"Artificial Intelligence for Next-Generation Cyber-security – Adaptive Threat Detection and Automated Response System

***Shivam Maithani**
****Prof. Y.P. Raiwani**

Abstract

The digital transformation of modern infrastructures has amplified both the complexity of networks and the sophistication of cyber attacks. Traditional rule-based and signature-driven security systems are increasingly inadequate, generating high false positives and lagging in response times. This paper investigates the role of artificial intelligence (AI) in advancing threat detection and incident response capabilities. Through a comprehensive literature review and comparative analysis of machine learning (ML), deep learning (DL), reinforcement learning (RL), and explainable AI (XAI) approaches, the study evaluates how AI-based models improve detection accuracy, reduce false alerts, and enable near real-time automated responses. Case studies of enterprise solutions such as Darktrace, IBM QRadar, and Microsoft Sentinel are examined to illustrate practical implementations. The research further explores applications across enterprise networks, IoT ecosystems, cloud computing, healthcare, and defense, while critically addressing challenges including adversarial AI, privacy, cost, and transparency. The expected outcomes highlight AI's transformative potential in enabling predictive threat intelligence, scalable automated defense, and resilient cybersecurity infrastructures. By providing a framework for technical adoption and ethical considerations, this paper contributes actionable insights toward building sustainable and adaptive cyber defense ecosystems.

Keywords: Machine Learning, Deep Learning, Reinforcement Learning, Explainable AI, Darktrace, IBM QRadar.

I. Introduction

The accelerated digitization of global economies has transformed cybersecurity risks, creating a shifting battlefield between attackers and defenders through expanded cloud, IoT, and smart technology surfaces. Modern threats—organized, persistent, and AI-leveraged—outpace traditional defenses, with ransomware, DDoS, and APTs exposing legacy systems' inadequacies (Salem, Azzam, Emam, & Abohany, 2024; Nguyen, Truong, & Lee, 2024; Roy, Li, & Bai, 2024).

Traditional systems rely on signature-based detection, failing against unknown threats, generating false positives, alert fatigue, and struggling with high-volume or encrypted data—leading to delayed responses and severe consequences (Sajid, Aldeer, Al-Haj, & Hasan, 2024; Chen, Guo, & Zhao, 2024; Im, Ahn, & Kim, 2024).

AI reshapes defense via machine learning, deep learning for dynamic patterns, SIEM/SOAR integration for real-time response, reinforcement learning for adaptive strategies, and explainable AI for interpretability—marking a paradigm shift to proactive security (Arreche, Guntur, & Abdallah, 2024; Fatema & Chowdhury, 2025; Yang, Pang, Zhang, & Zhao, 2024; Al-Khalidi & Al-Kuwari, 2024).

Research gaps remain in practical deployment amid adversarial attacks, privacy, resources, and regulatory needs across healthcare, finance, and infrastructure. This study bridges them by probing AI's role in detection accuracy, automated response, predictive intelligence, and challenges like trust and sustainability for resilient ecosystems (Bensaid, Labraoui, Abba Ari, Saidi, Mboussam Emati, & Maglaras, 2024; Bella et al., 2024)

II. Literature Review

Traditional intrusion detection relied on static rule-based monitoring and signature recognition of known attack patterns, which flagged network anomalies but became outdated against polymorphic code, encryption, and dynamic strategies. These systems struggled with growing digital traffic volumes, generating excessive false positives that diluted effectiveness and exposed organizations to zero-day exploits due to their reactive nature and inability to adapt quickly (Sajid, Aldeer, Al-Haj, & Hasan, 2024; Chen, Guo, & Zhao, 2024).

AI techniques overcame this rigidity: machine learning (ML) enabled classification of malicious/benign traffic from historical data without predefined variants; deep learning (DL) extracted complex hierarchical features from raw network data for precise stealth attack detection (Kimanzi, Mugo, & Muange, 2024); reinforcement learning (RL) provided adaptive, proactive responses through dynamic environment interaction (Yang, Pang, Zhang, & Zhao, 2024); and explainable AI (XAI) resolved black-box issues with interpretable outputs for analyst/regulator trust and compliance (Arreche, Guntur, & Abdallah, 2024; Fatema & Chowdhury, 2025).

AI integrates with SIEM (centralized log correlation) and SOAR (automated responses) platforms like IBM QRadar and Microsoft Sentinel to detect subtle patterns, automate workflows, and scale across distributed networks/cloud ecosystems (Al-Khalidi & Al-Kuwari, 2024). Recent reviews confirm AI's superior accuracy/false positive reduction but highlight gaps in generalization, adversarial robustness, IoT resource constraints, healthcare privacy-performance balance, and large-scale deployment—necessitating research for reliable global cyber defense transition (Salem et al., 2024;

Wang et al., 2025; Bella et al., 2024; Bensaid et al., 2024).

III. Problem Statement

The rapid evolution of cyber threats has fundamentally altered the security landscape, with attacks becoming increasingly sophisticated, targeted, and resilient against conventional defenses. One of the most pressing challenges is the emergence of zero-day exploits, which take advantage of previously unknown vulnerabilities before patches are available. These attacks bypass traditional signature-based systems, as no prior record exists to flag the intrusion. Similarly, polymorphic malware, capable of altering its code structure with each iteration, avoids detection by legacy mechanisms that rely on static patterns (Gueriani, Sebbar, Zervos, & Nachi, 2024). Compounding these developments is the use of adversarial machine learning, where attackers deliberately manipulate inputs to deceive AI-driven systems into misclassification, effectively turning advanced defense mechanisms into new points of vulnerability (Yang, Pang, Zhang, & Zhao, 2024). As digital infrastructures expand across cloud platforms, IoT networks, and critical infrastructure, the velocity and unpredictability of such threats present risks that static and rule-based solutions are unable to address (Bella et al., 2024).

Alongside the sophistication of attacks, legacy intrusion detection and prevention systems struggle with the persistent problem of false positives. These systems often flag benign anomalies as threats due to their reliance on rigid rules and predefined signatures. The result is a flood of alerts, many of which are irrelevant, leading to what is commonly described as alert fatigue. Security analysts face the daunting task of sifting through massive volumes of data, which not only diverts attention from genuine threats but also delays the investigation of high-risk incidents (Sajid, Aldeer, Al-Haj, & Hasan, 2024). The inability of such systems to contextualize and prioritize alerts undermines the efficiency of security operations, especially in environments characterized by high traffic or encrypted communication (Chen, Guo, & Zhao, 2024). Consequently, organizations risk missing critical intrusions hidden among the noise, increasing their vulnerability to large-scale compromises (Roy, Li, & Bai, 2024).

IV. Research Objectives

In light of these challenges, the overarching objective of this research is to investigate the potential of artificial intelligence to strengthen detection and response systems against evolving cyber threats. The first aim is to enhance detection accuracy by leveraging machine learning and deep learning models. Unlike rule-based systems, these approaches can analyze large datasets, extract complex features, and recognize subtle patterns, thereby reducing false positives and identifying threats that evade conventional detection (Kimanzi, Mugo, & Muange, 2024; Arreche, Guntur, & Abdallah, 2024).

The second objective focuses on automating incident response through reinforcement learning-based

models. Reinforcement learning enables systems to dynamically adapt response strategies based on the evolving characteristics of attacks, reducing reliance on human intervention and significantly decreasing mean time to response. This capability allows for more consistent and scalable defense mechanisms in large and complex environments (Hu, Li, & Zhou, 2024; Yang, Pang, Zhang, & Zhao, 2024).

A third aim is the integration of AI-driven models with existing SIEM and SOAR platforms. Such integration ensures that detection insights are not siloed but instead contribute to centralized monitoring and orchestration, thereby streamlining operations and improving situational awareness across distributed networks (Al-Khalidi & Al-Kuwari, 2024).

Finally, the research seeks to evaluate the real-world applications and challenges of AI-driven systems across multiple contexts, including enterprise, IoT, cloud, healthcare, and defense. This involves assessing scalability, resilience against adversarial manipulation, compliance with regulatory frameworks, and the sustainability of resource-intensive AI models (Bella et al., 2024; Bensaid et al., 2024; Roy et al., 2024). By addressing these objectives, the study aims to provide comprehensive insights into the promise and limitations of AI-enabled cybersecurity, offering both technical and strategic guidance for future adoption.

V. Scope of Study

The scope of this study encompasses four principal AI approaches: machine learning for learning from historical patterns and classifying threats by recognizing network behavior deviations (Sajid, Aldeer, Al-Haj, & Hasan, 2024); deep learning via convolutional and recurrent neural networks to identify intricate traffic features invisible to traditional classifiers, yielding higher anomaly detection accuracy and fewer false positives (Kimanzi, Mugo, & Muange, 2024); reinforcement learning for real-time autonomous decision-making and adaptive responses to shifting attack strategies, reducing manual intervention (Yang, Pang, Zhang, & Zhao, 2024); and explainable AI for transparency in detection/response reasoning to foster trust, accountability, and regulatory compliance (Arreche, Guntur, & Abdallah, 2024; Fatema & Chowdhury, 2025).

Domain applications include enterprise environments securing sensitive corporate data against breaches causing financial losses and stakeholder erosion (Salem, Azzam, Emam, & Abohany, 2024); IoT with billions of resource-constrained devices protected by CNN-based scalable intrusion detection for smart environments (Bella et al., 2024); cloud computing demanding AI-integrated orchestration for situational awareness and automated response in multi-tenant infrastructures (Al-Khalidi & Al-Kuwari, 2024); healthcare using federated privacy-preserving models for patient data and life-critical systems (Bensaid, Labraoui, Abba Ari, Saidi, Mboussam Emati, & Maglaras, 2024); finance leveraging predictive AI for real-time fraud detection against speed-based attacks (Roy, Li, &

Bai, 2024); and defense/critical infrastructure anticipating state-sponsored attacks to protect services and national assets (Yang et al., 2024).

These methodological pillars evaluate AI's detection precision and response effectiveness across sectors, highlighting its universal potential alongside unique adoption challenges in operationalizing intelligent security systems.

VI. Methodology

The methodology of this study is structured to provide a rigorous and systematic investigation into how artificial intelligence can advance threat detection and response systems. The first stage involves a comprehensive review of state-of-the-art models documented in recent literature. This review examines the evolution of machine learning, deep learning, reinforcement learning, and explainable artificial intelligence techniques in cybersecurity. By critically analyzing surveys and empirical studies, the review identifies strengths, limitations, and emerging trends across different approaches (Salem, Azzam, Emam, &Abohany, 2024; Wang, Li, & Zhang, 2025). In particular, emphasis is placed on understanding how these models are applied to intrusion detection, anomaly detection, and automated incident response, while also highlighting the recurring challenges of adversarial manipulation, resource intensiveness, and scalability across distributed networks. This step establishes a theoretical foundation and frames the analytical focus of the subsequent stages of the research.

The second stage centers on a comparative analysis of supervised, unsupervised, and reinforcement learning paradigms in the context of cybersecurity applications. Supervised learning has long been applied to intrusion detection through algorithms such as support vector machines, decision trees, and random forests, relying on labeled datasets to classify network traffic (Sajid, Aldeer, Al-Haj, & Hasan, 2024). While this method is effective in structured environments with abundant training data, its dependence on labeled inputs limits adaptability to novel or zero-day threats. Unsupervised learning, by contrast, uses clustering and dimensionality reduction to uncover anomalies in unlabeled data, making it particularly useful for identifying deviations in high-volume or encrypted traffic where labeling is infeasible (Chen, Guo, & Zhao, 2024). Reinforcement learning introduces a further dimension by enabling systems to autonomously optimize defense strategies based on interaction with dynamic environments, adapting response mechanisms in real time as threats evolve (Yang, Pang, Zhang, & Zhao, 2024). The comparative analysis evaluates these paradigms not only in terms of their theoretical capacity but also in their practical feasibility for enterprise-scale deployment, considering adaptability, robustness, and the balance between accuracy and computational cost.

In the third stage, the study incorporates case studies of established AI-driven cybersecurity platforms to demonstrate how theoretical advances translate into operational solutions. Darktrace,

for instance, applies unsupervised learning to create behavioral baselines within enterprise environments, enabling the identification of anomalies without prior knowledge of attack signatures. IBM QRadar integrates machine learning into a SIEM framework, providing improved event correlation and reducing false positives in large-scale corporate networks. Microsoft Sentinel, as a cloud-native solution, combines AI-driven analytics with SOAR functionalities to orchestrate rapid responses across distributed infrastructures (Al-Khalidi & Al-Kuwari, 2024). Examining these systems offers practical insights into how AI models perform when embedded in enterprise operations, highlighting both their benefits and their limitations in addressing scalability, integration, and compliance requirements.

The final stage involves establishing an evaluation framework to assess the effectiveness of AI-driven detection and response systems. The framework is designed around four critical metrics: accuracy, false positive rates, latency, and scalability. Accuracy is essential for determining how well a system can distinguish between legitimate and malicious activity, while false positive rates measure the system's reliability in avoiding irrelevant alerts that undermine operational efficiency (Roy, Li, & Bai, 2024). Latency evaluates the speed of detection and response, a vital consideration in high-frequency attack scenarios where delays exacerbate damage (Hu, Li, & Zhou, 2024). Scalability assesses the capacity of AI systems to operate effectively across large, distributed, and resource-intensive environments such as cloud platforms or IoT ecosystems (Bensaid, Labraoui, Abba Ari, Saidi, Mboussam Emati, & Maglaras, 2024). Together, these benchmarks ensure a balanced and multidimensional assessment of AI-enabled cybersecurity systems, capturing both their technical performance and their real-world applicability. This methodology, by combining literature synthesis, comparative analysis, practical case studies, and systematic evaluation, provides a comprehensive approach to understanding the promise and limitations of AI in advancing modern cyber defense.

VII. Outcomes

The outcomes anticipated from this study emphasize the transformative impact of artificial intelligence on modern cybersecurity practices. A primary expectation is the improvement of anomaly detection mechanisms, where machine learning and deep learning models are projected to outperform legacy systems by identifying complex patterns that traditional rule-based approaches cannot recognize. This improvement is also associated with the reduction of false positives, which have historically overwhelmed analysts and diverted attention from genuine threats. By training models on large-scale, diverse datasets, AI-driven systems can refine their predictive accuracy and minimize irrelevant alerts, ensuring that resources are concentrated on addressing real risks rather than wasted on misclassified anomalies (Kimanzi, Mugo, & Muange, 2024; Arreche, Guntur, & Abdallah, 2024).

Table 1. Key AI Methodologies in Cybersecurity

Methodology	Strengths	Limitations	Example Applications
Machine Learning	Learns from historical data, effective for classification	Requires labeled datasets, less effective for zero-day attacks	Supervised intrusion detection in enterprise networks
Deep Learning	Captures complex, nonlinear patterns in traffic data	Computationally expensive, less interpretable	CNNs for IoT intrusion detection (Bella et al., 2024)
Reinforcement Learning	Enables adaptive and autonomous defense strategies	Training requires large interaction data, risk of instability	Automated response in cloud and edge systems
Explainable AI (XAI)	Improves trust, transparency, and regulatory compliance	May reduce accuracy compared to black-box models	Compliance-driven sectors such as healthcare/finance

Another significant outcome is the acceleration of automated incident response processes. Reinforcement learning frameworks are expected to enable autonomous systems to adapt their defense strategies in real time, limiting the window of opportunity available to attackers and ensuring rapid containment of malicious activities. This capability is particularly important in contexts where cyber incidents unfold within seconds, rendering manual responses ineffective. By reducing both the mean time to detection and the mean time to response, AI-driven models can enhance resilience and mitigate the damage that might otherwise arise from delayed intervention (Hu, Li, & Zhou, 2024; Yang, Pang, Zhang, & Zhao, 2024).

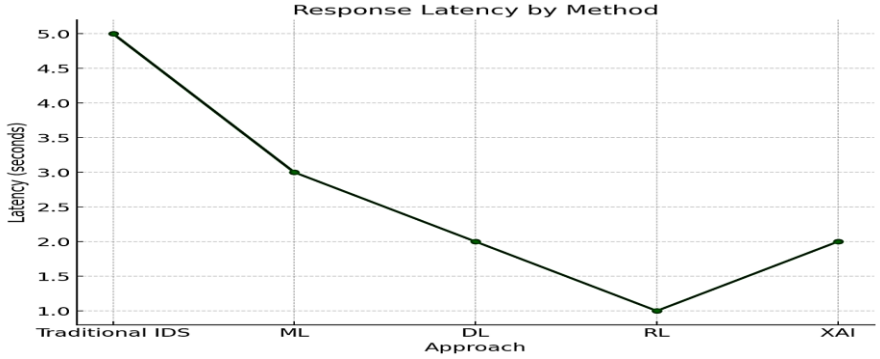
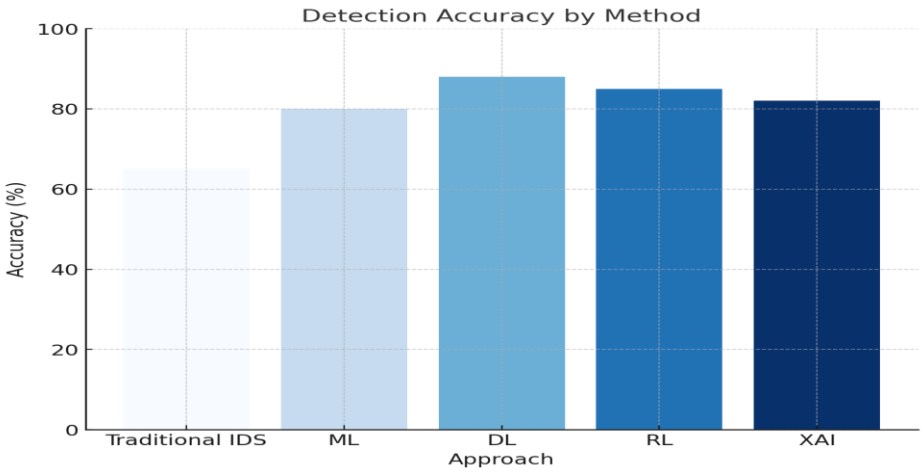


Table 2. Evaluation Framework for AI-Driven Cybersecurity

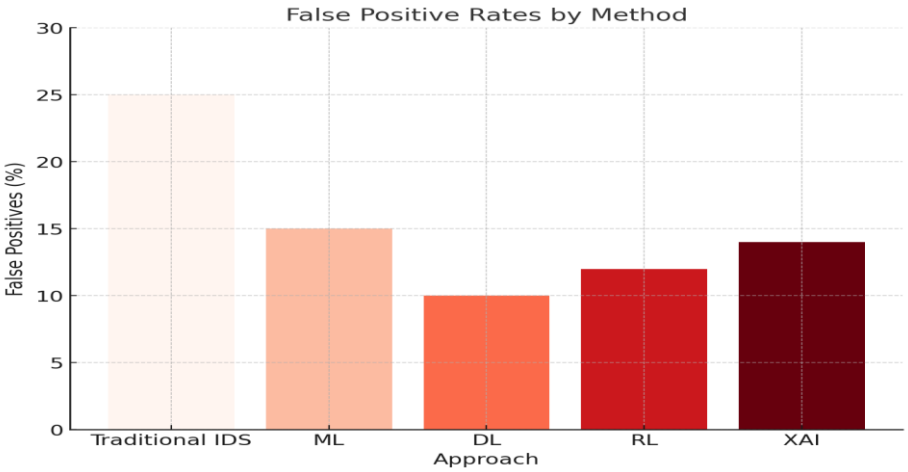
Metric	Definition	Importance in Cybersecurity
Detection Accuracy	Percentage of correct identification of attacks and benign traffic	Ensures reliable anomaly detection
False Positive Rate	Frequency of benign traffic incorrectly flagged as malicious	Reduces analyst workload and alert fatigue
Latency	Time required for detection and response	Critical in fast-moving cyberattacks where seconds matter
Scalability	Ability to operate across large and distributed networks	Essential for IoT, cloud, and enterprise deployments
Interpretability	Extent to which system decisions can be explained	Key for trust, compliance, and human validation of alerts

Table 3. Sector-Specific Applications of AI-Driven Security

Sector	Use Case Example	Benefits	Reference
Enterprise Networks	Behavioral anomaly detection with unsupervised ML	Reduces insider threats and data breaches	Salem et al. (2024)
IoT Ecosystems	CNN-based intrusion detection for connected devices	Secures billions of resource-constrained IoT devices	Bella et al. (2024)
Healthcare	Federated learning for privacy-preserving threat detection	Protects patient data and complies with regulations	Bensaid et al. (2024)
Cloud Computing	AI-integrated SIEM and SOAR platforms	Enhances situational awareness and real-time incident response	Al-Khalidi & Al-Kuwari (2024)
Finance	Predictive analytics for fraud detection	Mitigates risks in high-speed digital transactions	Roy, Li, & Bai (2024)
Defense/Critical Infrastructure	Predictive threat intelligence for state-level attacks	Protects essential services and national security assets	Yang et al. (2024)



A further anticipated outcome is the development of predictive threat intelligence capabilities. Through continuous analysis of large and heterogeneous datasets, AI systems can uncover early indicators of potential attacks, allowing defenders to take proactive measures rather than reacting after damage has occurred. Predictive intelligence is especially valuable in sectors such as finance and critical infrastructure, where the ability to forecast and neutralize threats in advance can prevent large-scale disruption (Salem, Azzam, Emam, &Abohany, 2024; Roy, Li, & Bai, 2024).



VIII. Applications

The applications of AI-enabled detection and response systems span diverse domains, reflecting the adaptability and scalability of these technologies. In enterprise environments, AI supports the monitoring of complex corporate networks that generate massive volumes of data. Tools such as Darktrace have demonstrated how unsupervised learning can establish behavioral baselines and detect deviations in real time, enabling organizations to prevent data breaches and reduce the reliance on manual oversight (Salem et al., 2024).

In the context of the Internet of Things and smart healthcare, AI-driven models play a vital role in addressing vulnerabilities across resource-constrained and highly distributed infrastructures. Convolutional neural network approaches have been applied to detect anomalies in IoT ecosystems, securing billions of connected devices against unauthorized access. Similarly, federated learning models support privacy-preserving threat detection in healthcare networks, enabling secure data sharing while protecting sensitive patient information (Bella et al., 2024; Bensaid et al., 2024).

Cloud and edge computing environments represent another critical application area. These infrastructures are characterized by multi-tenant architectures and high traffic volumes, making them attractive targets for cyberattacks. AI-driven defense mechanisms, when integrated with SIEM and SOAR platforms, enhance scalability and responsiveness in these contexts by enabling predictive analytics and orchestrating real-time responses across distributed networks (Al-Khalidi & Al-Kuwari, 2024).

Government and defense operations also benefit significantly from AI-enabled security. Predictive threat intelligence systems can provide early warnings of cyber espionage campaigns or state-sponsored attacks, thereby safeguarding critical infrastructure and ensuring continuity of essential services. The proactive capabilities of AI-driven defense are particularly important in national security contexts, where the consequences of delayed detection or response may extend beyond financial losses to societal disruption (Roy et al., 2024).

IX. Challenges and Limitations

Despite their potential, AI-based cybersecurity solutions face a series of technical, ethical, and practical challenges that limit their adoption. One of the foremost concerns is the threat of adversarial attacks targeting AI models themselves. Attackers can deliberately manipulate input data or generate adversarial samples to deceive models into misclassification, thereby undermining the reliability of automated detection systems (Yang et al., 2024). This highlights the need for robustness testing and the development of resilient architectures capable of withstanding adversarial interference.

Data privacy and ethical considerations also pose substantial obstacles. AI models require large datasets for effective training, yet many of these datasets contain sensitive information. Balancing the need for comprehensive data access with privacy-preserving techniques, such as federated learning and differential privacy, remains a critical concern for ensuring ethical deployment. Failure to address these issues risks regulatory violations and erosion of public trust (Fatema & Chowdhury, 2025).

High implementation costs present another barrier, particularly for small and medium-sized enterprises. Developing and maintaining advanced AI-driven security systems demands significant computational resources, specialized expertise, and continuous updates. While cloud-based AI services and cost-efficient frameworks may alleviate some financial pressure, the upfront investments remain prohibitive for many organizations (Roy et al., 2024).

Finally, the issue of explainability underscores the need for transparency in AI-driven cybersecurity. Many advanced models function as black boxes, providing little insight into how decisions are made. This lack of interpretability creates hesitancy in adoption, particularly in regulated industries where accountability and compliance are essential. Explainable AI frameworks address this challenge by making model outputs interpretable and validating the trustworthiness of detection systems, but their integration into high-performance models remains a complex task (Arreche et al., 2024). These limitations highlight the necessity of a balanced approach that combines innovation with ethical, economic, and regulatory considerations to ensure the sustainable advancement of AI in cybersecurity.

X. Conclusion and Future Directions

This study confirms AI's profound transformation in cybersecurity, surpassing traditional rule-based systems through adaptive machine learning, deep learning for anomaly detection, reinforcement learning for autonomous responses, and explainable AI for transparency (Arreche, Guntur, & Abdallah, 2024; Fatema & Chowdhury, 2025; Yang, Pang, Zhang, & Zhao, 2024). These advances enable proactive, predictive defenses that anticipate threats before impact (Salem, Azzam, Emam, & Abohany, 2024).

Looking ahead, large language models (LLMs) promise enhanced contextual analysis of logs, threat reports, and communications for automated log analysis, phishing detection, and analyst support—augmenting human expertise with interpretive speed (Xu, Zhang, Li, Wang, & Wang, 2024).

Future AI cybersecurity requires global standards for interoperability, fairness, accountability, performance, transparency, and privacy (Roy, Li, & Bai, 2024), alongside sustainable practices addressing computational costs through lightweight algorithms for resource-limited sectors (Bensaid, Labraoui, Abba Ari, Saidi, Mboussam Emati, & Maglaras, 2024).

In conclusion, AI excels in detection accuracy, automated responses, and predictive intelligence, but success hinges on resolving adversarial robustness, privacy, costs, and explainability via ethical, regulated, sustainable integration—forming secure digital infrastructures for the decade ahead.

Hemvati Nandan Bahuguna
Garhwal University
Srinagar, Uttarakhand

XI. References

1. Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (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
2. Arreche, O., Guntur, T., & Abdallah, M. (2024). XAI-IDS: An explainable AI framework for network intrusion detection systems. Applied Sciences, 14(10), 4170. https://doi.org/10.3390/app14104170
3. Sajid, M., Aldeer, M., Al-Haj, A., & Hasan, M. K. (2024). Enhancing intrusion detection: A hybrid machine and deep learning approach. Journal of Cloud Computing, 13, 123. https://doi.org/10.1186/s13677-024-00685-x
4. Roy, S., Li, J., & Bai, Y. (2024). Green intrusion detection systems: A comprehensive survey. Sensors, 24(17), 5516. https://doi.org/10.3390/s24175516
5. Chen, X., Guo, Y., & Zhao, H. (2024). Explainable deep learning-based intrusion detection for encrypted traffic. Sensors, 24(16), 5223. https://doi.org/10.3390/s24165223
6. Bella, K., Guezzaz, A., Benkirane, S., Azrour, M., Fouad, Y., Benyeogor, M. S., & Innab, N. (2024). Intrusion detection for IoT security using CNN decision forest. PeerJ Computer Science, 10, e2290. https://doi.org/10.7717/peerj-cs.2290
7. Bensaid, R., Labraoui, N., Abba Ari, A. A., Saidi, H., Mboussam Emati, J. H., & Maglaras, L. (2024). Federated learning-based intrusion detection for smart healthcare. PeerJ Computer Science, 10, e2414. https://doi.org/10.7717/peerj-cs.2414
8. Yang, Z., Pang, Y., Zhang, Y., & Zhao, X. (2024). Reinforcement learning for adaptive intrusion detection in dynamic networks. Electronics, 13(18), 3617. https://doi.org/10.3390/electronics13183617
9. Al-Khalidi, N., & Al-Kuwari, S. (2024). AI-enabled system for cyber incident detection and response in cloud environments. Applied Sciences, 14(22), 10567. https://doi.org/10.3390/app142210567
10. Wang, X., Li, J., & Zhang, P. (2025). Deep learning-based intrusion detection systems: A survey. Expert Systems with Applications, 245, 122117. https://doi.org/10.1016/j.eswa.2024.122117