iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VII **Month of publication:** July 2025

DOI: https://doi.org/10.22214/ijraset.2025.73249

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

AI-Driven Cyber Threat Detection and Mitigation in 5G and Beyond: Enhancing Security in the Telecom Industry - A Survey and Comparative Analysis

Kshitij Nirdhar[1], Amit Hatekar[2]
[1]*Undergraduate Student, Department of Electronics and Telecommunication Thadomal Shahani Engineering College*
[2]*Associate Professor, Department of Electronics and Telecommunication Thadomal Shahani Engineering College*

Abstract: ***The rise of 5G and Beyond-5G (B5G) networks has revolutionized the telecom industry, enabling high-speed, low-latency communication and massive IoT connectivity. However, these advancements have introduced complex and evolving cyber threats. Traditional security systems are no longer sufficient to defend against zero-day attacks, adversarial manipulations, and sophisticated intrusions. This pa- per provides a comprehensive survey and comparative analysis of AI-driven cyber threat detection and mitigation techniques in 5G/B5G networks, covering machine learning (ML), deep learning (DL), reinforcement learning (RL), and hybrid AI approaches. A layered AI-security architecture is proposed, and each method is evaluated across multiple dimensions such as accuracy, scalability, real-time feasibility, and computational complexity. The study also highlights future directions, including edge AI, federated learning, explainable AI (XAI), and quantum AI, offering a roadmap for secure and intelligent next-generation networks.***

I. INTRODUCTION

With the deployment of 5G networks and the emergence of B5G technologies, telecom systems now sup- port smart cities, autonomous vehicles, industrial automation, and healthcare systems. This exponential growth brings increasing attack surfaces and challenges traditional security methods.

AI, particularly ML, DL, and RL, offers promising capabilities in threat detection, anomaly identification, and automated response.

This paper presents a unified view of how AI methods are reshaping cybersecurity in 5G and B5G, while also comparing their strengths, limitations, and applicability in real-world telecom infrastructure.

II. AI-ENHANCED CYBERSECURITY ARCHITECTURE IN 5G/B5G

AI-driven security can be embedded across a layered architecture to enable proactive, adaptive, and scalable threat management. The following layers represent a typical AI-enhanced cybersecurity pipeline in 5G and Beyond networks[1, 2]:

1) Data Collection Layer: Collects raw traffic and telemetry data from IoT devices, mobile endpoints, base stations, and network slices.
2) Preprocessing & Feature Engineering Layer: Cleanses, normalizes, and extracts relevant statistical or time-series features from network traffic using techniques like PCA or embedding methods.
3) Detection Layer: Applies various AI models including supervised ML (e.g., SVM), deep learning (e.g., CNN, LSTM), and reinforcement learning (e.g., DQN) to detect anomalies, intrusions, and adversarial patterns[3, 6].
4) Response Layer: Dynamically triggers alerts, blocks traffic, or adjusts firewall and access control policies using automated orchestration tools.
5) Learning & Feedback Layer: Continuously updates detection models using feedback loops and online learning, ensuring resilience to zero-day attacks and evolving threat landscapes[7, 5].

Example: Leading telecom vendors like *Ericsson* and *Huawei* are deploying edge-based AI models integrated with federated learning at base stations to detect threats locally while maintaining global model consistency [2].

Figure 1: AI-based cybersecurity pipeline in 5G/B5G networks

III. AI-BASED CYBERSECURITY TECHNIQUES

A. *Machine Learning (ML)*

ML is widely used for analyzing network traffic patterns and identifying threats [11, 6]. Techniques include:

- Supervised learning (e.g., SVM, Random Forest) for classifying known attacks.
- Unsupervised learning (e.g., K-Means, Autoencoders) for anomaly detection.
- Semi-supervised learning to combine labeled and unlabeled data effectively.

B. *Deep Learning (DL)*

DL offers better feature extraction and accuracy in complex scenarios [7, 3]:

- CNNs for spatial pattern detection in packet data.
- RNNs and LSTMs for sequential/time-series attack recognition.
- GANs for generating synthetic threats to improve model robustness.

C. *Reinforcement Learning (RL)*

RL adapts in real-time by learning optimal defense strategies [2, 1]:

- Deep Q-Learning (DQN) for intelligent security policies.
- Multi-agent RL for large-scale network threat response coordination.

IV. COMPARATIVE ANALYSIS

Table 1: Comparison of AI-Based Cybersecurity Techniques

Technique	Accuracy	Real-Time Feasibility	Comp. Cost	Interpretability	Use Case
Supervised ML	High	Medium	Medium	High	Signature-based IDS
Unsupervised ML	Medium	High	Low	Medium	IoT anomaly detection
Deep Learning	Very High	Medium (Edge)	High	Low	Encrypted traffic analysis
Reinforcement RL	High	High (post-training)	Very High	Medium	Autonomous firewall
Hybrid Models	Very High	Medium	Very High	Low	Next-gen SOC sys- tems

V. CHALLENGES

The integration of AI into telecom cybersecurity introduces multiple technical, operational, and regu- latory hurdles [3, 5]. These challenges must be addressed to ensure scalable and resilient protection mechanisms in 5G/B5G environments.

1) Data Privacy: High-quality labeled datasets are crucial for training AI models. However, telecom data often contains sensitive personally identifiable information (PII), making it subject to strict regulations such as GDPR and CCPA. Acquiring and labeling such data is also resource-intensive [7, 6]..

2) Adversarial AI: AI models, particularly deep learning systems, can be deceived by carefully crafted adversarial inputs. Attackers exploit this vulnerability to bypass detection or trigger false alarms [3].

3) Computational Load: Advanced AI models, including deep neural networks and reinforcement learning agents, require significant computational resources. This imposes challenges for deploy- ment on edge devices and routers in a resource-constrained telecom environment [1].

4) Real-Time Demand: Cybersecurity systems in telecom must operate in real-time with ultra-low latency. Any delay in threat detection or response can disrupt critical services and lead to financial or reputational damage [2].
5) Interoperability and Standardization: Implementing AI-based security across heterogeneous telecom infrastructure is challenging. Different vendors and network components often lack stan- dardized APIs or formats, hindering seamless integration and coordination [5].

VI. FUTURE TRENDS

As cyber threats become increasingly sophisticated, several emerging AI technologies and paradigms are expected to redefine the cybersecurity landscape for 5G and B5G networks [1, 2, 3, 4, 5]..

1) Edge AI: Deploying AI models at the network edge (e.g., base stations, edge routers) enables real- time threat detection with minimal latency [1]. This is essential for latency-sensitive applications in telecom, such as autonomous vehicles and remote surgeries.
2) Federated Learning: Federated learning allows multiple telecom nodes to collaboratively train AI models without sharing raw user data [2]. This enhances privacy and complies with regulatory constraints, making it suitable for distributed 5G infrastructures.
3) Explainable AI (XAI): As AI systems make high-stakes decisions in security, explainability becomes critical . XAI provides interpretable outputs that help human operators understand why an input was flagged as malicious, improving trust, transparency, and regulatory compliance [3].
4) Quantum AI: Quantum computing holds promise for dramatically accelerating data processing and threat detection algorithms. Quantum-enhanced AI models could one day outperform classical approaches in handling encrypted or obfuscated traffic patterns [4].
5) Digital Twins for Cybersecurity: A digital twin is a virtual replica of the telecom network that continuously mirrors real-time operations. It can be used to simulate cyberattacks and evaluate AI-driven defense mechanisms without affecting the physical infrastructure [5].

VII. USE CASES AND APPLICATIONS

A. *Intrusion Detection Systems (IDS)*

AI-powered IDS can automatically learn patterns of malicious traffic and detect intrusions in real-time [6, 7]. Telecom companies deploy AI-based IDS at network gateways to identify anomalies and zero-day attacks with high accuracy.

B. *Spam and Fraud Detection*

Telecom operators use ML models to detect fraudulent messages, SIM card cloning, and phishing ac- tivities. AI systems analyze call and messaging behavior to block suspicious activities and notify users promptly [11].

C. *Traffic Analysis and Anomaly Detection*

Deep learning models such as autoencoders and CNNs are used to analyze encrypted traffic without needing payload decryption. This technique is crucial for detecting malware communication in secure 5G tunnels [1, 3].

D. *Self-Healing Networks*

Using reinforcement learning, telecom networks can dynamically reconfigure their security policies and restore operations after a cyber incident [2]. These self-healing systems minimize human intervention while maintaining service continuity.

E. *Real-Time Network Slicing Security*

5G networks use network slicing to allocate virtual resources. AI monitors each slice for compliance and isolation, detecting lateral movement of threats across slices [5].

F. *Jio's AI-Driven Network Optimization*

Reliance Jio leverages machine learning models to optimize network traffic and detect anomalies across its 5G backbone. AI is used to dynamically reroute data to prevent congestion and flag suspicious behavior indicative of cyber threats. The company also integrates AI-powered facial recognition and KYC validation in its customer onboarding pipeline [14].

G. Airtel's Xstream Fiber Security

Airtel has partnered with Norton to offer AI-enabled malware detection at the router level for home broadband users. Their real-time analytics platform uses behavior-based intrusion detection to pre- vent threats before they propagate through the home network. Airtel's research division also explores federated learning for smart city 5G security deployments [15].

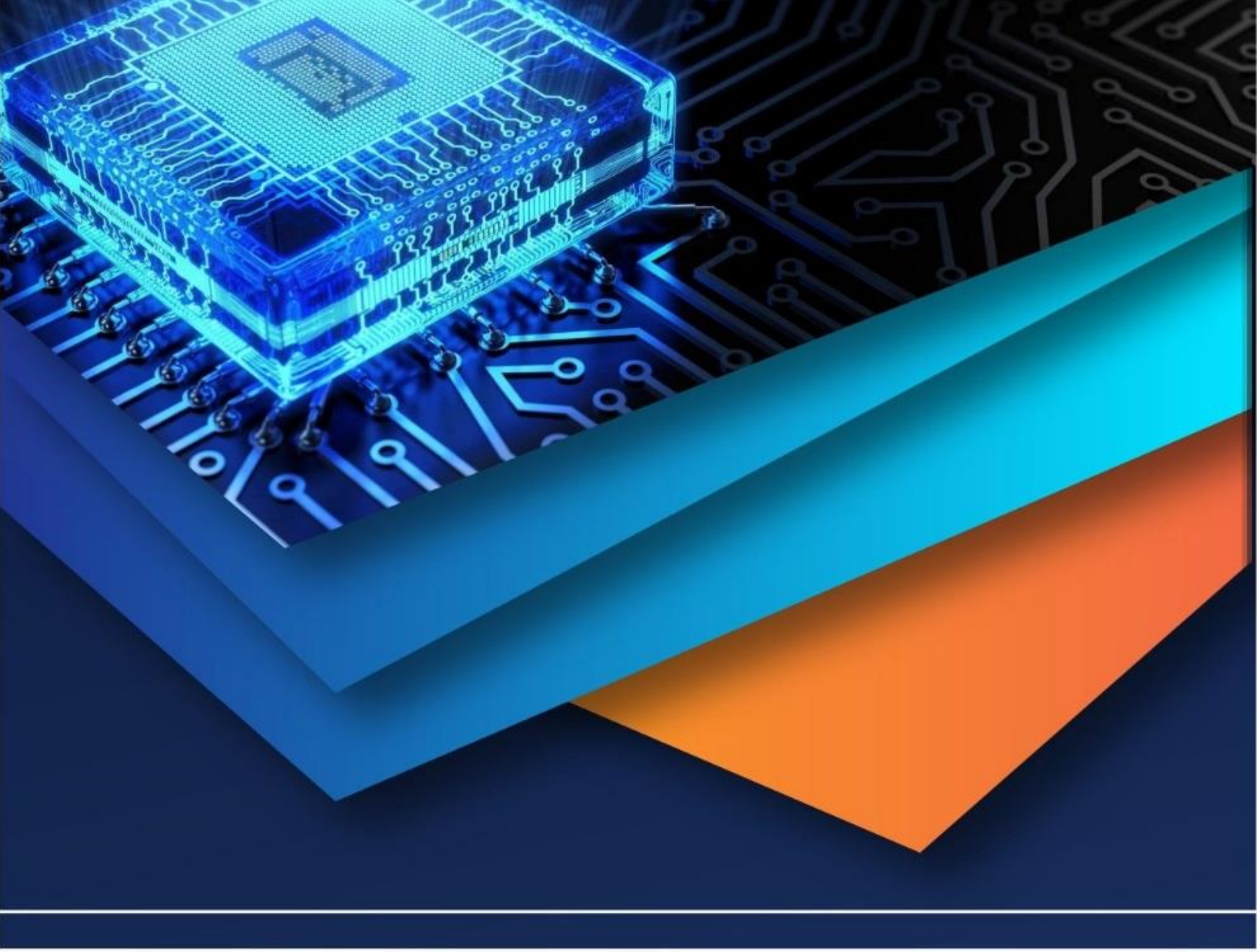
VIII. CONCLUSION

AI is transforming cybersecurity in 5G and B5G telecom networks by enabling intelligent threat detection and real-time response. This paper surveyed ML, DL, and RL techniques, proposed a layered AI-based security architecture, and highlighted real-world telecom use cases.

While challenges like data privacy, adversarial attacks, and latency persist, emerging trends such as Edge AI, Federated Learning, and Explainable AI show great potential. Moving forward, robust and interpretable AI solutions will be key to building secure and resilient telecom infrastructures.

REFERENCES

[1] Y. Chen, et al., "Edge AI: On-Demand Deep Learning Model Co-Inference with Device-Edge Syn- ergy," IEEE Transactions on Computers, vol. 69, no. 10, pp. 1526–1539, 2020.
[2] T. Li, et al., "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Processing Magazine, vol. 37, no. 3, pp. 50–60, 2020.
[3] A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on Explainable Artificial Intel- ligence (XAI)," IEEE Access, vol. 6, pp. 52138–52160, 2018.
[4] M. Schuld and F. Petruccione, Supervised Learning with Quantum Computers, Springer, 2018.
[5] A. Ferrari, et al., "Digital Twin for Cybersecurity: Concepts, Applications and Research Opportu- nities," IEEE Access, vol. 10, pp. 22723–22745, 2022.
[6] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in Proc. ICISSP, 2018.
[7] N. Moustafa, et al., "ToN IoT: The New Trend for Testing AI-Based IoT Security Solutions," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6393–6406, 2021.
[8] AUTOSAR Consortium, "AUTOSAR Adaptive Platform Specifications," [Online]. Available: https://www.autosar.org
[9] Tesla Inc., "Vehicle Service and Diagnostics Overview," 2022. [Online]. Available: https://www.tesla.com
[10] BMW Group, "Predictive Maintenance in Production and Aftersales," 2021. [Online]. Available: https://www.bmwgroup.com
[11] M. Mohri, A. Rostamizadeh, and A. Talwalkar, Foundations of Machine Learning, 2nd ed., MIT Press, 2018.
[12] L. A. Zadeh, "Fuzzy sets," Information and Control, vol. 8, no. 3, pp. 338–353, 1965.
[13] T. J. Ross, Fuzzy Logic with Engineering Applications, 3rd ed., Wiley, 2010.
[14] Reliance Jio, "AI and ML powering Jio's next-gen 5G network infrastructure," [Online]. Available: https://www.jio.com
[15] Airtel, "Airtel Xstream Fiber and AI-powered network security initiatives," [Online]. Available: https://www.airtel.in



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY