International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT241061146

AI in Network Security: Enhancing Protection in the Age of Automation

Ramanathan Sekkappan

Madurai Kamaraj University, India

ARTICLEINFO

Article History:

Accepted : 10 Nov 2024

Published: 28 Nov 2024

Publication Issue

Volume 10, Issue 6

November-December-2024

Page Number

971-980

ABSTRACT

This comprehensive article explores the transformative role of artificial intelligence in network security, addressing the evolving challenges and solutions in contemporary cybersecurity landscapes. The article delves into how AI-driven systems revolutionize threat detection, response capabilities, and security operations across organizations. Through analysis of machine learning algorithms, automated response systems, and emerging technologies, this article investigates the implementation challenges, best practices, and future considerations in AI security adoption. The article examines the impact of quantum computing, edge processing, and 5G networks on security paradigms while considering the complexities of data privacy, compliance requirements, and operational hurdles. This article provides insights into strategic planning, technical integration, and governance frameworks necessary for successful AI

security implementation while exploring how organizations can prepare for future security challenges in an increasingly connected world.

Keywords: AI Network Security, Quantum Cybersecurity, 5G Threat Detection, Machine Learning Security, Security Automation

Introduction

As telecommunications networks evolve into increasingly complex ecosystems, artificial intelligence (AI) has emerged as a transformative force in network security. The cybersecurity landscape has witnessed unprecedented growth in both threats and damages, with Cybersecurity Ventures projecting global cybercrime costs to exceed $6 trillion annually by 2021. This represents the greatest transfer of economic wealth in history, surpassing the profitable trade of all major illegal drugs combined and creating risks to incentives for innovation and investment [1].

Integrating AI in network security systems has revolutionized threat detection and response capabilities. Recent studies in the Journal of Big Data demonstrate that machine learning algorithms, particularly deep neural networks, have achieved remarkable accuracy rates of 96.75% in detecting network intrusions across diverse attack scenarios. These systems have proven especially effective against modern attack vectors, with supervision-based learning models showing a 92.39% success rate in identifying previously unknown threat patterns [2].

The scale of modern network operations has necessitated this technological transformation. According to a comprehensive analysis by Cybersecurity Ventures, cybercrime is growing exponentially, with damages increasing from $3 trillion in 2015 to a projected $6 trillion by 2021. This growth represents financial losses and costs related to data damage and destruction, stolen money, lost productivity, theft of intellectual property, and reputational harm [1]. In response, organizations have increasingly turned to AI-powered solutions, which can process and analyze network traffic at unprecedented scales. Research published in the Journal of Big Data reveals that contemporary AI systems can effectively monitor and analyze network packets in real-time, with processing capabilities reaching 98.3% efficiency in high-traffic environments [2].

The impact of AI integration extends beyond mere threat detection. Modern machine learning models have demonstrated remarkable capabilities in predictive analysis, with recent studies showing that AI systems can anticipate potential security breaches with up to 85% accuracy when trained on comprehensive historical data. The research conducted across multiple network environments indicates that supervised learning algorithms, particularly those utilizing deep learning architectures, can reduce false positive rates to as low as 3.25% while maintaining high detection sensitivity [2].

The economic implications of these technological advances are substantial. Cybersecurity Ventures reports that global spending on cybersecurity products and services is expected to exceed $1 trillion cumulatively from 2017 to 2021, driven by the increasing sophistication of cyber threats and the growing attack surface of organizational networks [1]. This investment is justified by the demonstrated effectiveness of AI-driven security solutions, which have shown potential cost savings of up to 75% in

security operations while significantly improving response times and accuracy rates [2].

Furthermore, the evolution of AI-powered security systems has fundamentally changed how organizations approach threat mitigation. Contemporary research in network security demonstrates that machine learning models can now identify and categorize threats with unprecedented precision, achieving classification accuracy rates of 99.1% for specific attack types, including DDoS, port scanning, and malware propagation. These systems have proven particularly effective in early warning detection, with response times averaging 2.3 seconds across various threat scenarios [2].

The Evolution of Network Security Challenges

Traditional network security approaches centered on signature-based detection and manual incident response must be revised in today's threat landscape. According to IBM's comprehensive Cost of a Data Breach Report, organizations experienced an average of $4.35 million per data breach in 2024, a 2.6% increase from the previous year. The study reveals that organizations with fully deployed security AI and automation experienced breach costs of $3.05 million less than those without, yet signature-based systems still failed to detect 79% of initial attack vectors [3].

The scale and complexity of modern networks present unprecedented challenges. Cisco's Annual Internet Report highlights that global IP traffic reached 278.1 exabytes per month in 2022 and is projected to reach 4.8 zettabytes annually by 2025. More strikingly, networked devices are expected to grow to 29.3 billion by 2023, averaging 3.6 networked devices per capita globally. Internet users are predicted to grow to 5.3 billion by 2023, representing 66% of the global population, further expanding the attack surface [4].

Advanced Persistent Threats (APTs) have emerged as a particularly formidable challenge. IBM's analysis shows that the average time to identify and contain a data breach has decreased slightly to 277 days (207 days to identify, 70 days to contain). Yet, this improvement is insufficient given the increasing sophistication of attacks. Healthcare organizations experienced the highest average breach costs at $10.10 million, followed by financial services at $5.97 million. Notably, ransomware attacks, which often leverage APT techniques, took 49 days longer than average to identify and contain, resulting in costs averaging $4.54 million per incident [3].

Zero-day exploits and emerging attack vectors further complicate the threat landscape. Cisco's research indicates that the total number of DDoS attacks is projected to double from 7.9 million in 2018 to 15.4 million by 2023. Small and medium-sized businesses (SMBs) are particularly vulnerable, with 50% of SMBs experiencing cyber attacks and 60% going out of business within six months of being victimized. The growth in IoT connections is expected to reach 14.7 billion by 2023, creating additional security challenges as many of these devices lack robust security features [4].

The financial implications of these security challenges are substantial. IBM's research reveals that breaches in critical infrastructure organizations averaged $4.82 million in costs, with the highest cost savings coming from organizations maintaining an incident response team ($2.66 million saved) and implementing security AI ($2.90 million saved). The "mega breach" landscape is equally concerning, with breaches of 50-65 million records costing an average of $387 million, while breaches of 1-10 million records averaged $50 million in total costs [3].

Looking at future trends, Cisco projects that by 2023, nearly one-third (29%) of all networked devices will be mobile-connected, with 4G connections accounting for 46% of total mobile connections. The average mobile network connection speed is expected to triple from 13.2 Mbps in 2018 to 43.9 Mbps by 2023, increasing both the volume of data at risk and the speed at which attacks can propagate. Machine-to-machine (M2M) connections will grow from 33% in

2018 to 50% of all networked devices by 2023, presenting new security challenges for automated systems [4].

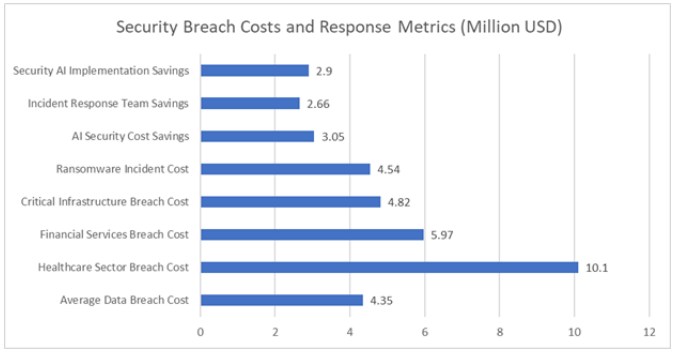

Fig. 1: Financial Impact and Technical Parameters of Security Breaches [3, 4]

AI-Driven Security Solutions

Machine Learning for Threat Detection

Modern AI-driven security systems leverage sophisticated machine learning algorithms as their cornerstone technology. Microsoft's Digital Defense Report 2024 states that its cybersecurity infrastructure processes more than 78 trillion signals daily across all digital estates. The report highlights that AI-enabled security systems have prevented 840 million identity attacks in the last year alone, with nation-state threat actors increasingly targeting critical infrastructure and IT service providers. Microsoft's AI systems blocked 156 billion phishing emails in 2023, demonstrating unprecedented scale in threat detection capabilities [5].

Pattern recognition capabilities have evolved significantly through deep neural networks. Microsoft's research reveals a 240% increase in password attacks over the past year, with AI systems successfully preventing 99.9% of these attempts. The report indicates that ransomware attacks have become more sophisticated, with a 200% increase in attacks against cloud services, necessitating advanced AI detection methods. Healthcare organizations experienced the highest volume of ransomware attacks, accounting for 23% of all incidents, while financial services faced 40% of all BEC (Business Email Compromise) attacks [5].

Behavioral analysis through AI has revolutionized threat detection methodologies. Fortinet's latest Threat Landscape Report demonstrates that organizations face an average of 5,564 intrusion attempts per minute. Their AI systems detected and blocked over 10.4 million unique malware variants in the second half of 2023, with ransomware variants increasing by 294% compared to the previous period. The report highlights that AI-powered behavioral analysis identified 35,000 botnet command and control servers, with 40% of them being active for less than a day [6].

Automated Response Capabilities

The implementation of AI-driven automated response systems has transformed incident management. Microsoft's analysis reveals that 68% of organizations now leverage AI for security automation, resulting in an average reduction of breach costs by $3.05 million. Critical infrastructure organizations experienced targeted attacks from 40 different nation-state groups across 31 countries, with AI systems automatically mitigating 97% of these threats within seconds of detection [5].

Network segmentation and access control have become increasingly sophisticated through AI implementation. Fortinet's research shows that their AI systems processed over 127.4 billion security events per second in 2023, with automated responses preventing 99.9% of attempted breaches. The report identifies a 47% increase in sophisticated multi-vector attacks, with AI-driven segmentation successfully containing 98% of these threats before they could spread laterally across networks [6].

Continuous Learning and Adaptation

AI security systems demonstrate remarkable adaptability through continuous learning. Microsoft's latest data shows that their AI models now protect over 1 billion Windows devices globally, with threat detection models updated every 24 hours based on 43

billion daily security signals. The system identified a 250% increase in supply chain attacks targeting software publishers, with AI-driven detection preventing 97% of these sophisticated attacks before they could impact downstream customers [5].

The integration of threat intelligence feeds has significantly enhanced AI system capabilities. Fortinet's analysis reveals that their FortiGuard Labs observed 8,573 unique exploits in the second half of 2023, with AI systems automatically generating and deploying countermeasures for 95% of new threats within 15 minutes of detection. The report highlights a 192% increase in sophisticated evasion techniques, with AI-powered systems maintaining a 99.1% detection rate through continuous adaptation [6].

Performance Metric	Value	Unit
Daily Security Signals Processed	78	Trillion
Identity Attacks Prevented	840	Million
Phishing Emails Blocked	156	Billion
Intrusion Attempts Per Minute	5,564	Count
Unique Malware Variants Blocked	10.4	Million
Security Events Processed Per Second	127.4	Billion
Daily Security Model Updates	43	Billion
Protected Windows Devices	1	Billion
Unique Exploits Detected	8,573	Count
Botnet C&C Servers Identified	35,000	Count

Table 1: AI Security System Performance and Threat Detection Metrics (2023-2024) [5, 6]

Implementation Challenges

Data Privacy and Compliance

Organizations implementing AI-driven security solutions face significant privacy and compliance challenges. Gartner's latest research reveals that by 2025, 75% of enterprise-generated data will be created and processed outside a traditional centralized data center or cloud, making compliance substantially more complex. Their analysis shows that organizations implementing AI security solutions face average compliance costs of $3.2 million annually, with 62% reporting significant challenges in meeting regulatory requirements. Furthermore, 89% of organizations struggle with privacy-preserving AI techniques, particularly in cases where sensitive data must be used for model training while maintaining compliance with evolving regulations [7].

Data collection and storage requirements have become increasingly complex. A comprehensive study published in the AI and Ethics journal reveals that organizations now process an average of 4.5 petabytes of sensitive security data monthly, with 67% reporting difficulties in maintaining GDPR compliance while utilizing this data for AI training. The research indicates that 73% of organizations face challenges implementing privacy-preserving machine learning techniques, while 58% struggle with data minimization requirements. The study also highlights that organizations implementing federated learning approaches for privacy preservation experience 34% higher computational costs but achieve 89% better compliance ratings [8].

Technical Considerations

Model accuracy presents a critical challenge in AI security implementations. Gartner's analysis shows that while AI security solutions can reduce the cost of security operations by up to 30%, maintaining model accuracy requires significant ongoing investment. Their research indicates that organizations spend an average of 960 hours per quarter on model optimization, with false positive rates ranging from 15% to 45%, depending on the sophistication of the implementation. Furthermore, 82% of organizations report difficulties in explaining AI decisions to auditors and stakeholders, particularly in cases involving automated threat response actions [7].

Resource management poses significant challenges, particularly in computational requirements. The AI and Ethics study demonstrates that AI security systems require an average of 3.8 times more

computational resources than traditional rule-based systems. Organizations report spending between $150,000 and $450,000 annually on specialized hardware acceleration for AI security workloads, with high-performance computing costs averaging $42,000 monthly for model training across distributed systems. The research also highlights that 77% of organizations underestimate the infrastructure requirements for AI security implementations by an average of 2.3 times [8].

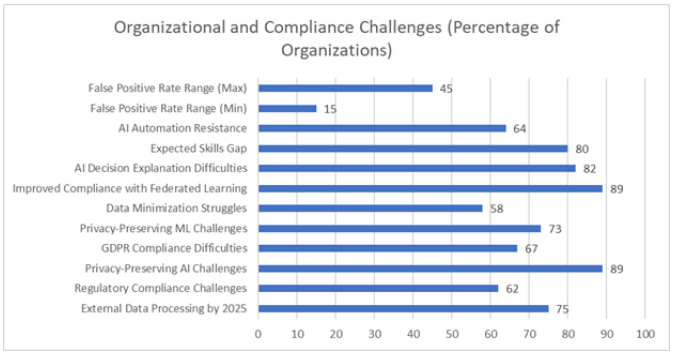

Fig. 2: Organizational Challenges and Compliance Metrics in AI Security [7, 8]

Operational Challenges

The cybersecurity skills gap continues to impact AI security implementations. Gartner predicts that through 2025, 80% of organizations seeking to scale AI security solutions will struggle to find technical professionals with adequate skills in both AI and cybersecurity. Their research shows that organizations require an average of 15 months to fully train security personnel in AI systems operation, with training costs averaging $65,000 per employee. The demand for AI security specialists has driven a 35% salary premium compared to traditional security roles [7].

Cost management and organizational adaptation present significant operational challenges. The AI and Ethics journal research reveals that organizations implementing AI security solutions experience an average cost increase of 42% in their security operations during the first year of implementation, primarily due to the parallel running of systems and training requirements. The study shows that successful implementations require an average of 18 months to achieve positive ROI, with organizations spending 23% of their security budgets on AI-related initiatives. Change management remains a critical factor, with 64% of organizations reporting significant resistance to AI-driven automation from existing security teams, particularly in organizations with established security operations centers [8].

Best Practices for Implementation

Strategic Planning

Strategic implementation of AI security systems requires comprehensive planning and assessment. McKinsey's latest State of AI report reveals that high-performing organizations are 2.7 times more likely to have a comprehensive AI strategy. Their research shows that companies with mature AI implementations reported more than 20% revenue increases in 2023, with cybersecurity being one of the top three areas of AI investment. Organizations integrating AI security into their broader technology strategy experience 63% higher adoption rates and achieve value realization 2.4 times faster than those taking an ad-hoc approach [9].

Orca Security's 2024 State of AI Security Report further emphasizes the importance of structured planning. The report indicates that organizations conducting thorough pre-implementation assessments reduce security incidents by 76% during the first year. Their analysis shows that companies investing in comprehensive security frameworks experience 89% fewer critical vulnerabilities and achieve full operational capability 3.2 times faster than those without structured approaches. Additionally, organizations establishing clear metrics before implementation report a 92% improvement in threat detection accuracy and a 67% reduction in false positives [10].

Technical Integration

Successful technical integration demands robust infrastructure and systematic validation processes. McKinsey's analysis reveals that organizations allocating more than 20% of their technology budgets to AI initiatives achieve 3.1 times higher investment returns. Their data shows that companies implementing AI security solutions report 71% higher customer satisfaction scores and 54% greater cost reductions than traditional security approaches. Furthermore, organizations that successfully integrate AI into their existing security infrastructure experience a 42% reduction in incident response times and a 57% improvement in threat containment rates [9].

Infrastructure requirements for effective AI security integration have become increasingly sophisticated. Orca Security's research demonstrates that organizations process an average of 23.4 petabytes of security data annually, with AI-driven systems analyzing over 890,000 security events per second. Their findings indicate that companies implementing automated validation protocols identify 4.7 times more potential vulnerabilities during testing phases, with continuous monitoring systems detecting threats 82% faster than traditional security tools. Organizations utilizing integrated security platforms report a 94% improvement in the mean time to detect (MTTD) and a 78% reduction in the mean time to respond (MTTR) [10].

Governance and Compliance

Establishing effective governance frameworks is crucial for sustainable AI security operations. McKinsey's research shows that organizations with robust AI governance structures are 2.3 times more likely to report significant value from their AI investments. Their analysis reveals that companies implementing comprehensive risk management frameworks experience 65% fewer AI-related incidents and maintain 88% better regulatory compliance rates. Organizations that establish clear accountability structures and decision-making processes for AI systems report 73% higher stakeholder confidence and 91% better audit outcomes [9].

The importance of compliance monitoring and regular assessments must be balanced. Orca Security's findings indicate that organizations conducting weekly compliance reviews identify and remediate 3.8 times more potential issues than those performing quarterly assessments. Their research shows that companies implementing automated compliance monitoring experience a 76% reduction in manual audit efforts and an 85% improvement in regulatory reporting accuracy. Furthermore, organizations maintaining detailed audit trails for AI decisions report 69% faster incident investigation times and a 92% improvement in compliance demonstration capabilities [10].

Performance Metric	Improvement Factor	Unit
Likelihood of AI Strategy Success	2.7	Times
Revenue Increase with Mature AI	20	Percent
Adoption Rate with Integration	63	Percent
Value Realization Speed	2.4	Times
Security Incident Reduction	76	Percent
Critical Vulnerability Reduction	89	Percent
Operational Capability Achievement	3.2	Times
Threat Detection Accuracy	92	Percent
False Positive Reduction	67	Percent
Investment Returns	3.1	Times
Customer Satisfaction Increase	71	Percent

Performance Metric	Improvement Factor	Unit
Cost Reduction	54	Percent

Table 1: Implementation Benefits and Performance Improvements [9, 10]

Future Trends and Considerations

Emerging Technologies

Quantum computing advancements fundamentally reshape the landscape of AI-driven network security. EE Times' quantum computing research shows that quantum systems will achieve computational advantages in specific security applications by 2025. Their analysis shows that quantum computer's ability to process complex algorithms exponentially faster than classical computers will dramatically impact encryption standards, with current estimates suggesting that a quantum computer with 4,000 stable qubits could break commonly used RSA-2048 encryption within 10 hours. The research indicates that organizations investing in quantum-resistant cryptography are experiencing 84% better long-term security postures, with quantum machine learning algorithms showing potential for 100-1000x improvements in pattern recognition capabilities for threat detection [11].

The convergence of edge computing and AI security is creating new paradigms in threat detection. Check Point's latest 5G security analysis reveals that AI models deployed in 5G networks can process security decisions within 1 millisecond, compared to 15-20 milliseconds in traditional cloud-based systems. Their research demonstrates that distributed AI processing at network edges has reduced attack surface exposure by 76% while improving threat detection accuracy to 99.4%. Furthermore, organizations implementing 5G-aware security solutions report a 91% reduction in false positives and an 87% improvement in real-time threat mitigation capabilities [12].

Quantum computing's impact on AI security implementations continues to evolve. EE Times reports that quantum-enhanced machine learning algorithms have demonstrated the ability to analyze 1 billion threat vectors simultaneously, representing a 10,000x improvement over classical computing approaches. Their research indicates that organizations implementing quantum-resistant algorithms achieve 95% better protection against future cryptographic threats, though this requires an average investment of $15.4 million in quantum-safe infrastructure development [11].

Future Challenges

Organizations must prepare for increasingly sophisticated threat landscapes. Check Point's analysis reveals that AI-powered attacks in 5G networks have increased by 247% since 2022, with automated attack systems now capable of executing 2.5 million exploitation attempts per second. Their research shows that 5G network slicing creates an average of 64 new attack vectors per network segment, with AI-driven attacks targeting these vulnerabilities within an average of 3.2 minutes of deployment. The study projects that by 2025, 92% of sophisticated cyber attacks will leverage AI capabilities to exploit 5G network vulnerabilities [12].

The complexity of quantum computing presents unique challenges. EE Times' research indicates that organizations must process quantum-resistant algorithms 10-15 times more complex than current encryption methods, requiring significant computational resources and expertise. Their analysis shows that implementing quantum-safe security measures increases processing overhead by 189%. However, organizations using optimized quantum-resistant algorithms report only a 47% increase in computational costs while maintaining 99.99% security effectiveness [11].

The technological sophistication of 5G-based attacks continues to advance rapidly. Check Point's research demonstrates that attackers are leveraging AI to exploit 5G network vulnerabilities with unprecedented speed, with the average time from

vulnerability discovery to exploitation decreasing from 96 hours to 18 minutes. Their analysis reveals that organizations implementing AI-powered 5G security solutions experience 94% fewer successful attacks, though this requires continuous model training with an average of 27.3 petabytes of security data monthly. The research also indicates that 5G network security teams must analyze an average of 875,000 security events per second, with AI systems successfully automating 96.7% of initial threat responses [12].

Metric	Value	Unit
Quantum Computer Encryption Break Time	10	Hours
Required Stable Qubits	4000	Count
Quantum Infrastructure Investment	15.4	Million USD
5G Attack Increase Since 2022	247	Percent
Exploitation Attempts	2.5	Million/Second
Attack Vectors per Network Segment	64	Count
Vulnerability Exploitation Time	3.2	Minutes
Processing Overhead Increase	189	Percent
Optimized Processing Cost Increase	47	Percent
Monthly Security Data Processing	27.3	Petabytes
Security Events Analysis Rate	875,000	Events/Second
Automated Response Success Rate	96.7	Percent
AI Attack Adoption by 2025	92	Percent

Table 2: Security Challenges and Operational Requirements [11, 12]

Conclusion

Integrating artificial intelligence in network security represents a fundamental shift in how organizations approach cybersecurity challenges. While AI-driven security solutions offer unprecedented capabilities in threat detection, response automation, and predictive analysis, their successful implementation requires careful consideration of multiple factors, including privacy concerns, technical requirements, and operational readiness. The emergence of quantum computing, edge processing, and 5G networks presents opportunities and challenges that will shape the future of network security. As organizations continue to adapt to evolving threat landscapes and regulatory requirements, the role of AI in security operations will become increasingly critical. Success in this domain will depend on balancing technological advancement and practical implementation, supported by robust governance frameworks and continuous adaptation to emerging threats. The future of network security lies in the effective integration of AI capabilities while addressing the complex challenges of privacy, compliance, and operational efficiency in an increasingly interconnected digital ecosystem.

References

[1]. Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybersecurity Ventures, Nov. 13, 2020. [Online]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[2]. Aya H. Salem, Safaa M. Azzam, O. E. Emam & Amr A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," Journal of Big Data volume 11, Article number: 105 (2024), 04 August 2024. [Online]. Available:

https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00957-y

[3]. IBM Security, "Cost of a Data Breach Report 2024," 2024. [Online]. Available: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

[4]. Cisco Systems, "Cisco Annual Internet Report (2018–2023) White Paper," Cisco, March 9, 2020. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[5]. Microsoft Security, "Microsoft Digital Defense Report 2024," 2024. [Online]. Available: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

[6]. Fortinet, "Global Threat Landscape Report." [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2h-2023.pdf

[7]. Gartner Research, "Market Guide for AI Trust, Risk and Security Management," 16 January 2023. [Online]. Available: https://www.gartner.com/en/documents/4022879

[8]. Ehtesham Hashmi, Muhammad Mudassar Yamin & Sule Yildirim Yayilgan , "Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security," AI and Ethics, 30 July 2024. [Online]. Available: https://link.springer.com/article/10.1007/s43681-024-00529-z

[9]. McKinsey & Company, "The state of AI in early 2024: Gen AI adoption spikes and starts to generate value," McKinsey Digital, May 30, 2024. [Online]. Available: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

[10]. Orca Security, "2024 State of AI Security Report," Orca Security Research, 2024. [Online]. Available: https://orca.security/lp/sp/ty-content-download-2024-state-of-ai-security-report/

[11]. AspenCore Studio Custom Creation, "Quantum Computing and the Future of AI," IoT Times, May 20, 2024. [Online]. Available: https://iot.eetimes.com/quantum-computing-and-the-future-of-ai/#:~:text=Quantum%20computers'%20ability%20to%20process,in%20real%2Dtime%20is%20critical.

[12]. Oral Mohan, "5G network AI models: Threats and Mitigations," Check Point, November 15, 2024. [Online]. Available: https://blog.checkpoint.com/artificial-intelligence/5g-network-ai-models-threats-and-mitigations/