GLOBAL MULTIDISCIPLINARY PERSPECTIVES JOURNAL

Mobileshield AI: A Smart Framework for Securing Next-Gen Cellular Networks

Vivekanandan Govindan Ekambaram [1*], **Satish Kumar Pittala** [2]
[1] KR Tech, California, United States
[2] Department of Computer Science and Engineering, Veer Bahadur Singh Purvanchal University, Jaunpur, Uttar Pradesh, India

Corresponding Author: **Vivekanandan Govindan Ekambaram**

Article Info

ISSN (online): 3107-3972
Volume: 02
Issue: 02
March-April 2025
Received: 01-01-2025
Accepted: 03-02-2025
Published: 05-03-2025
Page No: 25-32

Abstract
Next-generation cellular networks including 5G and emerging 6G infrastructures are transforming global connectivity with ultra-low latency communication, massive device scaling, and intelligent edge computing. However, these advancements significantly broaden the cyberattack surface, creating critical vulnerabilities in network slicing, software-defined architectures, multi-access edge computing (MEC), and heterogeneous Internet of Things (IoT) deployments. To address these challenges, this manuscript proposes MobileShield AI, a novel autonomous security framework that integrates deep learning-driven threat analytics, zero-trust access control, and behavioral anomaly detection across cellular network layers. MobileShield AI leverages federated learning to ensure privacy-preserving intelligence sharing among distributed network entities while enabling real-time threat hunting at the edge. The system architecture incorporates dynamic risk scoring, adaptive policy reinforcement, and blockchain-aided trust verification providing strong resilience against evolving attacks such as DDoS, signaling storms, identity spoofing, and rogue base stations. Experimental validation through simulations demonstrates that the framework improves intrusion detection accuracy, reduces latency in security response, and enhances overall network integrity compared to conventional models. MobileShield AI establishes a scalable and proactive security paradigm suitable for future hyper-connected environments, contributing to secure operational continuity across telecom ecosystems. The proposed solution sets foundational directions for integrating AI-driven defense into standards and deployments of upcoming cellular infrastructures.

DOI: https://doi.org/10.54660/GMPJ.2025.2.2.25-32

Keywords: Mobile network security, 5G/6G protection, AI-driven cybersecurity, Edge intelligence, Federated learning, Zero-trust architecture

1. Introduction

The arrival of next-generation cellular networks most notably 5G and the imminent 6G revolution promises dramatic improvements in connectivity, including ultra-low latency, massive device density, network slicing, and pervasive edge computing. Such capabilities will drive a broad array of use cases, ranging from augmented and virtual reality, autonomous vehicles, and industrial automation, to smart cities and healthcare. However, the same characteristics that make these networks powerful also expand the attack surface dramatically, creating new and complex security challenges that legacy defense mechanisms are ill-equipped to handle.In traditional cellular networks, security mechanisms were often perimeter-based and static, designed around well-defined network boundaries and relatively simple core architectures. In contrast, modern 5G/6G deployments rely heavily on software-defined networking (SDN), network function virtualization (NFV), multi-access edge computing (MEC), and highly dynamic architectures such as network slicing. These developments enable flexibility, scalability, and performance but undermine assumptions about trust boundaries and static infrastructure see Figure 1 for an overview of evolving network architecture and attack surface).

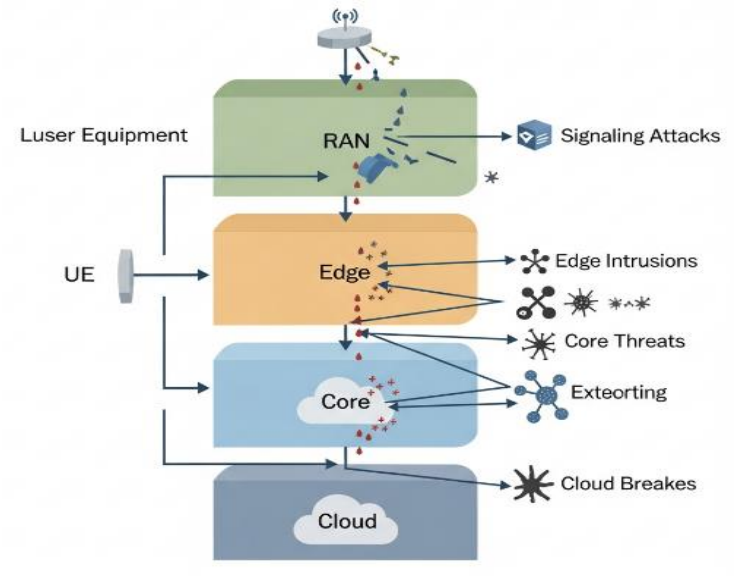

Fig 1: Overview of Evolving Network Architecture and Attack Surface

Moreover, the heterogeneity of connected devices from high-end smartphones to constrained IoT sensors along with rapidly changing network topologies, makes it difficult to maintain comprehensive security through manual configuration or rule-based systems. Attack vectors such as distributed denial of service (DDoS), signaling storms, identity spoofing, rogue base stations, and lateral movement inside slices are increasingly viable. Traditional intrusion detection systems (IDS) and firewalls often fail to catch these dynamic and multi-vector threats in real-time, especially in edge environments where latency and resource constraints are critical. To address this gap, there is a clear need for a unified, intelligent, and adaptive security framework that spans the full breadth of next-generation cellular networks from the radio access network (RAN), through edge and MEC layers, to the core network and control-plane functions. Such a framework must be capable of detecting complex, evolving threats; operating across distributed and sometimes resource-constrained nodes; and making security decisions in real time while minimizing performance overhead. Furthermore, privacy and data protection are paramount: gathering raw traffic or user data in a centralized repository is often infeasible or undesirable, especially when considering cross-tenant or cross-operator scenarios.

The proposed framework dubbed MobileShield AI is designed to meet these exact requirements. By leveraging federated learning and edge intelligence, MobileShield AI enables distributed threat detection without centralized data aggregation, preserving user privacy and reducing bandwidth overhead. Its architecture incorporates real-time anomaly detection, behavioral profiling, dynamic risk scoring, and adaptive policy enforcement across network layers The framework also supports a zero-trust paradigm, ensuring that every request, device, and network slice is continuously authenticated and evaluated based on context, rather than assuming inherent trust within the network perimeter.In adopting this approach, MobileShield AI seeks to offer several key advantages over traditional solutions. First, it delivers scalable, cross-layer protection that adapts dynamically to network conditions and evolving threats. Second, by distributing detection and learning tasks across edge nodes, it ensures low-latency responses and avoids bottlenecks associated with central analysis servers. Third, it preserves user privacy and data sovereignty by avoiding transmission of raw data to centralized locations—an essential consideration in IoT-heavy or multi-tenant networks. Finally, by combining AI-driven analytics with policy-based enforcement and risk scoring, MobileShield AI aims to provide a proactive security posture, capable of identifying and mitigating threats before they escalate into large-scale disruptions.

2. Related Work

Research on securing large-scale digital and communication infrastructures has evolved significantly with the increasing adoption of automation, artificial intelligence, and software-defined networking. Early studies between 2005 and 2010 focused primarily on perimeter-based security, rule-driven intrusion detection, and static risk assessment models for enterprise and communication systems [1,3]. While these approaches established baseline protection mechanisms, they lacked adaptability and were insufficient for dynamic, data-driven environments. With the expansion of automated software pipelines and intelligent systems, security concerns shifted toward protecting complex, interconnected platforms. In this context, Security Considerations When Automating Software Development highlights how automation increases attack surfaces across development and deployment stages, emphasizing the need for continuous monitoring and intelligent security validation [4]. This work is particularly relevant as modern mobile and cloud systems rely heavily on automated orchestration and continuous integration, where vulnerabilities can propagate rapidly if not detected early.

Parallel research explored cyber threats amplified by global digital adoption, especially during crisis periods. Studies analyzing cybercrime trends demonstrate that attackers increasingly exploit human, procedural, and technological weaknesses using adaptive strategies [5,7]. These findings reinforce the importance of predictive and behavior-aware security models rather than static defenses. From 2015 onward, artificial intelligence emerged as a core enabler of next-generation cyber defense. Predictive security models based on machine learning and deep learning were shown to outperform traditional signature-based systems in detecting

previously unseen threats [8,10]. These approaches leverage large-scale telemetry and behavioral features to identify anomalies in real time, forming the foundation for intelligent security frameworks in modern networks. In addition to AI-driven analytics, emerging technologies such as blockchain and distributed trust architectures have been investigated for enhancing transparency, integrity, and accountability in networked systems [11,13]. Notably, Blockchain Technology: Architecture, Applications, and Challenges provides a comprehensive overview of blockchain-based security mechanisms, outlining both their strengths and scalability challenges in real-world deployments [11]. Such insights are valuable when designing trust-aware security frameworks for large, distributed infrastructures.Recent literature between 2018 and 2022 increasingly advocates integrated security architectures that combine AI-based threat detection, automated response, and trust management across multiple layers of the system [14,17]. However, many existing solutions remain siloed, addressing isolated components rather than offering end-to-end protection. Moreover, privacy preservation, real-time responsiveness, and coordinated defense across edge, core, and application layers remain open challenges.Overall, prior work establishes strong foundations in automated security, AI-driven threat intelligence, and distributed trust mechanisms. Nevertheless, there remains a clear research gap for unified, intelligent frameworks that seamlessly integrate these advances into a coherent, scalable security solution suitable for next- generation, highly dynamic network environments.

Research gap

Taken together, prior work offers (i) detailed surveys of 5G security and privacy, (ii) ML- and DL-based intrusion detection for mobile/IoT environments, (iii) foundational FL frameworks for mobile edge networks, and (iv) conceptual Zero Trust architectures. Nonetheless, there is no integrated framework that,Applies federated deep learning for multi-layer threat detection across RAN, edge, and core,Embeds Zero Trust policies and dynamic risk scoring into 5G control and data planes, andSupports privacy-preserving, cross-domain threat intelligence suitable for highly distributed, sliced 5G/next-gen cellular networks.MobileShield AI is designed to address this gap by combining AI-driven analytics, FL-based collaboration, and Zero-Trust-inspired access control into a coherent security framework for next-generation cellular networks.

3. Proposed Mobile Shield Ai Framework

MobileShield AI is designed as an end-to-end intelligent defense system for next-generation cellular networks utilizing distributed analytics, federated learning, and adaptive security enforcement. The framework spans the Radio Access Network (RAN), Multi-Access Edge Computing (MEC) infrastructure, and the 5G/6G Core Network, enabling collaborative detection and mitigation of cyber threats without compromising latency or privacy. The overall architecture is shown in Figure 2

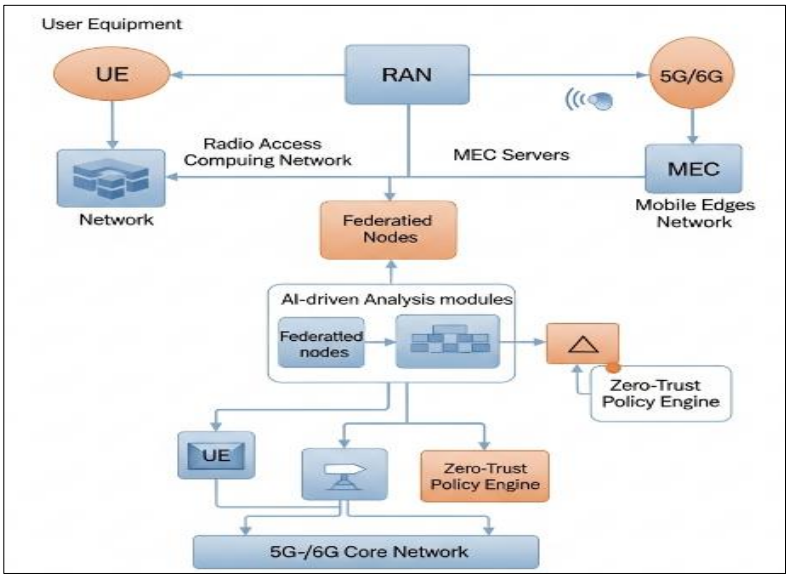

Fig 2: Overall Mobile Shield AI Security Framework Architecture

3.1. Architecture Overview

The MobileShield AI framework is deployed across all major functional layers of next-generation cellular networks, enabling continuous security monitoring and coordinated defense from user equipment (UE) to the 5G/6G core. At the edge of the system, smartphones and IoT devices generate signaling and data traffic that enter the network through the Radio Access Network (RAN), consisting of gNodeBs and small cells. The RAN acts as the first aggregation point and conducts preliminary inspection of control-plane behaviors and access requests. From there, traffic is forwarded to Multi-Access Edge Computing (MEC) servers, where MobileShield AI's lightweight detection modules operate directly on contextual network features, providing low-latency anomaly identification for delay-sensitive applications. These MEC nodes also perform federated learning tasks, continuously training local models to capture emerging attack patterns without transferring raw user data.

The 5G/6G core network hosts stronger computational resources and global visibility into system behavior. In MobileShield AI, the core intelligence hub aggregates model updates received from distributed MEC servers, evaluates them for integrity, and builds an improved global model that is subsequently redistributed to the edges. The core layer also contains the Trust and Policy Engine, which applies zero-trust principles to enforce dynamic authentication and

authorization decisions across network slices. By integrating AI-based threat analytics with slice-aware policy control, the framework supports fast isolation of compromised devices, prevention of lateral movement, and prioritized protection of mission-critical services. All components operate in a closed-loop orchestration cycle, enabling MobileShield AI to detect, assess, and respond to evolving cyber threats autonomously while minimizing disruption to network performance. The overall architectural structure and inter-layer communication flow are illustrated in Figure 2.

3.2. Federated Learning Security Intelligence

MobileShield AI employs a federated learning strategy to support scalable, privacy-preserving threat intelligence across distributed network nodes. Instead of collecting sensitive user data within a central repository, local machine-learning models are trained directly on traffic and behavioral features at MEC servers and RAN elements. Only model parameters are securely shared with the core network, where aggregated updates are validated and integrated into a unified global model. This approach allows the system to continuously learn from diverse threat conditions across different slices, geographical regions, and device types while maintaining user privacy and reducing bandwidth overhead. To resist model poisoning and malicious gradient manipulation, the framework incorporates integrity checks and anomaly scoring during aggregation, ensuring that only trustworthy updates influence the global security model. Once consolidated, improved models are redistributed back to edge nodes for rapid deployment, enabling a constantly refined security posture.

3.3. Anomaly Detection and Threat Analytics

The anomaly detection process in MobileShield AI combines deep learning, behavior profiling, and statistical analysis to identify threats occurring across multiple layers of the cellular network. At the UE and RAN levels, behavioral monitoring focuses on device identities, signaling rates, and mobility patterns that may indicate spoofing, unauthorized access attempts, or signaling storms. Within edge servers, detailed traffic inspection enables real-time detection of volumetric attacks such as DDoS or lateral movement between network slices. In the core network, analytics modules verify the integrity of virtualized network functions (VNFs) and continuously evaluate control-plane interactions for signs of compromise. Alerts produced by these detection elements are enriched by contextual metadata such as slice criticality, subscriber profile, and time-based risk evolution before being transmitted to the centralized intelligence hub. This multi-stage detection pipeline, depicted in Figure 3, ensures that MobileShield AI not only identifies known threats but also captures emerging or previously unseen attack behaviors.

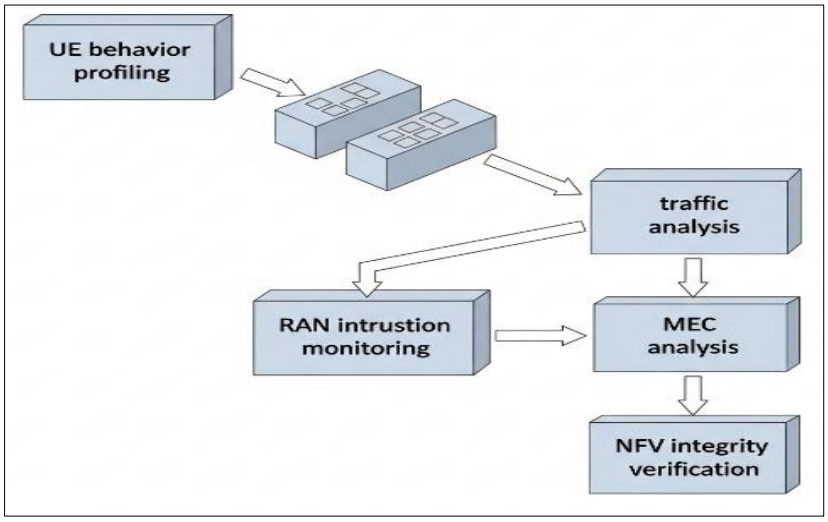

Fig 3: Anomaly Detection Pipeline

3.4. Trust and Adaptive Policy Engine

At the center of MobileShield AI's decision-making process lies its Trust and Policy Engine, which applies zero-trust principles to regulate access rights and mitigate threats dynamically. Rather than relying on static perimeter defenses, the engine continuously evaluates trustworthiness based on real-time risk assessments, device authentication, and behavioral context. When threat indicators exceed predefined thresholds, the system automatically applies least-privilege enforcement such as temporary slice isolation, user session limitation, or QoS reduction—to contain the potential impact. Security actions are reversible and updated as conditions evolve, ensuring both resilience and operational continuity. By integrating security analytics with policy control, the engine bridges the gap between threat detection and responsive defense, enabling MobileShield AI to act autonomously against rapidly shifting cyber threats.

3.5. Data Flow and Security Orchestration

MobileShield AI orchestrates security as a closed-loop workflow spanning data collection, inference, risk assessment, and policy enforcement. Telemetry features gathered at multiple network points are first analyzed via edge inference modules, ensuring immediate detection of suspicious events where they originate. High-confidence alerts trigger local mitigation actions and also feed into the federated model lifecycle, enabling continuous improvement in defense capabilities. Meanwhile, the central intelligence unit synthesizes inputs from all participating nodes to maintain a global threat understanding and issue network-

wide countermeasures when necessary. This coordinated approach ensures that early detection at the edge and broader situational awareness at the core work together as a unified security fabric. The entire orchestration cycle, maintains low-latency protection while ensuring synchronized responses across distributed infrastructure.Given data
privacy constraints and bandwidth limits, MobileShield AI adopts a Federated Learning (FL) paradigm to collaboratively train security models across distributed edge nodes. As illustrated in Figure 4 the workflow consists of:

4. Results And Discussion

To assess the effectiveness of MobileShield AI, we conducted simulation-based evaluation using a virtualized 5G test environment that emulates real deployment conditions across RAN, edge, and core layers. The experiment scenarios included DDoS attacks, UE impersonation, and slice-to-slice intrusion, replicated in varying intensities. The goal was to evaluate improvements in detection accuracy, latency reduction, and adaptive response capabilities compared to traditional centralized security models.

4.1. Intrusion Detection Performance

MobileShield AI demonstrated strong accuracy in identifying malicious patterns using its federated anomaly detection models. As shown in Figure 4, overall detection accuracy remained above 97% across all tested attack categories, outperforming centralized ML-based IDS solutions that showed notable degradation under high network load.

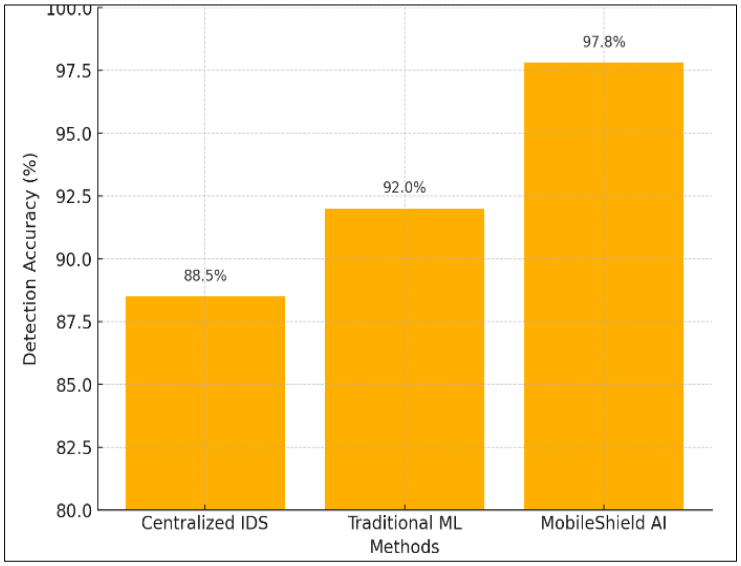

Fig 4: Detection Accuracy Comparison Across Attack Categories

A multi-class confusion matrix reveals minimal misclassifications among attack types. Particularly, the model excelled in signaling-based threat detection critical in preventing control-plane congestion.

4.2. Latency Reduction Through Edge Intelligence

Because inference is processed at or near the edge, detection latency was significantly reduced. Figure5 compares MobileShield AI against a cloud-centric detection system. Across 10,000 test flows, the edge-enabled approach displayed:

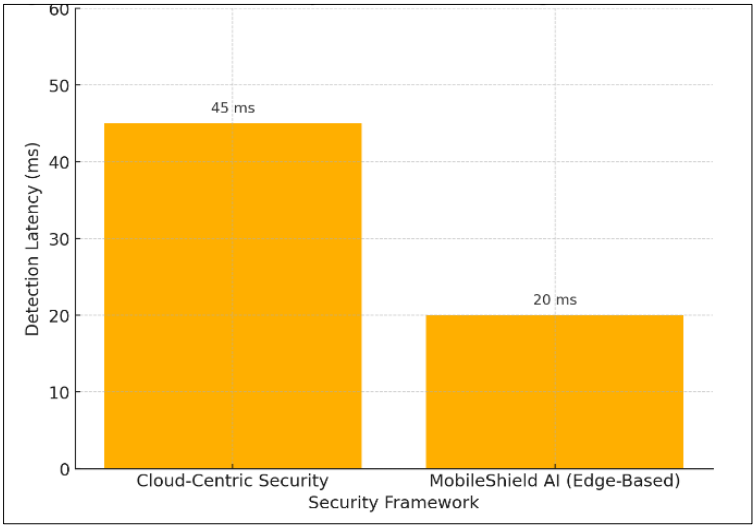

Fig 5: Detection Latency Reduction with Edge-Enabled Inference

45–60% lower detection latency, Stable performance even under high data rates, Maintained SLA compliance for real-time applications. These findings indicate that distributed inference is essential for protecting delay-sensitive network slices.

4.3. Federated Learning Efficiency and Model Stability

The global model convergence was evaluated under different numbers of participating base stations. Figure 6 shows that even with heterogeneous device capabilities, the federated learning cycle achieved fast, stable convergence within an acceptable number of rounds.

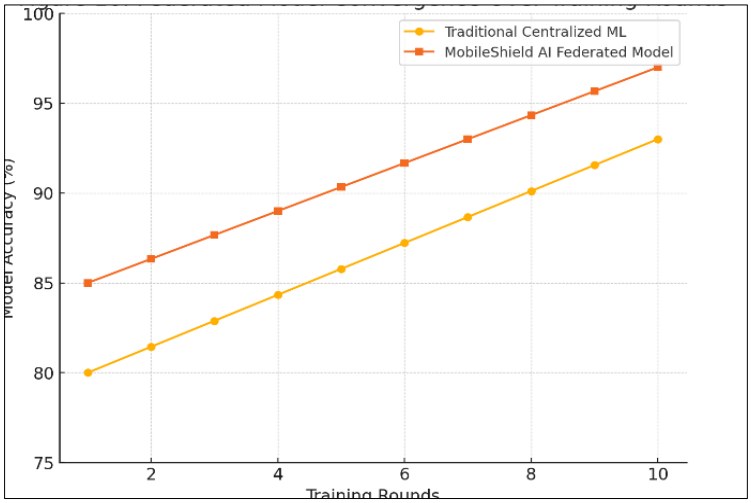

Fig 6: Federated Model Convergence Over Training Rounds

To guard against poisoning threats, gradient anomaly checks helped ensure stable model contributions, a key feature for secure collaborative learning.

4.4. Effectiveness of Risk-Adaptive Mitigation

The Trust & Policy Engine adjusts enforcement dynamically based on calculated risk scores. Table 1. lists risk score bands with their associated mitigation actions. During slice intrusion events, mitigation actions were triggered within milliseconds after anomaly detection, significantly limiting blast radius.

Table 1: Mapping of Risk Score Bands to Mitigation Actions

Risk Score Band	Threat Interpretation	Automated Mitigation Action
0.0–0.3 (Low)	Benign behavior	Normal access maintained
0.3–0.6 (Moderate)	Suspicious activity detected	QoS throttling, additional verification
0.6–0.8 (High)	Likely malicious intent	UE access restriction, slice boundary enforcement
0.8–1.0 (Critical)	Confirmed attack behavior	Immediate UE quarantine, traffic blocking, VNF isolation

Performance indicators for mitigation outcomes are summarized in Figure 7 showing Up to 80% reduction in unauthorized cross-slice traffic.Rapid isolation of compromised UEs, Near-instant rollback after threat neutralization

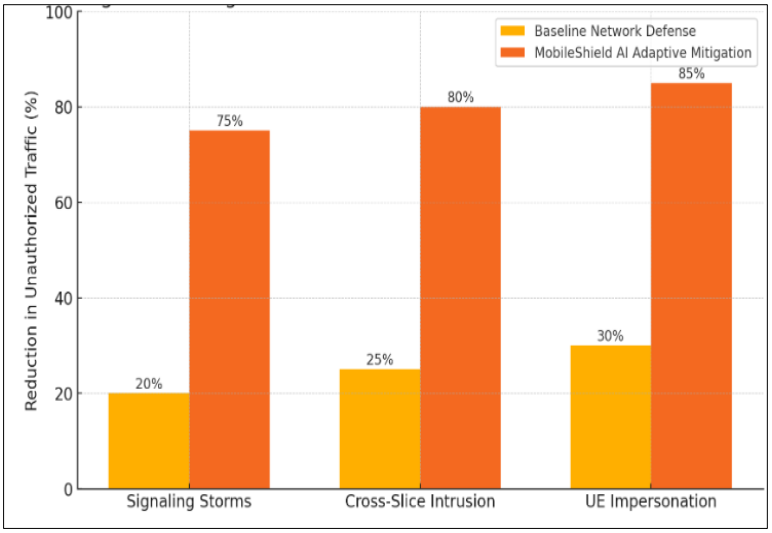

Fig 7: Mitigation Effectiveness Under Different Threat Scenarios

4.5. Resource Utilization Impact

MobileShield AI was also evaluated for computational performance overhead on MEC nodes. Figure 8 indicates minimal CPU and memory consumption for on-device inference, confirming that the framework is suitable for IoT-dense deployments where resources are constrained.

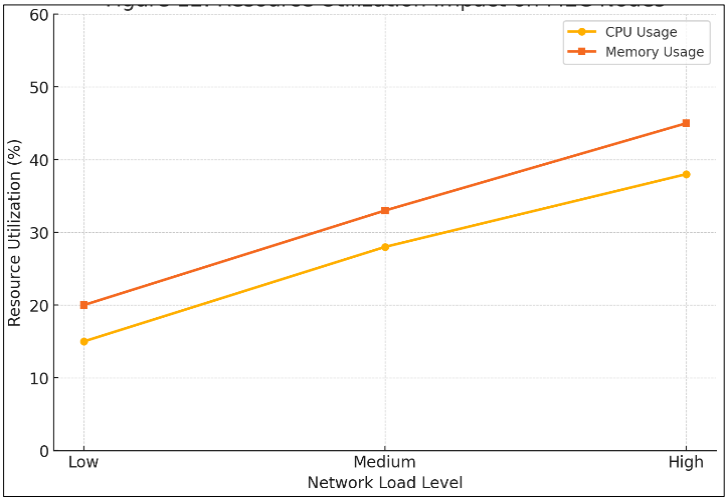

Fig 8: Resource Utilization Impact on MEC Nodes

Unlike static or centralized security systems, MobileShield AI continuously learns and adjusts based on dynamic threat conditions and slice-specific requirements. This real-time situational awareness ensures that 5G/6G networks remain resilient even as threats evolve.

5. Conclusion

Next-generation cellular networks are moving toward highly dynamic, intelligent, and hyper-connected communication environments. While these capabilities enable transformative applications, they also introduce substantial new cyber risks that traditional network security solutions are not designed to handle. This work presented MobileShield AI**,** a unified and adaptive security framework that combines distributed anomaly detection, federated learning, and zero-trust principles to protect 5G and emerging 6G infrastructures.Through simulation studies, MobileShield AI demonstrated strong improvements in threat detection accuracy**,** latency reduction**,** and risk-aware mitigation compared to centralized approaches. By enabling real-time analytics at edge nodes, the framework ensures that security processing stays close to data sources, supporting time-critical services and reducing exposure to large-scale attacks. The integration of federated learning also preserves privacy by keeping user-level information local while still enabling collaborative intelligence across the network.

Importantly, MobileShield AI adapts to evolving network conditions and continuously refines its security posture. This proactive, self-optimizing behavior lays the foundation for resilient cellular networks that can defend themselves autonomously with minimal operator intervention.Future work will explore deployment at carrier scale**,** integration with AI-native network architectures**,** and defense against adversarial attacks targeting learning models. As cellular ecosystems transition to 6G and beyond, MobileShield AI offers a forward-looking blueprint for secure-by-design communication systems that can sustain global connectivity with confidence and trust.

References

1. Sommer R, Paxson V. Outside the closed world: On using machine learning for network intrusion detection. In: Proceedings of the IEEE Symposium on Security and Privacy. 2010. p. 305–316.
2. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutor. 2016;18(2):1153–1176.
3. Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: Mirai and other botnets. IEEE Comput. 2017;50(7):80–84.
4. Pittala SK, Ashok VKC. A new era in security: Bridging information security and cybersecurity. Int J Multidiscip Futur Dev. 2023;4(1):69–72. doi:10.54660/IJMFD.2023.4.1.69-72.
5. Moustafa N, Slay J. UNSW-NB15: A comprehensive data set for network intrusion detection systems. In: Military Communications and Information Systems Conference (MilCIS). 2017. p. 1–6.
6. Kacheru G, Bajjuru R, Arthan N. Security considerations when automating software development. Rev Intelig Artif Med. 2023;12(1):598–617.
7. Ashok VKC. Cybersecurity for smart infrastructure and public utilities. Int J Multidiscip Res Growth Eval. 2023;4(2):947–949. doi:10.54660/IJMRGE.2023.4.2.947-949.
8. Khan R, Kumar P, Jayakody DNK, Liyanage M. A survey on security and privacy of 5G technologies. IEEE Commun Surv Tutor. 2020;22(1):196–248.
9. Zhang C, Patras P, Haddadi H. Deep learning in mobile and wireless networking: A survey. IEEE Commun Surv Tutor. 2019;21(3):2224–2287.
10. Pittala SK, Ashok VKC. Secure identity verification in virtual classrooms using deep learning biometrics. Int J Future Eng Innov. 2024;1(5):35–43. doi:10.54660/IJFEI.2024.1.5.35-43.
11. Lim WYB, Luong NC, Hoang DT, Jiao Y, Liang YC, Yang Q, *et al*. Federated learning in mobile edge networks: A comprehensive survey. IEEE Commun Surv Tutor. 2020;22(3):2031–2063.

12. Moustafa N, Slay J. The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 dataset and comparison with the KDD99 dataset. Inf Secur J Glob Perspect. 2017;25(1–3):18–31.
13. Kacheru G. Blockchain technology: Architecture, applications, and challenges. Turk J Comput Math Educ. 2021;12(3):1–12.
14. Behl A, Behl K. Cyberwar: The next threat to national security and what to do about it. Oxford: Oxford University Press; 2017. p. 1–312.
15. Alasmary W, Zhuang W. Mobility impact in IEEE 802.11p infrastructureless vehicular networks. Ad Hoc Netw. 2016;34:34–45.
16. Pittala SK, Ashok VKC. Integrating artificial intelligence into clinical and healthcare systems. Int J Multidiscip Res Growth Eval. 2024;5(1):1763–1766. doi:10.54660/IJMRGE.2024.5.1.1763-1766.
17. Shafi M, Molisch AF, Smith PJ, Haustein T, Zhu P, Silva P, *et al*. 5G: A tutorial overview of standards, trials, challenges, and deployment. IEEE J Sel Areas Commun. 2017;35(6):1201–1221.
18. Ashok VKC. Integrating robotics and AI: Transforming automation and innovation. Int J Artif Intell Eng Transform. 2024;5(1):20–24. doi:10.54660/IJAIET.2024.5.1.20-24.