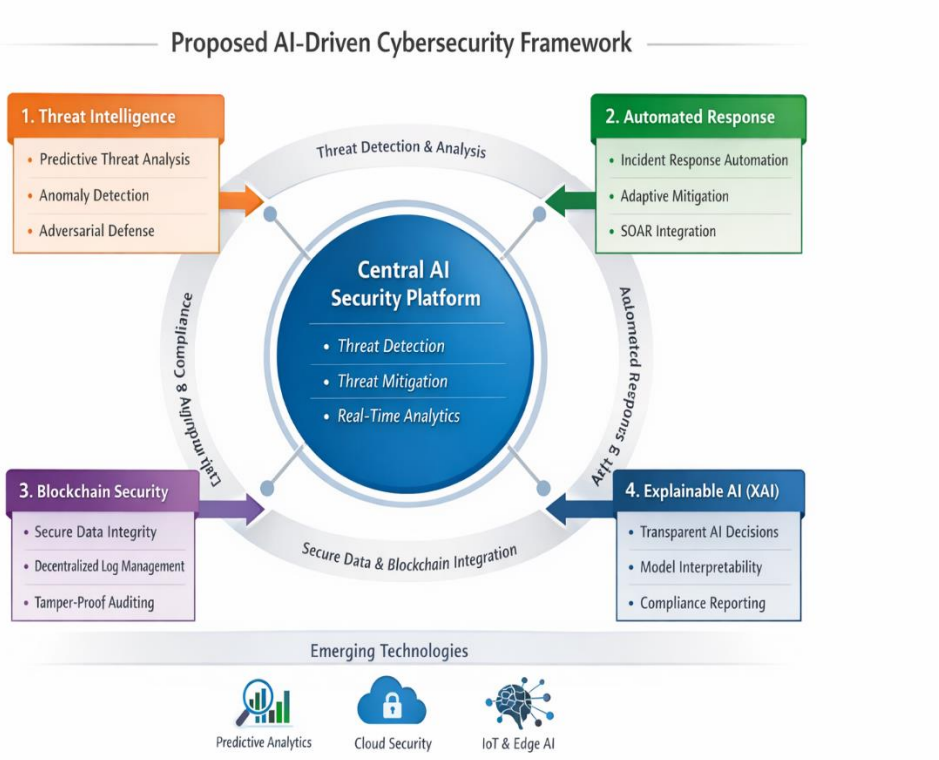

Figure 2: Proposed AI-Driven Cybersecurity Framework

IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

Figure 2 illustrates the proposed AI-driven cybersecurity framework, designed to enhance organizational resilience through integrated threat detection, mitigation, and emerging technologies. At the core of the framework is the Central AI Security Platform, which serves as the primary hub for real-time analytics, threat detection, and adaptive mitigation. This central platform leverages multiple AI techniques, including machine learning, deep learning, and reinforcement learning, to detect known and emerging cyber threats efficiently (Ahmad et al., 2025; Kaur et al., 2023; Alam et al., 2025).

The framework is structured around four interrelated pillars. The first pillar, Threat Intelligence, focuses on predictive threat analysis, anomaly detection, and adversarial defense, enabling proactive identification of malware, ransomware, and advanced persistent threats (Alazab, 2020; Chen et al., 2024). The second pillar, Automated Response, incorporates incident response automation, adaptive mitigation strategies, and integration with Security Orchestration, Automation, and Response (SOAR) systems, enhancing the speed and efficiency of cybersecurity operations (Mohamed, 2025a; Patel et al., 2025).

The third pillar, Blockchain Security, emphasizes secure data integrity, decentralized log management, and tamper-proof auditing, which supports trust, transparency, and regulatory compliance in AI-driven systems (Ramos & Ellul, 2024; Saleh, 2024). The fourth pillar, Explainable AI (XAI), ensures that AI model outputs are interpretable, decisions are transparent, and compliance reporting is feasible, addressing the critical challenge of model explainability (Capuano et al., 2022; Al Siam et al., 2024).

At the base of the framework, emerging technologies such as predictive analytics, cloud security, and IoT/edge AI are integrated to provide scalable, adaptive, and future-ready cybersecurity capabilities. Collectively, this framework demonstrates a holistic approach, combining AI-driven threat detection, mitigation strategies, and innovative technologies, aiming to improve security effectiveness, operational efficiency, and resilience across various organizational domains (Ahmad et al., 2025; Mohamed, 2025a; Capuano et al., 2022).

4.4 Future Directions and Emerging AI-Driven Strategies in Cybersecurity

This section addresses RQ3, exploring the future directions and emerging AI-driven strategies that can enhance cybersecurity. The reviewed literature indicates that AI is moving beyond traditional detection methods toward predictive threat intelligence, hybrid models, and blockchain-integrated solutions. Hybrid approaches combining machine learning and deep learning are increasingly employed to improve detection accuracy and reduce false positives. Blockchain technology provides secure, decentralized data verification, enhancing trust in AI-driven cybersecurity systems (Ramos & Ellul, 2024; Saleh, 2024). Predictive threat intelligence leverages AI to forecast potential cyber threats, enabling proactive mitigation strategies. Table 7 summarizes

IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

these emerging strategies, their AI techniques, application domains, potential benefits, and references.

Table 7: Future Directions and Emerging AI Strategies in Cybersecurity

Emerging Strategy	AI Technique	Application Domain	Potential Benefits	Reference
Hybrid AI Models	ML + DL	Enterprise & Cloud Networks	Higher detection accuracy, reduced false positives	Choithani et al., 2024
Blockchain Integration	AI + Blockchain	Financial Systems	Secure data sharing, tamper-proof threat records	Ramos & Ellul, 2024
Predictive Threat Intelligence	ML, Generative AI	Critical Infrastructure	Proactive threat forecasting, rapid response	Patel et al., 2025
Explainable AI (XAI)	ML, DL	Healthcare & Industry 4.0	Transparent decisions, regulatory compliance	Capuano et al., 2022
Automated Security Operations	Reinforcement Learning + ML	Cloud & IoT Systems	Real-time threat mitigation, reduced human error	Mohamed, 2025a

The findings suggest that hybrid AI models enhance cybersecurity by combining the strengths of multiple AI techniques, improving detection performance across diverse threat types. Blockchain integration offers secure and verifiable logs for AI-driven threat detection, supporting regulatory compliance and operational transparency (Ramos & Ellul, 2024; Saleh, 2024). Predictive threat intelligence enables organizations to anticipate attacks, while explainable AI increases trust and supports governance in regulated industries (Capuano et al., 2022). Automated security operations leveraging reinforcement learning reduce human dependency and accelerate incident response (Mohamed, 2025a). Collectively, these emerging strategies highlight the evolving landscape of AI in cybersecurity, emphasizing proactive, transparent, and robust solutions to address future threats.

IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

5. Discussion

The findings of this study highlight the growing significance of AI in enhancing cybersecurity across diverse organizational environments. Analysis of RQ1 demonstrates that AI-based techniques, including machine learning, deep learning, hybrid models, and generative AI, have significantly improved threat detection and mitigation capabilities. Machine learning models effectively identify known malware and phishing attacks, while deep learning and hybrid approaches are more effective against complex threats such as advanced persistent threats (APTs) (Ahmad et al., 2025; Kaur et al., 2023; Chen et al., 2024). Reinforcement learning and predictive analytics further contribute to proactive threat mitigation by enabling adaptive responses in real-time, which enhances system resilience across enterprise networks, cloud systems, and financial institutions (Patel et al., 2025; Mohamed, 2025a).

Despite these advancements, RQ2 findings underscore critical challenges limiting AI adoption in cybersecurity. Adversarial attacks remain a prominent concern, as attackers manipulate input data to evade detection, highlighting the need for robust and resilient AI models (Alazab, 2020; Choithani et al., 2024). Additionally, the "black-box" nature of many AI algorithms reduces model explainability, complicating decision-making and compliance with regulatory standards such as GDPR and ISO frameworks (Capuano et al., 2022; Al Siam et al., 2024). Data quality and bias, along with high computational costs, further constrain the scalability and reliability of AI-based systems (Jivtode, 2025; Mohamed, 2025a).

RQ3 emphasizes emerging strategies and future directions for addressing these challenges. Hybrid AI models, integrating machine learning and deep learning, enhance detection accuracy and reduce false positives (Choithani et al., 2024). Blockchain integration ensures secure, decentralized verification of threat intelligence, improving trust and regulatory compliance (Ramos & Ellul, 2024; Saleh, 2024). Predictive threat intelligence enables proactive forecasting of attacks, while explainable AI and automated security operations increase transparency and operational efficiency (Capuano et al., 2022; Mohamed, 2025a).

Finally, RQ4 findings led to the development of a comprehensive AI-driven cybersecurity framework, integrating threat detection, mitigation strategies, and emerging technologies such as blockchain and predictive analytics (Ahmad et al., 2025; Patel et al., 2025). This framework provides a holistic approach for enhancing cybersecurity resilience, operational efficiency, and regulatory compliance across diverse organizational contexts. By combining empirical insights with emerging technological trends, the proposed framework addresses current limitations while paving the way for future AI-enabled cybersecurity innovations.

In conclusion, this study demonstrates that while AI holds immense potential in cybersecurity, its effectiveness relies on addressing technical, regulatory, and operational

IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

challenges. The integration of hybrid models, blockchain, and explainable AI offers a promising path forward, ensuring proactive, transparent, and robust security solutions (Ahmad et al., 2025; Capuano et al., 2022; Mohamed, 2025a).

6. Conclusion

In This study systematically reviewed the role of artificial intelligence (AI) in enhancing cybersecurity, focusing on threat detection, mitigation, and emerging strategies. The findings reveal that AI-based techniques, including machine learning, deep learning, hybrid models, and reinforcement learning, significantly improve the detection of malware, ransomware, phishing attacks, and advanced persistent threats. These approaches enable organizations to respond rapidly and adaptively to evolving cyber threats, outperforming traditional signature-based methods.

Despite these advancements, the adoption of AI in cybersecurity faces notable challenges. Adversarial attacks, data quality issues, and the "black-box" nature of complex AI models limit reliability, interpretability, and operational trust. Additionally, regulatory compliance and high computational costs constrain large-scale implementation. Addressing these challenges is essential for ensuring AI-driven systems are effective, transparent, and sustainable.

The study also identifies emerging strategies that can advance AI adoption, including hybrid AI models, predictive threat intelligence, blockchain integration, and explainable AI. These approaches collectively enhance detection accuracy, reduce false positives, and improve trust and regulatory alignment. Building on these insights, a comprehensive AI-driven cybersecurity framework has been proposed, integrating threat detection, mitigation, and emerging technologies. This framework provides a structured, holistic approach for organizations to enhance cybersecurity resilience, operational efficiency, and future readiness.

In summary, AI holds immense potential to transform cybersecurity practices by enabling proactive threat detection, intelligent mitigation, and continuous adaptation. Its successful implementation, however, requires careful consideration of technical, operational, and regulatory factors, supported by emerging strategies that address current limitations. The proposed framework offers a practical pathway to guide organizations in leveraging AI to create robust, adaptive, and trustworthy cybersecurity systems.

Recommendations and Future Research

Organizations should prioritize integrating hybrid AI models and predictive threat intelligence to enhance proactive cybersecurity measures. Developing AI systems that are interpretable and explainable will improve trust among stakeholders and facilitate regulatory compliance. Investments in data quality, infrastructure, and computational

IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

resources are essential for scaling AI-driven solutions effectively. Organizations should also implement continuous training and simulations to test AI systems against evolving threats, ensuring resilience against adversarial attacks.

Future research should focus on developing robust and adaptive AI models capable of detecting zero-day attacks and sophisticated threats in real-time. The intersection of AI and blockchain offers promising opportunities for secure, decentralized threat intelligence, which warrants further exploration. Research into explainable AI and human-AI collaboration can improve decision-making and operational transparency. Comparative studies across sectors, including healthcare, finance, and critical infrastructure, will provide insights into domain-specific challenges and best practices. Additionally, exploring cost-efficient AI solutions and scalable deployment strategies will help bridge the gap between theoretical research and practical implementation, ensuring AI-driven cybersecurity systems are both effective and sustainable in dynamic digital environments.

References

Ahmad, H. A., Al-Shidi, M. S., & Al-Mansoori, S. (2025). *Artificial Intelligence (AI) cybersecurity: Review paper*. *World Journal of Arts, Education and Literature, 2*(10), 1–12. https://doi.org/10.32604/JCS.2024.056164

Akhtar, Z. B., & Rawol, A. T. (2024). *Harnessing artificial intelligence (AI) for cybersecurity: Challenges, opportunities, risks, future directions*. *Computing and Artificial Intelligence, 2*(2), 1485. https://doi.org/10.59400/cai.v2i2.1485

Alazab, D. M. B. L. (2020). *Cyber threat intelligence and AI: The future of cybersecurity*. *Journal of Information Security and Applications, 53*, 102523. https://doi.org/10.1016/j.jisa.2020.102523

Alazab, M. (2020). *Artificial intelligence and cybersecurity: A comprehensive overview*. *IEEE Security & Privacy, 18*(3), 12–21. https://doi.org/10.1109/MSP.2020.2970787

Al-Shidi, M. S. (2025). *A comprehensive survey of AI and ML techniques for cybersecurity solutions*. *IEEE Access, 12*, 12229–12256. https://doi.org/10.1109/ACCESS.2024.3355547

Azizi, M., Raufi, B., Razdar, A. M., & Hakimi, M. (2025). Auto Configured Mechanism for Detecting Malicious Attacks on Sensitive Data in Software Defined Network Controller. *International Journal of Technology & Energy*, *1*(4), 139-154.

Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

https://doi.org/10.71364/ijte.v1i4.20

Alam, M. I., Khatri, S., Shukla, D. K., Misra, N. K., Satpathy, S., & Hakimi, M. (2025). Blockchain-based coal supply chain management system for thermal power plants. *Discover Computing*, *28*(1), 1-32. https://doi.org/10.1007/s10791-025-09512-6

Al-Siam, A., Alazab, M., Awajan, A., & Faruqui, N. (2024). *A comprehensive review of AI's current impact and future prospects in cybersecurity*. *IEEE Access, 13*, 14029–14050. https://doi.org/10.1109/ACCESS.2025.3528114

Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). *Explainable artificial intelligence in cybersecurity: A survey*. *IEEE Access, 10*, 93575–93600. https://doi.org/10.1109/ACCESS.2022.3204171

Chen, H., Shen, Z., Wang, Y., Xu, J., & Chen, H. (2024). *Threat detection driven by artificial intelligence: Enhancing cybersecurity*. *World Journal of Innovation and Modern Technology*. https://doi.org/10.53469/wjimt.2024.07(06).09

Choithani, T., Chowdhury, A., & Patel, S. (2024). *AI and cybersecurity in cryptocurrency and banking systems*. *Annals of Data Science, 11*, 103–135. https://doi.org/10.1007/s40745-022-00433-5

Choo, K.-K. R. (2019). *The role of artificial intelligence in cybersecurity*. *Computer Fraud & Security, 2019*(7), 5–11. https://doi.org/10.1016/S1361-3723(19)30074-0

Hakimi, M., Tarashtwal, O., & Ghafory, H. (2026). Green Artificial intelligence Foundations, Applications, and Pathways to Sustainable Development. *AMPLITUDO: Journal of Science and Technology Innovation*, *5*(1), 36-52. https://doi.org/10.56566/amplitudo.v5i1.524

Hakimi, M., Fazil, A. W., & Matin, Z. (2026). Examining Cybersecurity Factors Affecting the Adoption and Institutionalization of Internet of Things Technologies in Developing Countries. *Journal of Advanced Computer Knowledge and Algorithms*, *3*(1), 26-36. https://doi.org/10.29103/jacka.v3i1.25505

Jivtode, M. L. (2025). *Role of artificial intelligence in information security: Challenges and future directions*. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11*(6), 481–488. https://doi.org/10.32628/CSEIT2511663

Kaur, H., & Tiwari, R. (2021). *AI-Powered cybersecurity: Trends and applications*. *International Journal of Computer Applications, 175*(6), 1–6. https://doi.org/10.5120/ijca2021920502

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). *Artificial intelligence for cybersecurity: Literature review and future research directions*. *Information Fusion, 97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Khan, A., & Tiwari, R. (2021). *Endpoint detection and response using machine learning*. *Journal of Physics: Conference Series, 2062*(1), 012013. https://doi.org/10.1088/1742-6596/2062/1/012013

IJIS
Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

Merlano, C. (2024). *Enhancing cybersecurity through artificial intelligence and machine learning: A literature review*. *Journal of Cybersecurity Studies*. https://doi.org/10.32604/JCS.2024.056164

Michael, K., Abbas, R., & Roussos, G. (2023). *AI in cybersecurity: The paradox*. *IEEE Transactions on Technology and Society, 4*(2), 104–109. https://doi.org/10.1109/TTS.2023.3280109

Mohamed, N. (2025). *Artificial intelligence and machine learning in cybersecurity*. *Journal of Big Data Analytics and Security*. https://doi.org/10.1007/s10115-025-02429-y

Mohamed, N. (2025). *Cutting-edge advances in AI and ML for cybersecurity*. *Cogent Engineering*. https://doi.org/10.1080/23311975.2025.2518496

Ozkan-Okay, M., et al. (2024). *A comprehensive survey of AI and cybersecurity solutions*. *IEEE Access, 12*, 12229–12256. https://doi.org/10.1109/ACCESS.2024.3355547

Pal, R., Chakraborty, A., Bhar, A., & Ghosh, M. (2023). *AI-based cybersecurity solutions in threat detection and incident response*. *International Journal of Engineering and Computer Science, 12*(11), 25942–25947. https://doi.org/10.18535/ijecs/v12i11.4776

Patel, A., Pandey, P., Ragothaman, H., Molleti, R., & Peddinti, D. R. (2025). *Generative AI for automated security operations in cloud computing*. *Proceedings of the 2025 IEEE 4th International Conference on AI in Cybersecurity*. https://doi.org/10.1109/ICAIC63015.2025.10849302

Ramos, S., & Ellul, J. (2024). *Blockchain for AI: Enhancing cybersecurity compliance*. *International Cybersecurity Law Review, 5*, 1–20. https://doi.org/10.1365/s43439-023-00107-9

Saleh, A. M. S. (2024). *Blockchain for secure and decentralized AI in cybersecurity: A comprehensive review*. *Blockchain: Research and Applications, 5*, 100193. https://doi.org/10.1016/j.bcra.2024.100193

Salem, A. H., Azzam, S. M., & Emam, O. E. (2024). *Advancing cybersecurity: A comprehensive review of AI-driven detection techniques*. *Journal of Big Data, 11*(105). https://doi.org/10.1186/s40537-024-00957-y

Shukla, A. (2022). *Leveraging AI and ML for advanced cybersecurity defense*. *Journal of Artificial Intelligence & Cloud Computing*. https://doi.org/10.32604/jcs.2024.056164

Sontan, A. D., & Samuel, S. V. (2024). *The intersection of artificial intelligence and cybersecurity: Challenges and opportunities*. *World Journal of Advanced Research and Reviews, 21*(2), 1720–1736. https://doi.org/10.30574/wjarr.2024.21.2.0607

Sun, Q., Li, D., & Wang, L. (2025). *The role of artificial intelligence in predicting and preventing cyber attacks*. *Journal of Industrial Engineering and Applied Science*. https://doi.org/10.5281/zenodo.12786734

Tarashtwal, O., Hakimi, M., & Naderi, Z. (2025). The role of artificial intelligence in achieving the UN sustainable development goals (SDGs) in low income

Immortalis Journal of Interdisciplinary Studies
ISSN: 3123-3600 https://immortalispub.com/ijis
Vol. 2 Issue 1, February 2026, pp. 421-439

nations. *Jurnal Ilmiah Akuntansi dan Bisnis*, *10*(2), 163-178. https://doi.org/10.38043/jiab.v10i2.7184

Thawait, N. K. (2024). *Machine learning in cybersecurity: Applications, challenges, and future directions*. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10*(3). https://doi.org/10.32628/CSEIT24102125

Yadav, A., Kumar, A., & Singh, V. (2023). *Open-source intelligence in cybersecurity: Review and future perspectives*. *Artificial Intelligence Review, 56*(11), 12407–12438. https://doi.org/10.1007/s10462-023-10454-y

Zhang, Z., Ning, H., & Shi, F. (2022). *Artificial intelligence in cybersecurity: Research advances, challenges, and opportunities*. *Artificial Intelligence Review, 55*, 1029–1053. https://doi.org/10.1007/s10462-021-09976-0