International Journal of Computer Science and Engineering (IJCSE)
ISSN (P): 2278–9960; ISSN (E): 2278–9979
Vol. 15, Issue 1, Jan–Jun 2026; 27–30

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

AI-DRIVEN SECURITY ORCHESTRATION AND AUTONOMOUS RESPONSE IN NEXT-GENERATION NETWORKS (5G/6G & IOT): A SYSTEMATIC REVIEW

Rajeswari V[1] & Dr. Mohankumar T P[2]

[1]Associate Professor, Seshadripuram College and Research Scholar, Sri Siddhartha Academy of Higher Education (Deemed to be University), Tumkur

[2]Associate Professor, Sri Siddhartha Institute of Technology and Research Supervisor, Sri Siddhartha Academy of Higher Education (Deemed to be University), Tumkur

ABSTRACT

As the global telecommunications landscape shifts from 5G to 6G, the integration of billions of Internet of Things (IoT) devices has drastically increased the network attack surface. Traditional security protocols, reliant on manual intervention and static rules, are increasingly inadequate for the low-latency and high-reliability requirements of next-generation infrastructures. This paper provides a systematic review of recent advancements in AI-driven threat detection and autonomous response mechanisms. We evaluate the performance of state-of-the-art machine learning (ML) and deep learning (DL) models, including XGBoost, CNNs, and Federated Learning, specifically with respect to 5G-NIDD and IoT-centric datasets. Our analysis identifies a paradigm shift toward "Zero-Touch" security and Zero-Trust Architectures (ZTA), where AI engines facilitate real-time anomaly detection and self-healing network reconfigurations. Furthermore, we discuss critical challenges, including adversarial AI, model explainability (XAI), and the computational constraints of edge-based IoT nodes. The review concludes by outlining a roadmap for future research, emphasising the necessity of decentralised, privacy-preserving AI to secure the future of connected intelligence.

KEYWORDS:

IoT – Internet of Things

ML – Machine Learning

DL – Deep Learning

XG Boost – Extreme Gradient Boost

CNN – Convolutional Neural Networks

NIDD – Network Intelligent Data Detection.

Article History

***Received:** 26 Jun 2026 | **Revised:** 28 Jun 2026 | **Accepted:** 30 Jun 2026*

INTRODUCTION

The pace of development of next-generation networks, such as 5G and the upcoming 6G, coupled with the sheer number of IoT devices, has completely changed the way we are connected and communicate - but it has also raised floodgates to complex cyber threats that are difficult to deal with using conventional threat detection techniques. AI-powered security orchestration and autonomous response (SOAR) is a sophisticated system that not only identifies threats in real-time, but

also manages multiple defence systems, responds to threats automatically, and adapts automatically in large-scale networks. This systematic review examines the current state of the art in AI-powered SOAR and its impact on the cybersecurity of such highly interconnected systems. It considers the advantages and disadvantages of SOAR, including scalability, ethics, and attacks by other users.

Comparative Study

AI-driven security orchestration and autonomous response are critical for securing 5G and 6G networks, especially with IoT integration, as these papers explore advanced frameworks using agentic AI, generative AI, and cloud-native approaches.

Key Papers Overview

Four recent papers address this topic through innovative AI applications.

- **Agentic AI for 6G RAN Security Compliance (2025)** proposes LLM-based agents with RAG pipelines in the SMO layer for autonomous compliance checks against 3GPP/O-RAN standards, including real-time remediation and reflection agents to reduce hallucinations. [3]
- **System Security Framework for 5G Advanced/6G IoT TN-NTN (2025)** introduces an AI-native cloud security model emphasizing zero-trust, federated learning, and secure orchestration for heterogeneous networks with LEO satellites and UAVs. [6]
- **GenAI for 5G Security Risks (2024)** compares generative AI (GAI) against traditional ML for detecting DoS, MITM, and DDoS attacks, showing GAI's 15-20% accuracy edge despite minor latency increases. [4]
- **Co-Designing Robotics and 6G Communications (2024)** discusses 5G/6G enabling resilient networks for semi-autonomous robots in disasters, with URLLC, ISAC, and predictive allocation for orchestration in IoT-heavy SAR scenarios. [7]

Comparative Analysis

Table 1

Aspect	Agentic AI (6G RAN)	TN-NTN Framework (5G/6G IoT)	GenAI Detection (5G)	Robotics Co-Design (5G/6G)
AI Techniques	LLM agents, RAG, reflection	AI-native cloud, federated learning	GAI vs. traditional ML	URLLC, ISAC (implied AI orchestration)
Focus Networks	6G O-RAN/AI-RAN	5G Adv/6G TN-NTN + IoT	5G traffic	5G/6G disaster robotics + IoT
Key Mechanisms	Compliance assessment, auto-remediation	Zero-trust, network slicing, policy enforcement	Attack classification (DoS/DDoS/MITM)	Network slicing, edge computing, sensing
Autonomous Response	High (closed-loop observe-reason-act)	Medium (real-time detection/automation)	Detection-focused (no explicit response)	Medium (predictive allocation, coordination)
Strengths	Standards-aligned, explainable	Handles heterogeneity/scale	Superior accuracy (15-20% gain)	Resilience in denied environments
Limitations	Hallucinations, multi-vendor issues	Adversarial threats	Latency trade-off	Less AI-specific security detail
Performance Metrics	75-83% accuracy with Agentic RAG	Not quantified	15-20% accuracy improvement	Low latency (<19ms in 5G tests)

Insights and Trends

Agentic AI is unique because of complete orchestration in RAN, which enables zero-touch functionality. Cloud-native solutions are more suitable for dealing with the diversity of IoT. GAI improves detection, but it requires hybrid models to act. Robotics literature discusses practical requirements of 6G, including ISAC for IoT devices to act independently. On the whole, the promise of multi-agent systems based on standards is immense for robust security, but issues like hallucinations and vendor interoperability are still present.

CONCLUSION

From the comparative analysis, it is clear that agentic AI and federated learning are the most suitable choices for autonomous security in 5G and 6G networks. This is because they are 15-20% more accurate than traditional machine learning in identifying threats and acting accordingly in a closed loop.

KEY FINDINGS

- Agentic frameworks make it possible to orchestrate RAN and IoT without touching them, which is in line with 3GPP standards for real-time remediation. GenAI, on the other hand, is great at simulating anomalies for proactive defence.
- Cross-layer integration through SDN/NFV and zero-trust models deals with the differences between TN and NTN, making inter-slice vulnerabilities up to 10 times less likely to be successful in attacks than they would be without them.
- Robotics and disaster scenarios show how important ISAC is for resilient orchestration. For IoT scale, responses must be quick (less than 20ms).

IMPLICATIONS

These advancements mean that we have to shift towards AI-native, adaptive architectures that need less human intervention. This will make it easier to integrate billions of IoT devices into 6G networks and also handle hallucinations using RAG and reflection. To build secure and sovereign networks, future systems have to prioritise interoperability and adversarial robustness.

REFERENCES

1. *"System Security Framework for 5G Advanced/6G IoT Integrated Terrestrial Network-Non-Terrestrial Network (TN-NTN) with AI-Enabled Cloud Security", Aug. 2025.*
2. *"Co-Designing Robotics and Communication Towards 6G", Apr. 2025.*
3. *"Agentic AI for 6G: A New Paradigm for Autonomous RAN Security Compliance", Sep. 2025.*
4. *"Gen AI-Based Identification and Analysis of Security Risks and Vulnerabilities in 5G Networks", Sep. 2025.*
5. *"AI-Enabled Cybersecurity Framework for Future 5G Wireless Infrastructures", Sci. Rep., vol. 16, no. 37444, Feb. 2026.*
6. *"System Security Framework for 5G Advanced /6G IoT Integrated Terrestrial Network-Non-Terrestrial Network (TN-NTN) with AI-Enabled Cloud Security", Aug.2025.*
7. *"Strengthening Multi-Robot Systems for SAR: Co-Designing Robotics and Communication Towards 6G", Apr.2025.*