



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** X **Month of publication:** October 2026

DOI: <https://doi.org/10.22214/ijraset.2026.85059>

www.ijraset.com

Call: ☎ 08813907089

E-mail ID: ijraset@gmail.com

Modern Networks, Security Threats, and the Role of Artificial Intelligence: A Review

Rajalakshmanan

Department of Electronics and Communication Engineering (ECE)

Abstract: Networks now connect mobile users, cloud platforms, edge nodes and billions of small devices, and every new connection widens the area that attackers can reach. This paper reviews the present state of networking, the main security threats, and the ways artificial intelligence (AI) is being used both to manage networks and to defend them. It describes 5G and emerging 6G systems, software-defined and virtualized infrastructure, the Internet of Things (IoT) and zero trust architecture. It then examines current threats, from record-scale denial-of-service attacks to AI-assisted intrusion. The core of the paper covers AI applications in intrusion detection, traffic optimization, automated response and self-managing networks, followed by a critical look at the weaknesses of AI itself: adversarial manipulation, data poisoning, false alarms, privacy and limited explainability. Evidence from recent surveys, standards and industry reports indicates that AI can shorten detection and response times and reduce breach costs, but only when it is governed carefully and protected as a target in its own right.

Keywords: network security, artificial intelligence, intrusion detection, zero trust, 6G, federated learning, adversarial machine learning

I. INTRODUCTION

Computer networks are the shared infrastructure behind banking, healthcare, education, manufacturing and public administration. As they grow, they also become harder to defend. Traffic is encrypted and spread across data centers, cloud services and an enormous number of small connected devices, so the older picture of a trusted internal network behind a protected border no longer matches how systems are actually built and used.

Artificial intelligence has become a central part of the response to this complexity. IBM's 2025 study of data breaches found that organizations making extensive use of AI and automation in their security operations saved an average of about USD 1.9 million per breach and shortened the breach lifecycle by an average of 80 days [1]. The same study also reported that one in five organizations had experienced a breach linked to unsanctioned "shadow AI," and that only 37% had policies for managing AI or detecting such use [1]. AI is therefore both a defensive tool and a new source of risk.

The pressure from attackers is also rising. Cloudflare reported that its network mitigated 23.2 million network-layer DDoS attacks in the first half of 2026, of which 935 exceeded one terabit per second, and that the number of such very large attacks rose from 130 in the first quarter to 805 in the second [2], [3]. Defenders cannot respond to this scale and speed with manual procedures alone.

This paper has five objectives: (1) to describe the main features of modern network infrastructure; (2) to summarize the current threat landscape; (3) to review how AI is applied to network security and operations; (4) to assess the risks and limitations of these applications; and (5) to outline likely future directions. The work is a narrative review. It draws on recent academic surveys, standards from the National Institute of Standards and Technology (NIST) and industry telemetry reports, and it does not present new experiments.

II. THE MODERN NETWORK LANDSCAPE

A. From 5G to AI-native 6G

Fifth-generation (5G) networks brought network slicing, very dense device connectivity and cloud-style core networks, and the industry is now defining the sixth generation. The ITU-R framework for IMT-2030, the formal name for 6G, treats the combination of AI and communication as a usage scenario of its own, which is a first for any generation of mobile standards [4]. Researchers describe 6G as AI-native, meaning that communication, computing, sensing and AI are expected to be merged into one highly autonomous system [5]. This integration promises better performance, but it also means that threats can cross layers, so isolated, technology-specific security measures are unlikely to be enough [5].

B. Cloud, Edge and Virtualized Networks

Software-defined networking (SDN) separates the control plane from the data plane, so that a logically central controller decides how traffic is forwarded. Network function virtualization (NFV) runs functions such as firewalls and load balancers as software on ordinary servers rather than as dedicated hardware. Edge computing moves processing closer to users and devices to reduce delay. Together these technologies make networks flexible and programmable, but they also concentrate risk: a compromised controller, a poorly protected management interface or a misconfigured virtual function can affect a very large part of the infrastructure at once.

C. The Internet of Things

IoT deployments connect sensors, cameras, vehicles, medical devices and industrial controllers. Many of these devices have little processing power, cannot run conventional security software, are rarely updated and stay in service for years. They are difficult to monitor centrally, and they are attractive building blocks for botnets. For network defenders, IoT adds a very large number of weakly protected endpoints that generate traffic of many different kinds.

D. Zero Trust Architecture

NIST Special Publication 800-207 describes zero trust as a set of security ideas that move protection away from wide network perimeters and toward individual resources, on the principle that no asset or user account receives implicit trust merely because of where it sits on the network [6]. The publication presents this as a response to remote users and cloud-hosted assets that lie outside an enterprise-owned boundary [6]. Zero trust depends on continuous verification of identities, devices and requests. That is a high-volume decision problem, and it is one of the areas where AI-based risk scoring and behavior analysis can add value.

III. NETWORK SECURITY CHALLENGES

A. Distributed Denial of Service

DDoS remains one of the most visible threats to availability. Beyond the half-year totals already cited, Cloudflare's report notes that terabit-scale attacks are now arriving at a rate of hundreds per quarter [2]. A record attack of 31.4 Tbps was attributed to the Aisuru/Kimwolf botnet [7]. Most attacks are in fact small and short, and Cloudflare stresses that even the largest can finish within seconds, which leaves no practical window for a human analyst to react after an alert is raised [2]. This is a strong argument for automated, always-on mitigation.

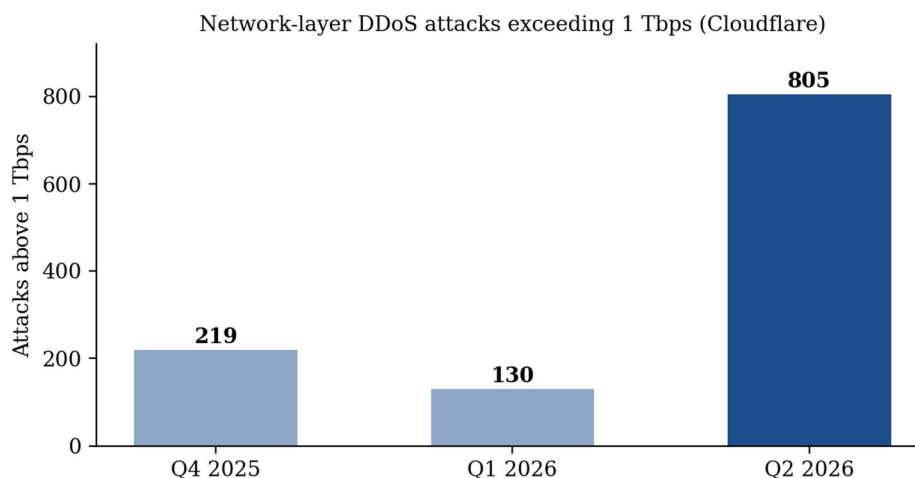


Fig. 1. Network-layer DDoS attacks above 1 Tbps per quarter (data from [2], [3]).

B. Ransomware, Phishing, Credential Abuse and Insider Threats

Many serious incidents do not begin with a technical exploit of the network itself. They begin with a stolen password, a convincing phishing message, an unpatched server or a careless or malicious insider. Once inside, attackers move laterally across flat networks, escalate privileges and then encrypt or steal data. Detection speed matters greatly in these cases: IBM found that organizations that discovered a breach themselves, rather than being told by the attacker, saved about USD 900,000 on average [1].

C. Weak Points in IoT, Cloud and the Supply Chain

Default credentials on devices, exposed cloud storage, over-permissive access roles and vulnerable third-party software components all create openings that traditional perimeter tools do not see. Because modern networks are assembled from many vendors and services, the security of the whole depends on the weakest component.

D. AI-enabled Attacks

Attackers are adopting AI as well. A recent survey of attack agents built on large language models (LLMs) explains that such agents can scout targets, reason about next steps, generate malicious code and deceptive content, and coordinate with other agents or human operators [8]. The authors argue that this lowers the time, skill and money needed to mount an attack and increases the scale at which attacks can be run, a trend they call cyber threat inflation [8]. Defenders should therefore assume that attacks will become more frequent and more adaptive.

IV. ARTIFICIAL INTELLIGENCE IN NETWORKS

A. Intrusion and Anomaly Detection

Intrusion detection is the most mature use of AI in network security. Early intrusion detection systems relied on hand-written rules and signatures of known attacks, and the field has since moved through machine learning (ML) toward deep learning (DL) [9]. A signature-based system cannot recognize an attack it has never seen. Learning-based systems instead model normal and malicious behavior from data, which in principle lets them generalize to new attacks, including those that exploit previously unknown vulnerabilities [10]. Systematic reviews classify DL-based detectors by the kind of neural architecture they use, including autoencoders, recurrent networks, restricted Boltzmann machines and convolutional networks [11]. Autoencoders and other generative models are typically used for anomaly detection, where only normal traffic is available for training. Convolutional and recurrent models are more often used for supervised classification of flows and sequences. In practice, detectors are usually deployed at several points, such as network gateways, cloud workloads and endpoints, and their alerts are combined.

B. Traffic Prediction and Network Optimization

Outside security, AI is widely used to run networks more efficiently. Time-series models can forecast traffic load and help operators plan capacity. Reinforcement learning and related methods have been proposed for routing, spectrum and energy management, and for allocating resources among network slices. These functions also support security indirectly, because a network that understands its normal load patterns finds abnormal behavior easier to spot.

C. Automated Threat Response

Detection has limited value if response is slow. Security orchestration, automation and response (SOAR) platforms execute predefined playbooks, for example by isolating a host, blocking an address or revoking a token. AI adds the ability to rank alerts, correlate events across sources and suggest or trigger the playbook that fits. The financial effect reported by IBM, described above, is the strongest published indication of the benefit of this approach at scale [1]. A recent survey of agentic AI in security operations looks at the workflows of security operations centers, including threat-intelligence processing, detection engineering and incident-response automation, where LLM-based agents combine reasoning with tools and memory [12]. Given the very short duration of many DDoS events [2], automated mitigation is essential rather than optional.

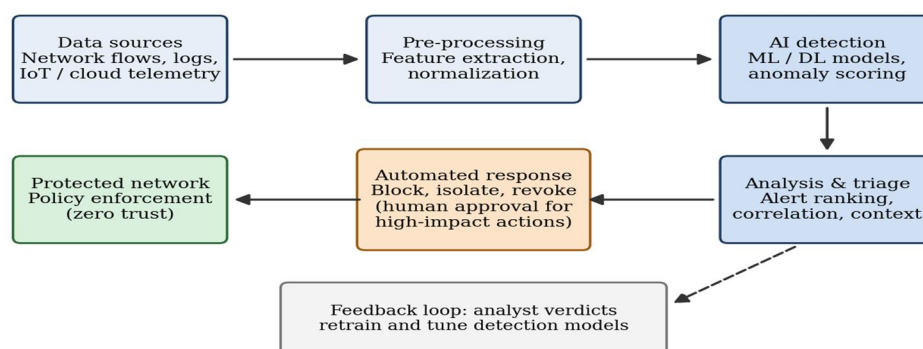


Fig. 2. Conceptual pipeline of AI-based network detection and response (author's illustration).

D. Self-healing and Intent-based Networking

In intent-based networking, an operator states a goal in high-level terms, for example that a group of services must remain isolated and reachable within a given delay, and the system translates the goal into configuration, checks that the result matches the goal and corrects drift. Self-healing extends this idea to faults: the network detects a failure, diagnoses its probable cause and applies a fix. LLMs are now being placed in such operational roles, where they query telemetry, propose configuration changes and, in some deployments, apply them to live infrastructure [13]. International standardization is also moving in this direction, with the IMT-2030 framework treating AI as a native network capability [4].

Table I. Common AI techniques in network security and operations

Technique	Typical network use	Main strength	Main limitation
Supervised classifiers (e.g., random forests, CNNs)	Classifying flows or packets as benign or malicious	High accuracy on known attack types	Needs labeled data; weaker on new attacks
Autoencoders and generative models	Anomaly detection from normal traffic only	Can flag previously unseen behavior	Prone to false alarms when normal traffic changes
Sequence models (RNNs, transformers)	Detecting multi-step attacks and temporal patterns	Captures order and timing of events	Higher computing cost
Reinforcement learning	Routing, slicing, resource and policy decisions	Learns from interaction and feedback	Unsafe exploration; hard to validate
Federated learning	Training detectors across devices or sites without sharing raw data	Privacy-friendly; reduces data transfer	Vulnerable to poisoned updates; uneven data
LLM-based agents	Alert triage, investigation, drafting changes and responses	Flexible reasoning over text and logs	Hallucination; manipulation; excessive autonomy

V. RISKS AND LIMITATIONS OF AI IN NETWORKS

A. Adversarial Manipulation and Data Poisoning

AI systems can be attacked directly. NIST's taxonomy of adversarial machine learning groups attacks on predictive systems into evasion, poisoning and privacy attacks, and adds misuse attacks for generative systems [14]. Evasion changes an input after deployment so that the model responds incorrectly, which for an intrusion detector could mean shaping malicious traffic so that it looks normal. Poisoning corrupts the data used for training, so the model learns the wrong behavior from the start. NIST describes mitigation strategies together with their limitations [14]. Any organization that deploys AI in its security stack should therefore treat the models and their training pipelines as assets that need protection.

B. False Positives and the Operational Gap

A long-standing criticism holds that machine learning for network intrusion detection faces difficulties that are less severe in other application areas, including the high cost of mistakes, the huge variety of normal traffic and the difficulty of evaluating detectors fairly [15]. A detector that is accurate on a benchmark dataset can still produce so many false alarms in a real network that analysts stop trusting it. Models trained on old public datasets may also fail to reflect current traffic and attacks.

C. Privacy and Data Governance

Training detectors requires network data, which can contain personal information. Federated learning reduces this problem by letting each participant train locally and share only model updates [16], [17]. It is not a complete solution, however. Surveys of federated intrusion detection for cloud and IoT settings list poisoning and inference attacks, differences among clients, and non-identically distributed data among the open challenges [18].

D. Explainability and Accountability

Security analysts must understand why an alert was raised before acting on it, and auditors may need to justify automated decisions. Deep models are often hard to interpret, which makes it difficult to verify their reasoning, to debug them or to assign responsibility when an automated action causes harm. Explainable detection remains an active research topic.

E. Governance, Shadow AI and Excessive Autonomy

Weak governance is already visible in practice. As noted earlier, IBM found that few organizations had policies for managing AI or detecting shadow AI [1]. The risk grows when AI agents are given authority over infrastructure. A security commentary on a survey of agentic AI in network and IT operations describes the situation as a confused-deputy problem, in which an agent with legitimate access to change-management systems and network controllers could be manipulated, for example through falsified telemetry, into taking harmful actions [13]. The proposed architectural remedy is a strict split between proposing and committing changes: the model may analyze, retrieve evidence and draft proposals but cannot execute writes, and changes are applied only through a separate, controlled path [13].

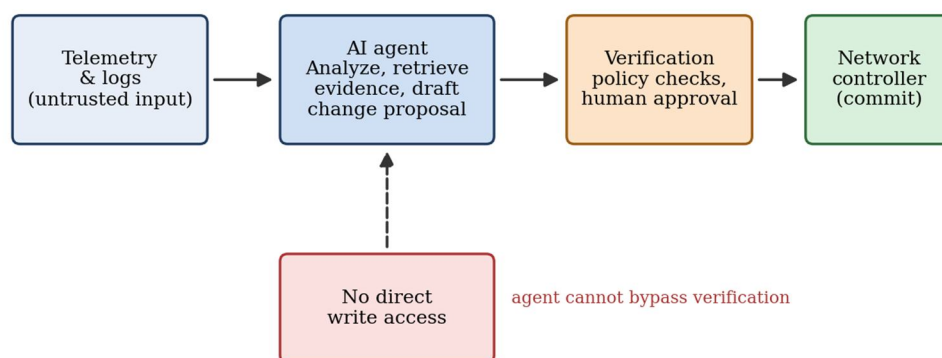


Fig. 3. Propose-commit pattern for safe agentic network operations (propose-commit idea from [13]; the verification stage is the author's illustration).

VI. TRADITIONAL VERSUS AI-BASED NETWORK SECURITY

Table II summarizes the main differences. The comparison is conceptual and based on the sources discussed above. Real systems are usually hybrids in which signature rules, policy engines and learned models complement each other.

Table II. Comparison of traditional and AI-based network security

Aspect	Traditional security	AI-based security
Detection method	Fixed signatures, static rules and thresholds	Learned models of normal and malicious behavior
Unknown attacks	Poor; needs a signature or rule first	Possible through anomaly detection, with more false alarms
Speed and scale	Limited by human analysts and manual updates	Can process large data volumes and respond automatically
Maintenance	Rules updated manually by experts	Models need retraining and monitoring for drift
Transparency	Easy to read and audit	Often hard to interpret
Own attack surface	Rule bypass and evasion	Adversarial inputs, poisoning, model theft, prompt manipulation
Data needs	Low	High; privacy and quality issues

VII. FUTURE TRENDS

A. Agentic AI for Network and Security Operations

The next stage is likely to be agentic systems that plan multi-step work, use tools and act with limited supervision. Surveys of this area describe progress from single LLM assistants to multi-agent pipelines for security operations [12]. The practical question is no longer whether such agents can help, but how to bound their authority. Designs that separate proposal from execution, log every action and require independent verification [13] are likely to become standard practice.

B. Federated and Privacy-preserving Learning

Federated learning is expected to grow in IoT and edge security because it fits distributed devices and data-protection rules [16], [17]. Research priorities include resistance to poisoned participants, handling of uneven data and combination with techniques such as differential privacy and secure aggregation [18].

C. AI-native 6G Security

As 6G moves toward AI-native operation, learning-based defense is expected to become part of the radio access network and the core network instead of an external add-on. One recent survey of AI-native security for 5G and 6G open RAN, drawing on 177 studies, argues for exactly this design, while also stressing that the defenses themselves must be tested for adversarial robustness [4]. A cross-layer security and privacy framework has also been proposed to avoid fragmented solutions [5].

D. Quantum-safe Security

Large quantum computers would break widely used public-key algorithms such as RSA and elliptic-curve schemes. NIST finalized its first post-quantum standards on August 13, 2024: FIPS 203 (ML-KEM) for key establishment, FIPS 204 (ML-DSA) for digital signatures and FIPS 205 (SLH-DSA) as a hash-based signature alternative [19]. Network operators will need to find where vulnerable cryptography is used and migrate it. This is a likely area for AI-assisted inventory and monitoring, although that application is a prospect rather than an established practice.

VIII. CONCLUSION

Modern networks are larger, more distributed and more programmable than their predecessors, and the threats against them are growing in volume and speed. The evidence reviewed here indicates that AI is already useful in detecting intrusions, managing operations and automating response, and that organizations using it extensively in security have reported lower breach costs and shorter breach lifecycles [1]. The same evidence shows that AI is not a cure-all. Models can be fooled or poisoned, produce costly false alarms, depend on sensitive data and resist explanation, and autonomous agents with broad permissions create new ways to cause harm [13], [14], [15].

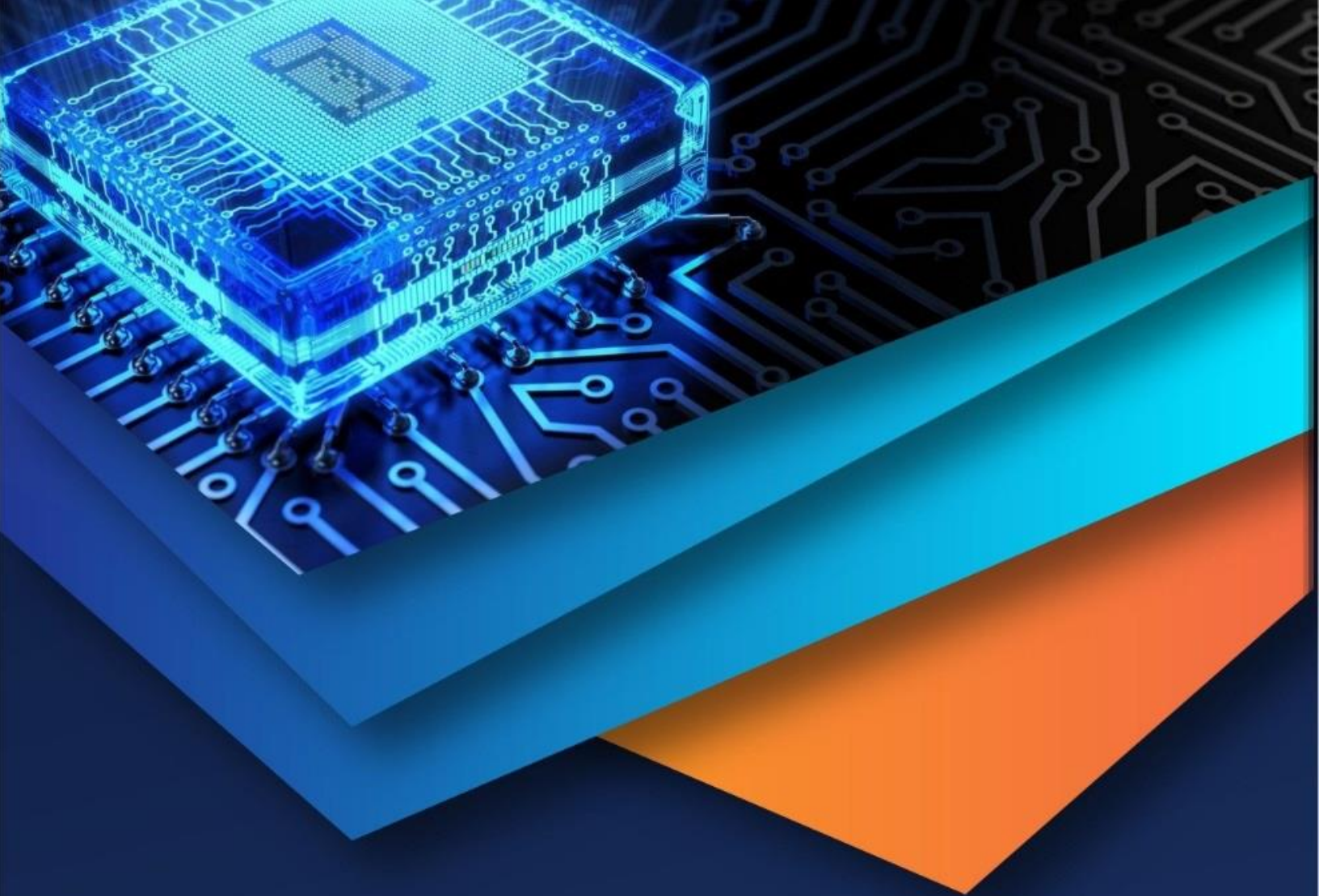
Several practical recommendations follow. Organizations should adopt zero trust principles as the architectural base [6]; use AI for detection and response where speed matters, with humans in control of high-impact actions; protect models and training data as security assets, following guidance such as NIST's adversarial machine learning taxonomy [14]; establish clear governance for all AI use, including unsanctioned tools [1]; and begin planning the migration to quantum-safe cryptography [19]. Future research should focus on evaluation with realistic and current data, robust and explainable detection, safe limits on agent autonomy and privacy-preserving collaboration among networks.

This review has limits. It is a narrative synthesis of selected recent sources, several of which are industry reports and preprints that have not all been through formal peer review, and the field changes quickly. Readers should treat the figures quoted here as snapshots from the cited dates.

REFERENCES

- [1] IBM, "IBM report: 13% of organizations reported breaches of AI models or applications, 97% of which reported lacking proper AI access controls," IBM Newsroom (Cost of a Data Breach Report 2025, with Ponemon Institute), Jul. 30, 2025. [Online]. Available: <https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls>
- [2] Cloudforce One, "Cloudflare DDoS threat report H1 2026: 1 Tbps attacks soar as DNS floods and geopolitical tensions drive a new wave," Cloudflare Blog, Aug. 11, 2026. [Online]. Available: <https://blog.cloudflare.com/ddos-threat-report-2026-h1/>
- [3] "Cloudflare says 1 Tbps DDoS attacks grew sixfold in the second quarter," SiliconANGLE, Aug. 11, 2026. [Online]. Available: <https://siliconangle.com/2026/08/11/cloudflare-says-1-tbps-ddos-attacks-grew-sixfold-second-quarter/>
- [4] I. W. A. J. Pawana, V. Abella, E. Aaron Miele, H. Park, and I. You, "AI-native security for 5G and 6G O-RAN: A survey of learning-based defense against false base stations, DDoS, and signaling storms," *Comput. Model. Eng. Sci.*, vol. 148, no. 3, p. 6, Sep. 2026, doi: 10.32604/cmes.2026.087445.
- [5] B. Barua et al., "Toward a unified security and privacy framework for AI-native 6G networks," arXiv:2607.01019, Jul. 2026, doi: 10.48550/arXiv.2607.01019.

- [6] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, Aug. 2020, doi: 10.6028/NIST.SP.800-207.
- [7] B. Toulas, "DDoS attacks over 1 Tbps surged fivefold in the second quarter," BleepingComputer, Aug. 11, 2026. [Online]. Available: <https://www.bleepingcomputer.com/news/security/ddos-attacks-over-1-tbps-surged-fivefold-in-the-second-quarter/>
- [8] M. Xu et al., "Forewarned is forearmed: A survey on large language model-based agents in autonomous cyberattacks," arXiv:2505.12786, 2025, doi: 10.48550/arXiv.2505.12786.
- [9] J. Liu et al., "Generative AI and federated learning for intrusion detection systems: A survey," arXiv:2607.01305, Jul. 2026, doi: 10.48550/arXiv.2607.01305.
- [10] Z. Xu et al., "Deep learning-based intrusion detection systems: A survey," arXiv:2504.07839, 2025, doi: 10.48550/arXiv.2504.07839.
- [11] J. Lansky et al., "Deep learning-based intrusion detection systems: A systematic review," IEEE Access, vol. 9, pp. 101574–101599, 2021, doi: 10.1109/ACCESS.2021.3097247.
- [12] V. Vinay, "The evolution of agentic AI in cybersecurity: From single LLM reasoners to multi-agent systems and autonomous pipelines," arXiv:2512.06659, 2025, doi: 10.48550/arXiv.2512.06659.
- [13] "When your AI assistant has the keys to production," Help Net Security, May 20, 2026. [Online]. Available: <https://www.helpnetsecurity.com/2026/05/20/agentic-ai-security-llm-research/>
- [14] National Institute of Standards and Technology, "Adversarial machine learning: A taxonomy and terminology of attacks and mitigations," NIST AI 100-2e2025, Mar. 2025, doi: 10.6028/NIST.AI.100-2e2025.
- [15] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proc. IEEE Symp. Security and Privacy, 2010, pp. 305–316.
- [16] U. A. Isma'ila, K. U. Danyaro, A. A. Muazu, and U. D. Maiwada, "Review on approaches of federated modeling in anomaly-based intrusion detection for IoT devices," IEEE Access, vol. 12, pp. 30941–30961, 2024.
- [17] A. Vyas, P.-C. Lin, R.-H. Hwang, and M. Tripathi, "Privacy-preserving federated learning for intrusion detection in IoT environments: A survey," IEEE Access, vol. 12, pp. 127018–127050, 2024, doi: 10.1109/ACCESS.2024.3454211.
- [18] K. Matthew and T. John-Dewole, "Federated learning-driven intrusion detection in cloud-IoT settings: A security-centric survey," Lead City Univ. Postgraduate Multidisciplinary Serials, vol. 2025, no. 1, pp. 603–618, 2025.
- [19] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," FIPS 203, Aug. 13, 2024, doi: 10.6028/NIST.FIPS.203; "Module-Lattice-Based Digital Signature Standard," FIPS 204, doi: 10.6028/NIST.FIPS.204; "Stateless Hash-Based Digital Signature Standard," FIPS 205, doi: 10.6028/NIST.FIPS.205.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)