International Journal of Technoinformatics Engineering
Vol: 02; **Issue**: 02; Jul-Dec 2025; **Pg**: 014-025

Adaptive 6G Network Security through Artificial Intelligence and Machine Learning Techniques

Mrs. Darakshan Javed Ansari[1*], Dr Alam. N. Shaikh[2]

[1]Research Scholar, Thadomal Shahani Engineering College, Assistant professor M.H.S.S. College (E&TC), Byculla, Mumbai Maharashtra, India
*Corresponding Email Id: darakshan.javed.2012@gmail.com

[2]Principal PVPPCOE, Sion, Mumbai Maharashtra, India
Email Id: dralamshaikh99@gmail.com

Received: 22th August 2025 / Accepted: 18th September 2025 / Published: 25th October 2025

Abstract: The emergence of 6G networks heralds an era of unprecedented connectivity, speed, and complexity, paving the way for revolutionary advancements such as holographic communications, autonomous systems, and the Internet of Everything (IoE). However, with these enhanced capabilities comes a host of critical security challenges, including sophisticated cyber threats, privacy vulnerabilities, and the protection of billions of interconnected devices. Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing the security landscape of 6G networks, emerging as powerful catalysts for transformation. These technologies enable proactive threat detection, adaptive defense mechanisms, and real-time response strategies, fostering a resilient and intelligent security framework. AI-driven models can dynamically detect anomalies, autonomously refine protective measures, and facilitate self-optimizing security operations, ensuring a robust and future-ready defense system. Meanwhile, ML techniques facilitate predictive analytics, continuous learning, and advanced encryption strategies, tailored to the ever-changing threat environment. Furthermore, AI plays a pivotal role in securing network slices, IoT ecosystems, and edge infrastructures, offering robust and scalable protection within a highly virtualized and decentralized network architecture [1,3]

Key innovations such as federated learning, behavioural analytics, and post-quantum cryptography serve as critical enablers for enhancing privacy, resilience, and trust in 6G environments. Despite their vast potential, challenges such as model robustness, explainability, and seamless integration with legacy systems must be addressed to fully harness the power of AI and ML in securing next-generation networks. By providing a comprehensive exploration of AI and ML-driven security solutions, this study aims to foster trust, inspire innovation, and lay the foundation for secure and reliable 6G adoption worldwide [14,15].

Problem Statement: As 6G networks evolve, they introduce new security challenges due to their complex architecture, massive connectivity, and ultra-low latency requirements. Traditional security mechanisms are inadequate to combat advanced cyber threats, including AI-powered attacks and vulnerabilities arising from edge computing and decentralized networks. Furthermore, the advent of quantum computing threatens existing cryptographic standards, rendering them obsolete and exposing 6G networks to unprecedented security risks. Therefore, there is a critical need to leverage AI, ML, and quantum-resistant security solutions to enhance threat detection, automate response mechanisms, and develop resilient cryptographic techniques to secure 6G communications against both classical and quantum cyber threats.

INTRODUCTION

The sixth generation (6G) of wireless communication networks marks a revolutionary leap forward, delivering unprecedented data speeds, ultra-low latency, vast device connectivity, and seamless integration of artificial intelligence. These innovations will lay the groundwork for transformative applications, from smart cities and autonomous vehicles to holographic communications and the Internet of Everything (IoE). Yet, this rapid evolution brings with it a complex and ever-evolving threat landscape, necessitating cutting-edge security strategies to safeguard the future of connectivity. Traditional defense mechanisms may struggle to keep pace with the vast attack surface of 6G networks, which encompasses cyberattacks on virtualized infrastructures, vulnerabilities in IoT ecosystems, and sophisticated privacy breaches. As a result, securing these next-generation networks requires a paradigm shift—one that embraces intelligence, adaptability, and automation. Within this landscape, Artificial Intelligence (AI) and Machine Learning (ML) serve as foundational pillars in redefining 6G security. With their remarkable ability to process vast streams of data in real time, detect anomalies, and anticipate emerging threats,

these technologies have become indispensable in safeguarding the resilience and integrity of next-generation networks. By leveraging intelligent threat detection, predictive analytics, and autonomous decision-making, AI and ML pave the way for proactive and scalable security solutions. From protecting IoT ecosystems and securing network slices to developing post-quantum cryptographic frameworks, these technologies offer a robust and resilient defense against the evolving challenges of 6G security. This study delves into the profound impact of AI and ML on safeguarding the future of wireless communication, fostering trust, and enabling the seamless adoption of 6G worldwide.

LITERATURE REVIEW

Quantum Threats, Quantum Solutions: ML Approaches to 6G Security" (2023) delves into the shortcomings of traditional encryption in the era of 6G networks, shedding light on the escalating vulnerabilities brought about by advances in quantum computing. The study underscores the urgent need for encryption algorithms and security protocols resilient to quantum threats. It explores the promise of post-quantum cryptography and quantum key distribution (QKD) as groundbreaking solutions for ensuring secure data transmission in next-generation networks.

AI and 6G Security: Opportunities and Challenges" (2021): This research explores the integration of AI in 6G networks, focusing on its dual role in enhancing security and presenting new challenges. It provides an overview of AI-enabled security solutions, discusses potential attacks on AI/ML systems, and identifies future research directions to ensure robust security in AI-driven 6G environments.

The paper "Quantum for 6G Communication: A Perspective" (2023) offers a comprehensive analysis of the integration of quantum technologies into 6G networks, with a particular emphasis on the evolution of quantum communication systems. It examines the application of quantum cryptography, specifically Quantum Key Distribution (QKD), as a robust solution for securing data transmission, making it virtually immune to interception or unauthorized access by third parties.

Quantum-Inspired Machine Learning for 6G: Fundamentals, Security, Resource Allocations, Challenges, and Future Research Directions" (2022): This study explores the application of quantum-inspired machine learning in 6G networks, highlighting the potential of quantum computing to solve computationally complex optimization challenges. It also examines the integration of Quantum Key Distribution (QKD) as a means to strengthen communication security. Additionally, the paper addresses key challenges in this evolving domain and outlines future research directions to advance the field.

The 2022 study explores a hierarchical framework for integrating Quantum Key Distribution (QKD) into federated learning within 6G networks. It emphasizes adaptive resource allocation and dynamic routing strategies to optimize deployment costs while maintaining robust security. By addressing uncertainties such as fluctuating security demands, the research validates the efficiency of the proposed model through experimental analysis.

Generative Adversarial Learning for Intelligent Trust Management in 6G Wireless Networks" (2022) The paper explores a trust management approach for 6G wireless networks, leveraging generative adversarial learning. It reviews AI-driven trust management strategies and introduces a prospective heterogeneous and intelligent 6G architecture. The study highlights how the proposed method enhances both intelligence and security, ensuring reliable and real-time communication.

The study ″Quantum-Secured Space-Air-Ground Integrated Networks: Concept, Framework, and Case Study" (2022) introduces the concept of quantum-secured space-air-ground integrated networks (SAGIN) for 6G. It presents a universal Quantum Key Distribution (QKD) service provisioning framework designed to ensure secure communication across space, air, and ground nodes. Through a detailed case study, the research demonstrates the effectiveness of this framework in dynamic and uncertain communication environments, highlighting its potential for enhancing security in next-generation networks.

The article ″6G AI Nets: Harnessing Artificial Intelligence for 6G Network Security – Impacts and Challenges" (2024) explores AI's critical role in securing next-generation 6G networks. It examines the dual nature of AI integration, highlighting both its transformative potential and the challenges it presents. The study further investigates strategic applications of AI in 6G security, proposing innovative solutions to enhance network resilience against emerging threats.

Challenges and Open Research Directions

In sixth-generation (6G) communication systems, the hyper-connected Internet of Everything (IoE) enables the extensive generation and aggregation of data, bringing forth critical privacy concerns that demand innovative security measures. The exploitation of vulnerabilities within the Internet of Things (IoT) by malicious actors can lead to breaches of data privacy, location privacy, and identity privacy, ultimately undermining trust in 6G infrastructures. Moreover, the distributed architecture of 6G networks, particularly the integration of Multi-Access Edge Computing (MEC), introduces novel attack vectors. Given its proximity to end-users and edge devices, MEC is highly vulnerable to physical tampering, man-in-the-middle attacks, and various other cybersecurity threats. Furthermore, maintaining scalability and computational efficiency in resource-constrained environments continues to be a significant challenge.

Ethical and privacy concerns further emerge in the deployment of artificial intelligence (AI) for security purposes. Addressing these challenges is imperative to the development of secure, resilient, and
reliable 6G networksThe network simulator ns-3 is highly suited for modeling diverse network architectures and technologies, making it especially valuable for capturing the complexity of next-generation 6G environments. Its modular design enables seamless customization and configuration, facilitating community contributions and broad access to various models and protocols. Furthermore, ns-3 supports detailed simulations of both wired and wireless networks, enabling the replication of high data rates and low-latency communication, which are fundamental to 6G applications. The simulator also incorporates built-in tools for monitoring key network performance metrics, such as throughput and latency, as well as for analysing simulation results with high precision [16.17].

Section I: AI-Driven Security Model for 6G Networks: Real-Time Threat Detection and Mitigation

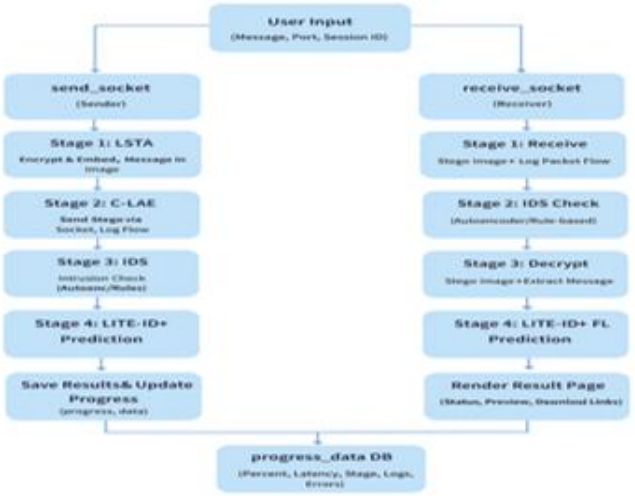

Figure 1. AIML based proposed model for 6G wireless network security.

The proposed security model is designed to observe, analyse and counteract cyber threats within the 6G network environment in real time. The framework enables secure data transmission using LSTA-based steganography over socket communication. Intrusion Detection (IDS) validates traffic integrity at both sender and receiver.AI-based attack prediction identifies potential threats in real time. Results, latency, and logs are stored in a central database and presented to the user.

Encryption and Decryption Time versus Payload Size

The analysis of encryption and decryption time versus payload size is essential for evaluating the performance and scalability of secure communication systems. As payload size increases, cryptographic processing time also increases, affecting latency, throughput, and Quality of Service. Efficient encryption mechanisms minimize time overhead while ensuring data security, making this analysis critical for real-time and high-speed networks. [18,19].

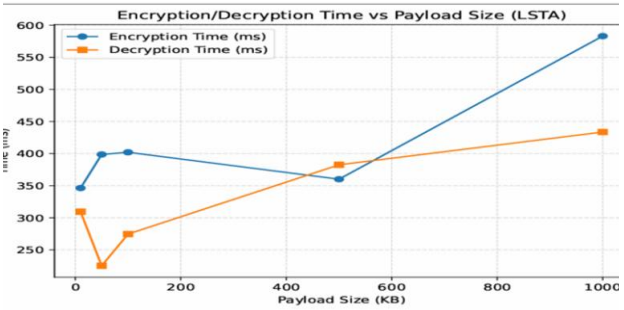

Figure 2. Encryption and Decryption Time versus Payload [18,19].

PSNR drop by Payload Size

The PSNR drop with increasing payload size is a critical metric in 6G wireless networks for evaluating steganographic imperceptibility and signal quality. A controlled PSNR reduction indicates efficient data embedding with minimal distortion, ensuring reliable ultra-high-speed transmission and low-latency.

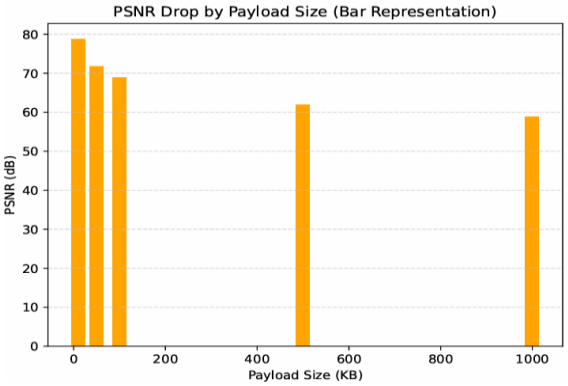

Figure 3. PSNR Drop by Payload Size.

The bar analysis illustrates a consistent reduction in PSNR as payload size increases, confirming that higher data embedding introduces greater distortion. Nevertheless, PSNR values remain within acceptable limits, indicating that the proposed LSTA scheme maintains satisfactory steganographic quality while supporting increased payload capacity for secure communication. X-axis: Payload size (KB), Y-axis: PSNR (dB), PSNR decreases with larger payloads but stays acceptable.

Overall integrity verification results

Overall integrity verification results are crucial in 6G systems to ensure data authenticity, reliability, and trustworthiness under ultra-high data rate and low-latency conditions. High integrity verification performance confirms robustness against transmission errors and cyberattacks while maintaining Quality of Service. This assurance is essential for secure, mission-critical, and real-time 6G applications**.**

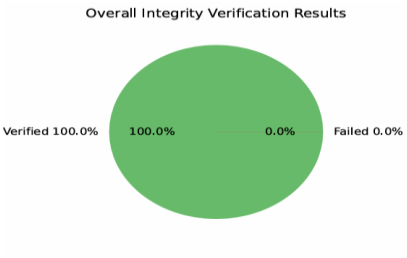

Figure 4. Integrity Verification Results.

The integrity verification results show a 100% success rate with zero failures, confirming that the proposed security mechanism reliably preserves data integrity during transmission. Chart Pie (100% verified vs failed), Most transmission are verified successfully. [5,6].

Lsta Final Performance Overview

The LSTA final performance overview is important in 6G wireless networks as it provides a comprehensive evaluation of security, efficiency, and reliability under ultra-high data rate and low-latency conditions. By collectively analyzing metrics such as throughput, latency, integrity, and resource utilization, LSTA validates system robustness and scalability. This holistic assessment confirms the suitability of LSTA for secure and high-performance 6G applications

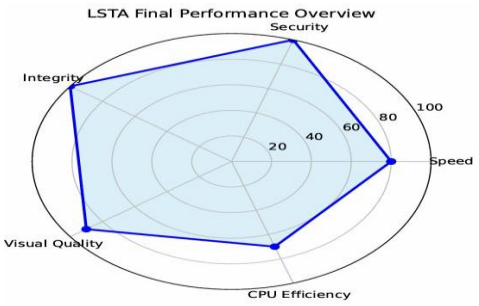

Figure 5. LSTA FINAL PERFORMANCE.

The radar analysis demonstrates that the proposed LSTA achieves high security and integrity, strong visual quality preservation, and balanced speed with efficient CPU utilization, confirming its suitability for secure and efficient data transmission in 6G networks. Throughput: with larger payloads. (Slower)CPU Usage: gradually with larger payloads. (Efficient)Overall LSTA: Strong on Integrity (95), Security (100). System is Secure & Efficient with Acceptable Quality (65).

Performance Outcome

1. LSTA Secure Transmission Performance Report
2. Integrity Verification: 100.0%
3. Avg Encryption Time: 418.06 ms
4. Avg Decryption Time: 325.09 ms
5. Avg PSNR: 68.02 dB
6. Avg CPU Usage: 36.60 %
7. Avg Throughput: 701.26 KB/s

Threat Detection in Deep learning

This framework performs threat detection by first scaling processed network data and learning compact latent representations using a CLAE autoencoder. The extracted bottleneck features capture hidden attack patterns and are classified using a Random Forest, enabling accurate intrusion prediction. Final performance is validated through accuracy, classification reports, and confusion matrix, demonstrating effective detection of malicious activities.

Data Set Distribution

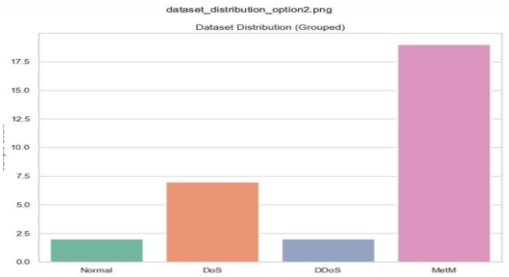

Figure 6. Data set Distribution.

The dataset distribution is highly imbalanced, with MITM attacks dominating, followed by DoS, while Normal and DDoS samples are underrepresented, justifying the use of robust learning and evaluation metrics for effective threat detection. The dataset distribution is highly **imbalanced**, with **MITM attacks dominating**, followed by **DoS**, while **Normal** and **DDoS** samples are underrepresented, justifying the use of robust learning and evaluation metrics for effective threat detection.

Key Rotation Frequency (6G –level System Confidentiality)

Key rotation frequency is a critical parameter for ensuring system confidentiality in 6G wireless networks, where ultra-high data rates and long session durations increase exposure to cryptographic attacks. Frequent key rotation limits the impact of Key compromise, enhances forward secrecy, and strengthens resistance against advanced persistent threats. This parameter is essential for maintaining robust, adaptive, and future-proof security in 6G systems.

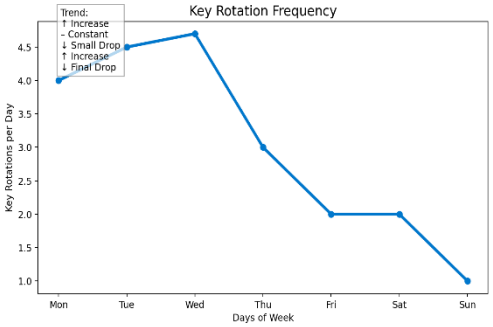

Figure 7. key rotation frequency.

The key rotation frequency shows an early-week increase peaking midweek, followed by a steady decline toward the weekend, indicating reduced security update activity over time.
Mon-Wed: Frequency\up-arrow from **4.0** to **4.7** (Peak). **Wed-Thu:** Sharp drop to **3.0**.
Thu-Sat: Drops to **2.0** and remains **constant**. **Sun,** Final drop to **1.0** (Lowest) [14]

Unauthorized Access Attempts (6G Intrusion visibility)

Unauthorized access attempts are a vital intrusion visibility parameter in 6G wireless networks, enabling early detection of malicious activities in ultra-dense and highly dynamic environments. Monitoring this metric helps identify attack patterns, prevent privilege escalation, and strengthen access control mechanisms. Its analysis is essential for proactive security enforcement and maintaining trust in 6G communication systems.

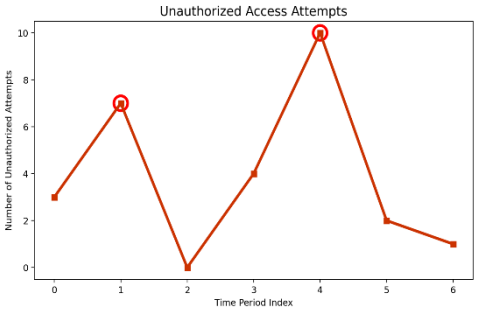

Figure 8. Unauthorized Access Attempts.

The plot reveals fluctuating unauthorized access attempts with intermittent peaks, indicating episodic security threats rather than a consistent attack pattern over time. Detected **illegal/blocked 6G access** attempts, Anomalous spikes at **7 (P1)** and **10 (P4)**, Attempts dropped to **zero (P2)**.

Post-Quantum Ready Encryption (6G future Attack)

Post-quantum ready encryption is a vital parameter in 6G wireless networks for safeguarding communication against emerging quantum-based attacks. Given the long operational lifespan and high sensitivity of 6G data, adopting quantum-resistant cryptographic techniques ensures long-term confidentiality and integrity. This capability is fundamental to establishing resilient, future-proof, and secure 6G communication systems.

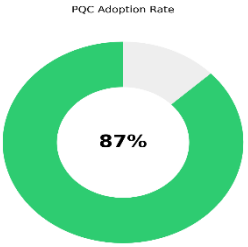

Figure 9. Post-Quantum Ready Encryption.

The chart indicates a high PQC adoption rate of 87%, reflecting strong readiness for post-quantum cryptographic security.
Represents: The percentage of adoption shown in green.
Unadopted: The remaining portion is 13%.

Encrypted Data Throughput

Encrypted data throughput is a critical parameter in 6G wireless networks as it measures the ability to transmit securely at ultra-high data rates without performance degradation. High encrypted throughput indicates efficient cryptographic processing with minimal latency overhead. This parameter is essential for ensuring secure, real-time, and bandwidth-intensive 6G applications while maintaining Quality of Service.

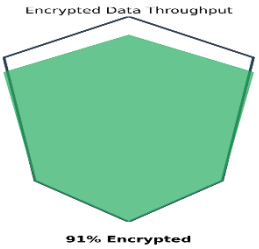

Figure 10. Encrypted Data Throughput.

The system achieves high detection accuracy with a low false alarm rate, ensuring reliable and precise threat identification. Rapid model convergence demonstrates efficient learning, while minimal latency overhead preserves real-time performance. Additionally, strong privacy preservation is maintained by retaining data locally during training, preventing raw data exposure. Encrypted Data Throughput is 91%, Nearly all data is encrypted.

Device Trust Attestation success

Device trust attestation success is a vital security parameter in 6G wireless networks for
verifying the authenticity and integrity of connected devices. High attestation success ensures that only trusted and uncompromised devices participate in communication, reducing the risk of insider and spoofing attacks. This parameter is essential for maintaining secure access, reliability, and trust in ultra-dense 6G environments.

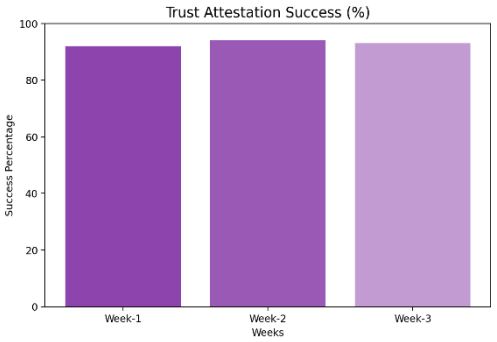

Figure 11. Device Trust Attestation success.

The trust attestation success rate remains consistently high across all three weeks, with a slight improvement in Week-2 and stable performance in Week-3. This trend demonstrates the reliability and robustness of the trust attestation mechanism, indicating its effectiveness in maintaining secure and trustworthy system validation over time. Attestation success = **secure/trusted** device verification. Success Rate is **consistently high** over **3 weeks**. Rate is
always > 90%. **Peak** success\sim **95%** (Week-2) [10].

Non-Repudiation Audit-Logs

Non-repudiation audit logs are a critical security parameter in 6G wireless networks for ensuring accountability and traceability of communication events. These logs provide verifiable evidence of user and device actions, preventing denial of transactions or malicious activities. This capability is essential for regulatory compliance, forensic analysis, and maintaining trust in secure 6G systems.

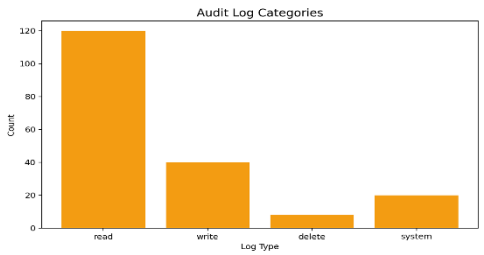

Figure 12. Non- Repudiation Audit – Logs.

The audit log distribution is dominated by read operations, followed by a moderate number of write actions, while delete and system events occur infrequently. This pattern indicates that the system primarily performs data access activities, with limited modification and deletion, reflecting stable operation and controlled system-level interventions. Read' logs dominate at a count of 120, Write' (40) and system (20) logs are less frequent.

Mean Time Recovery (MTTR)

MTTR in 6G is important because it ensures fast recovery from failures, enabling ultra-reliable, low-latency, and resilient communication for mission-critical applications.

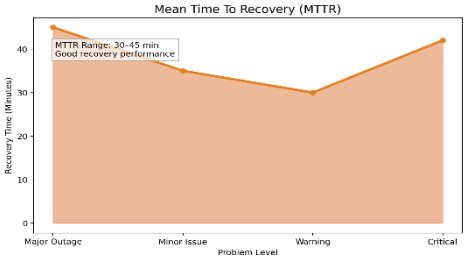

Figure 13. Mean Time Recovery.

LITE-ID – A Lightweight Intrusion Detection System Using Quantized LSTM for Resource-Constrained 6G Environments.

Key Evaluation Parameters

Model Size (MB) Throughput, CPU Utilization (%), Memory Usage, F1 Score per class (Quantized), Accuracy Vs Latency, Power Consumption

Model Size (MB)

Model Size (MB) is important in 6G because smaller models enable faster inference, lower latency, reduced energy consumption, and efficient deployment on edge devices, supporting real-time, AI-driven wireless operations.

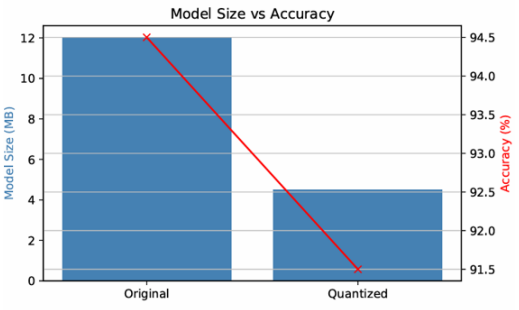

Figure14. Model Size (MB).

The figure illustrates the trade-off between model size and accuracy before and after quantization. The original model achieves higher accuracy but requires a significantly larger memory footprint, whereas the quantized model substantially reduces model size with only a marginal decrease in accuracy. This demonstrates that quantization is an effective optimization technique, enabling efficient storage and deployment while preserving near-original performance, making it suitable for resource-constrained and real-time systems.
Quantized model processes more requests per second. Analysis shows faster inference boosts throughput and scalability with implication suited for large scale network and cloud- based services.

Throughput

Throughput is crucial in 6G federated learning because higher data rates enable faster model updates, reduced training time, and scalable collaboration across edge devices, supporting real-time, low-latency distributed AI.

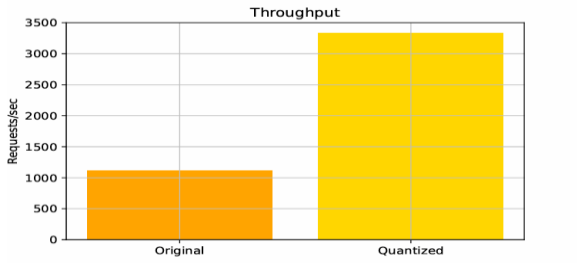

Figure 15. Throughput.

The throughput analysis shows a significant improvement after model quantization, with the quantized model processing substantially more requests per second than the original model. This increase indicates enhanced computational efficiency

and faster inference, achieved by reducing model complexity and memory overhead. The results confirm that quantization not only preserves acceptable accuracy but also markedly improves system performance, making the model more suitable for high-throughput and latency-sensitive applications.

CPU Utilization (%)

CPU Utilization (%) is important in 6G federated learning because it reflects computational efficiency at edge devices, ensuring low latency, energy efficiency, and stable real-time model training without overloading network nodes.

Figure 40: CPU Utilization (%)

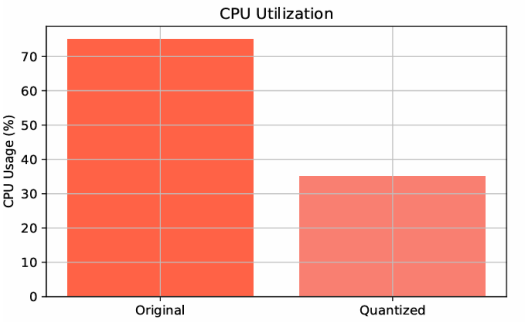

Figure 16. CPU utilization results.

The CPU utilization results demonstrate a notable reduction in resource consumption after model quantization. The original model exhibits high CPU usage, whereas the quantized model operates with significantly lower utilization. This reduction indicates improved computational efficiency and reduced processing overhead, enabling more effective use of system resources. Consequently, quantization enhances scalability and makes the model better suited for deployment in resource-constrained and real-time environments**.**

Memory Usage

Memory usage is a key enabler for efficient, secure, and scalable federated learning, making it essential for intelligent and future-ready 6G wireless networks.

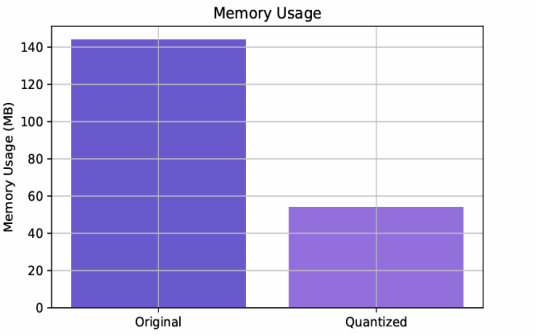

Figure17. Memory Usage.

The memory usage comparison highlights a substantial reduction in resource requirements after model quantization. The original model consumes significantly higher memory, while the quantized model requires considerably less storage. This decrease in memory footprint demonstrates the effectiveness of quantization in compressing model parameters without compromising functionality, thereby enabling efficient deployment on memory-constrained platforms and supporting scalable, high-performance inference.

F1 Score per class (Quantized)

The F1 score per class provides a balanced measure of precision and recall for each individual class, rather than offering a single averaged performance metric. This is essential in 6G systems where traffic types, network events, and security threats are highly heterogeneous and often imbalanced. A high overall accuracy may mask poor detection of minority but critical classes, such as rare cyber-attacks or ultra-reliable low-latency traffic. Quantization can introduce performance degradation that may not be uniform across all classes.

Moreover, per-class F1 evaluation supports fairness, reliability, and robustness of AI-driven decision-making in 6G networks. It ensures that quantized models deployed on edge devices can meet the stringent requirements of URLLC, network security, and intelligent automation, even under constrained computational resources.

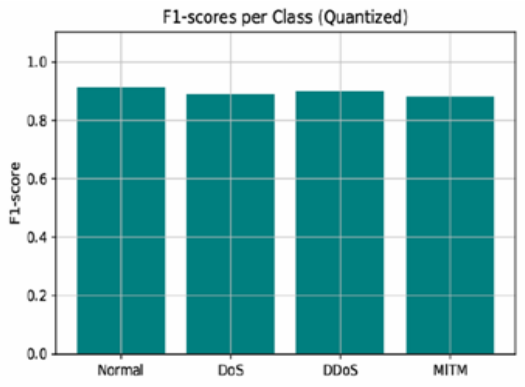

Figure18. F1 Score per class.

The class-wise F1-score analysis of the quantized model demonstrates consistently high and well-balanced performance across all traffic categories, including Normal, DoS, DDoS, and MITM attacks. The close proximity of F1-scores indicates that quantization does not introduce class bias and preserves the model's ability to accurately detect both benign and malicious activities. This consistency confirms the robustness and reliability of the quantized model for multi-class intrusion detection in practical network security environments.

Accuracy Vs Latency

In 6G wireless systems, the accuracy–latency trade-off is crucial because next-generation applications require high decision accuracy at ultra-low latency. Optimizing this balance enables reliable real-time intelligence, stringent QoS compliance, and safe operation of latency-critical 6G services**.**

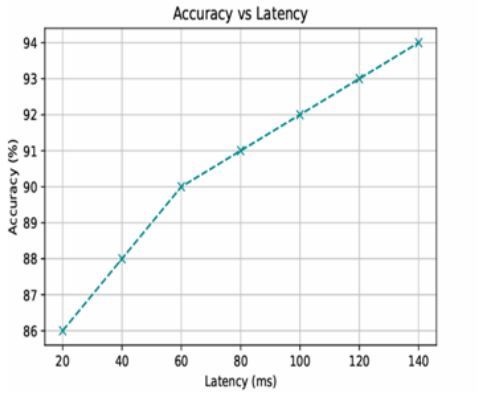

Figure19. Accuracy Vs Latency.

The accuracy–latency relationship illustrates a clear trade-off between inference speed and model performance. As latency increases, accuracy improves progressively, indicating that more computational time enables enhanced feature processing and decision accuracy. This trend highlights the need to balance latency constraints with accuracy requirements, particularly for real-time and latency-sensitive applications, where an optimal operating point must be selected to achieve efficient and reliable system performance.

Power Consumption

Efficient power utilization directly impacts network sustainability, operational cost, and device longevity, particularly for battery-constrained user equipment and edge nodes. In 6G systems, where real-time processing and continuous learning are required, minimizing power consumption without compromising performance is essential. Therefore, power-efficient techniques such as model quantization play a vital role in enabling scalable, green, and intelligent 6G wireless networks.

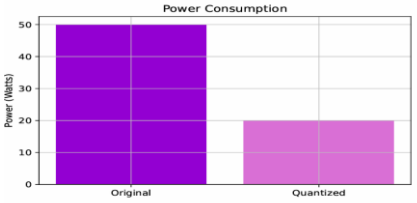

Figure 20. Power Consumption.

The power consumption comparison reveals a substantial reduction in energy usage after model quantization. The original model exhibits significantly higher power demand, whereas the quantized model operates with considerably lower consumption. This reduction demonstrates that quantization enhances energy efficiency by lowering computational and hardware overhead, making the model more suitable for deployment in energy-constrained, edge, and large-scale network environments.

CONCLUSION

AI-enabled security for 6G wireless networks integrates advanced machine learning models to deliver adaptive, real-time threat detection with high accuracy and low latency. Performance metrics such as accuracy, precision, recall, and latency are critical to ensuring effective classification of diverse network traffic classes, including complex threats like Man-in-the-Middle attacks. Federated learning emerges as a superior paradigm over centralized learning by enhancing model accuracy and scalability through active client participation while reducing privacy risks. Moreover, privacy-preserving techniques like differential privacy further mitigate gradient leakage risks, providing robust protection of sensitive data during model training. Overall, these AI-driven approaches, optimized for edge deployment, enable scalable energy-efficient, and secure communication necessary to meet the stringent demands of 6G wireless networks.

REFERENCES

1. ETSI GS QKD 004, "Quantum Key Distribution (QKD);
2. Application Interface", December 2020
3. ETSI GS QKD 014, "Quantum Key Distribution (QKD);
4. Protocol and data format of REST-based key deliveryAPI", February 2019
5. ETSI GS QKD 015, "Quantum Key Distribution (QKD);Control Interface for Software Defined Networks", March 2021
6. [8] ITU-T Y.3803, "Quantum key distribution networks - Key
7. management", December 2021.
8. P. Kela and T. Veijalainen, “Cooperative action branching deep reinforcement learning for uplink power control,” in Joint European Conference
9. on Networks and Communications & 6G Summit (EuCNC/6G Summit),2023.
10. M. Ylianttila, R. Kantola, and A. Gurtov, “6g white paper:
11. research challenges for trust, security and privacy,” 2023,
12. https://arxiv.org/abs/2004.11665.
13. P. Yang, N. Xiong, and J. Ren, “Data security and privacy protection for cloud storage: A survey,” IEEE Access, vol. 8, pp. 131723–131740,2023
14. Shah, H., & Fatangare, S. (2020). Review on the Integration of Artificial Intelligence and 6G Communications.
15. Union, “IMT traffic estimates for the years 2020 to 2030,” Report ITU, vol. 2370, 2015.
16. Ahammed, T. B., Patgiri, R., & Nayak, S. (2022). A vision on the artificial intelligence for 6G communication. ICT Express.
17. Chang, L., Zhang, Z., Li, P., Xi, S., Guo, W., Shen, Y., ... & Wu, Y. (2022). 6G-enabled Edge AI for Metaverse: Challenges, Methods, and Future Research Directions. arXiv preprint arXiv:2204.06192.
18. Tan, J., Xue, R., & Shi, Y. (2022). Exploration and Application of AI in 6G Field. arXiv preprint arXiv:2207.13382.
19. Letaief, K. B., Shi, Y., Lu, J., & Lu, J. (2021). Edge artificial intelligence for 6G: Vision, enabling technologies, and applications. IEEE Journal on Selected Areas in Communications, 40(1), 5-36.
20. U. Challita, A. Ferdowsi, M. Chen, and W. Saad, ‘Machine Learning for Wireless Connectivity and Security of Cellular-Connected UAVs’, IEEE Wirel. Commun., vol. 26, no. 1, pp. 28–35, 2019, doi: 10.1109/MWC.2022.1800155. 83.
21. D. G. Riviello, F. Di Stasio, and R. Tuninato, ‘Performance Analysis of Multi-User MIMO Schemes under Realistic 3GPP 3-D Channel Model for 5G mmWave Cellular Networks’, Electronics, vol. 11, no. 3, 2023,
22. doi: 10.3390/electronics11030330. 84. S. Khan, ‘The 5G Network Backbone: A Guide to Small Cell Technology’, Telit. Accessed: Feb. 06, 2024. [Online]. Available: https://www.telit.com/blog/5g-networks-guide-to-small-cell-technology
23. Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals. IT Professional, 18(5), 42–47. https://doi.org/10.1109/MITP.2016.77 /
24. Tariq, M. R. Khandaker, K.-K. Wong, M. A. Imran, M.
25. Bennis, and M. Debbah, "A speculative study on 6g,"
26. IEEE Wireless Communica tions, vol. 27, no. 4, pp. 118-
27. 125, 2020.
28. K. Matsuda et al., "Field Demonstration of Real-time 14
29. Tb/s 220 m FSO Transmission with Class 1 Eye-safe 9- aperture Transmitter," Optical Fiber Communications Conference and Exhibition (OFC), San Francisco, CA,USA, 2021, pp. 1-3

30. https://gtr.ukri.org/projects?ref=45364 [4] ITU-T Y.3800, "Overview on networks supporting quantum key distribution", October 2023.
31. ETSI GS QKD 004, "Quantum Key Distribution (QKD);
32. Application Interface", December 2023.
33. ETSI GS QKD 014, "Quantum Key Distribution (QKD);
34. Protocol and data format of REST-based key delivery
35. API", February 2023.
36. ETSI GS QKD 015, "Quantum Key Distribution (QKD);
37. Control Interface for Software Defined Networks", March
38. 2024
39. I TU-T Y.3803, "Quantum key distribution networks - Key
40. management", December 2023
41. Y. Wu et al., "AI and Machine Learning for 6G Wireless Security: Challenges and Solutions", IEEE Network, 2023.
42. M. Chen et al., *"Deep Learning-Based Intrusion Detection for 6G Networks: A Survey"*, IEEE Communications Surveys & Tutorials, 2022.
43. Z. Ning et al., *"Artificial Intelligence-Empowered Cybersecurity in 6G: Challenges, Techniques, and Future Directions"*, IEEE Internet of Things Journal, 2023.
44. Q. Yang et al., "Federated Learning for 6G: Applications, Challenges, and Future Directions", IEEE Wireless Communications, 2022.
45. K. Bonawitz et al., "Towards Federated Learning at Scale: System Design", Proceedings of Machine Learning and Systems (MLSys), 2019.
46. L. Lyu et al., "Privacy and Robustness in Federated Learning: Attacks and Defenses", IEEE Transactions on Neural Networks and Learning Systems, 2023.
47. C. Dwork et al., "The Algorithmic Foundations of Differential Privacy", Foundations and Trends in Theoretical Computer Science, 2014.
48. M. Abadi et al., "Deep Learning with Differential Privacy", ACM CCS, 2016.
49. R. Shokri et al., "Membership Inference Attacks Against Machine Learning Models", IEEE Symposium on Security and Privacy, 2017.
50. M. Peng et al., "Edge Intelligence for 6G Networks: Challenges and Solutions", IEEE Wireless Communications, 2023.
51. Y. Mao et al., "A Survey on Mobile Edge Computing for 6G: Fundamentals, Applications, and Challenges", IEEE IoT Journal, 2022.