AI LEADING FIELDS IN CYBERSECURITY

Bozorov Suhrobjon
Department of Cryptology, TUIT named after Muhammad al-Khwarizmi
https://doi.org/10.5281/zenodo.20353809

Abstract. Artificial Intelligence (AI) has become one of the most transformative technologies in modern cybersecurity. The rapid increase in cyber threats, ransomware attacks, phishing campaigns, and zero-day vulnerabilities has accelerated the integration of AI-driven solutions into security infrastructures. AI technologies such as Machine Learning (ML), Deep Learning (DL), Federated Learning (FL), and Generative AI are increasingly used in intrusion detection systems, malware analysis, behavioral analytics, automated incident response, and threat intelligence. This article analyzes the leading fields where AI significantly contributes to cybersecurity, compares major AI methods, and evaluates their advantages and limitations. Recent studies published between 2020 and 2025 are reviewed to identify emerging trends and future directions. Statistical evidence demonstrates that AI-based cybersecurity systems improve threat detection accuracy, reduce response time, and enhance proactive defense capabilities. However, challenges such as adversarial attacks, privacy concerns, explainability, and model bias remain critical research issues.

Keywords: Artificial Intelligence, Cybersecurity, Machine Learning, Deep Learning, Federated Learning, Intrusion Detection System, Threat Intelligence, Generative AI.

Introduction

The rapid digital transformation of governments, enterprises, and individuals has significantly increased cybersecurity risks. Traditional security mechanisms are no longer sufficient to detect and prevent sophisticated cyberattacks in real time. As cyber threats evolve in complexity and scale, Artificial Intelligence (AI) has emerged as a critical technology for enhancing cybersecurity resilience.

AI enables systems to learn from large volumes of network traffic, identify anomalies, automate threat responses, and predict future attacks. According to recent statistics, the global AI cybersecurity market exceeded 31 billion USD in 2024 and is expected to reach approximately 134 billion USD by 2030. Additionally, around 67% of organizations worldwide have already integrated AI technologies into their cybersecurity strategies.

Modern cyberattacks increasingly use AI-driven techniques. Generative AI tools enable attackers to automate phishing, malware generation, and vulnerability exploitation. Simultaneously, defensive cybersecurity systems also

utilize AI to detect malicious activities faster than traditional rule-based systems. Verizon's recent cybersecurity report highlighted that AI-assisted attacks are accelerating vulnerability exploitation from months to hours.

This article examines the leading applications of AI in cybersecurity, evaluates contemporary AI methods, compares their effectiveness, and discusses future challenges.

Related works

Numerous studies conducted between 2020 and 2025 demonstrate the growing importance of AI in cybersecurity.

A comprehensive study by Mohamed (2025) analyzed state-of-the-art AI and ML techniques used in cybersecurity and emphasized their role in advanced threat detection, malware classification, and automated response systems. Research on federated learning highlighted the importance of decentralized AI systems in preserving privacy while improving collaborative cybersecurity intelligence. Liu et al. (2022) investigated threats and defense mechanisms in federated learning environments and identified poisoning attacks, inference attacks, and communication vulnerabilities as major challenges.

Recent studies have also explored hybrid AI models that combine machine learning and federated learning. Moussaoui et al. (2025) reported that hybrid models provide better scalability, privacy preservation, and robustness compared to standalone ML systems. Deep learning methods have demonstrated high accuracy in malware detection and intrusion detection systems. Fattahi (2024) reviewed deep neural networks, convolutional neural networks (CNN), and recurrent neural networks (RNN) for digital forensics and cybersecurity applications.

Another emerging area involves autonomous AI agents in cybersecurity operations. Recent reports indicate that AI-driven systems are now capable of performing penetration testing, vulnerability analysis, and security monitoring with minimal human intervention.

Leading Fields of AI in Cybersecurity

Intrusion Detection Systems (IDS). AI-based Intrusion Detection Systems are among the most important cybersecurity applications. Traditional IDS systems rely heavily on predefined rules and signatures, making them ineffective against zero-day attacks and unknown threats.

Machine Learning models analyze network traffic patterns and identify anomalies automatically. Deep Learning algorithms improve the detection of

sophisticated attacks by learning complex relationships between network behaviors.

Malware Detection and Classification. AI technologies enable automated malware analysis by identifying suspicious patterns in executable files, memory behavior, and system calls.

Deep learning models such as CNN and RNN are highly effective for malware classification because they can process large datasets and recognize hidden malicious patterns.

Table 1. Statistical distribution of ai usage in cybersecurity

AI Application Area	**Organizational Usage**
Anomaly Detection	57%
Malware Detection	50.5%
Incident Response Automation	49%
Network Traffic Monitoring	45%
Threat Intelligence	41%

Threat Intelligence and Predictive Analytics. AI-based threat intelligence systems collect and analyze massive volumes of cybersecurity data from multiple sources including logs, endpoints, social media, and dark web forums.

Predictive analytics enables organizations to forecast future attacks and proactively mitigate vulnerabilities before exploitation occurs.

Generative AI tools are increasingly used to simulate attack scenarios and strengthen cyber defense strategies. However, attackers also exploit generative AI to automate phishing emails and social engineering attacks.

Federated Learning in Cybersecurity. Federated Learning (FL) allows multiple organizations to collaboratively train AI models without sharing sensitive data. This approach enhances privacy preservation and supports secure distributed cybersecurity systems.

Table 2. Comparison table of ai methods in cybersecurity

Criteria	**Machine Learning**	**Deep Learning**	**Federated Learning**
Detection Accuracy	High	Very High	High
Privacy Preservation	Medium	Medium	Very High
Computational Cost	Medium	High	High
Explainability	Moderate	Low	Moderate
Real-time Capability	High	Medium	Medium
Scalability	High	Medium	High

The comparison indicates that Deep Learning provides the highest detection performance, while Federated Learning offers superior privacy protection. Hybrid AI systems integrating ML and FL are emerging as promising solutions for modern cybersecurity infrastructures.

Challenges of AI in Cybersecurity

- Despite its advantages, AI introduces several cybersecurity challenges:
- Adversarial attacks: Attackers manipulate AI models using poisoned or deceptive inputs.
- Bias and explainability: Many AI models operate as "black boxes."
- Privacy risks: Large datasets may expose sensitive information.
- Resource requirements: Advanced AI models require powerful computational infrastructure.
- AI-powered cybercrime: Generative AI enables sophisticated phishing and automated malware generation.

Recent reports indicate that AI-generated phishing attacks increased by nearly 49% during 2025, demonstrating the growing offensive use of AI technologies.

Conclusion

Artificial Intelligence has become a leading technological force in cybersecurity. AI-driven systems significantly improve intrusion detection, malware analysis, threat intelligence, and automated incident response. Machine Learning, Deep Learning, and Federated Learning represent the most influential AI approaches currently shaping cybersecurity research and practice.

Statistical evidence confirms the increasing adoption of AI technologies by organizations worldwide. AI enhances detection accuracy, reduces response times, and strengthens proactive cyber defense mechanisms. However, challenges related to adversarial attacks, explainability, privacy, and ethical concerns remain unresolved.

Future cybersecurity systems will increasingly rely on autonomous AI agents, hybrid AI architectures, explainable AI, and federated learning environments. Therefore, continuous research and international collaboration are essential for building secure, transparent, and resilient AI-powered cybersecurity ecosystems.

References:

1.Mohamed, N. "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms." Knowledge and Information Systems, 2025.

2.Moussaoui, J. et al. “A Systematic Review on Hybrid AI Models Integrating Machine Learning and Federated Learning.” Journal of Cybersecurity and Privacy, 2025.
3.Liu, P., Xu, X., Wang, W. “Threats, attacks and defenses to federated learning: issues, taxonomy and perspectives.” Cybersecurity, 2022.
4.Feng, Y. et al. “A survey of security threats in federated learning.” Complex & Intelligent Systems, 2025.
5.Fattahi, J. “Machine Learning and Deep Learning Techniques used in Cybersecurity and Digital Forensics: a Review.” 2024.
6.Verizon Cybersecurity Report, 2026.
7.Statista. “Artificial intelligence (AI) in cybersecurity – statistics & facts.” 2024.
8.Statista. “Global organizations using AI in cybersecurity strategy 2024, by use areas.” 2025.
9.TechRadar. “The rise of agentic AI in cybersecurity.” 2025.
10.Alansary, S. et al. “Emerging AI threats in cybercrime: a review of zero-day attacks via machine, deep, and federated learning.” Knowledge and Information Systems, 2025.