International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ENHANCING 6G NETWORK SECURITY WITH ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING INTEGRATION.

Mrs. Darakshan Javed Ansari Dr Alam. N. Shaikh

Research Scholar, Thadomal Shahani Engg College., Principal PVPPCOE,

Assistant professor M.H.S.S. College (E&TC) Byculla, Mumbai Maharashtra ,India
darakshan.javed.2012@gmail.com

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 encryptionstrategies, 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]

next-generation networks. By providing a comprehensive 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 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

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

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 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

developin post- cryptograph framework 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:

1. 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.

2 "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,

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

discusses potential attacks on AI/ML systems, and identifies future research directions to ensure robust security in AI-driven 6G environments.

3.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.

4."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.

5.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.

1.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

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

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].

6."GenerativeAdversarialLearningforIntelligentTrust**1.1 Section I: AI-Driven Security** 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.

7. "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

Real-Time Threat Detection and Mitigation:

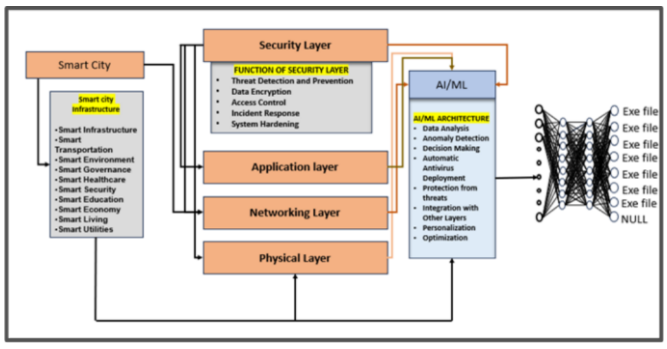


Figure 1:AIML based proposed model for 6G wireless network

effectiveness of this framework in dynamic and uncertain **security.**

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

communication environments, highlighting its potential for enhancing security in next-generation networks.

8."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. The proposed security model is designed to observe, analyseand counteract cyber threats within the 6G network environment in real time. By integrating learning datasetsadvanced simulation techniques such as Wireshark 4.4.3, along with supervised and unsupervised, the system continuously monitors network activity to detect and mitigate potential attacks with high precision. Aligned with the conceptualized 6G architecture, the model operates across three fundamental layers.

1.2 Physical Layer**:** Comprising a vast network of resources and nodal sources, optimized through Reconfigurable Intelligent Surfaces **(RIS)** to enable with minimal loss. Network Layer**:** Utilizing AI/ML algorithms to monitor and respond to various cyber threats, including malware intrusions, DDoS attacks, and other malicious activities.

Application Layer**:** Ensuring secure end-user interactions by actively detecting threats and implementing preventative measures. A dedicated security layer is embedded within this framework, functioning as a real-time sentinel that continuously analyses network operations. Artificial Intelligence (AI) algorithms work in tandem with this layer, monitoring, analysing, and dynamically adapting to potential security threats. When anomalies or malicious activities are detected, the system immediately triggers high-priority alerts and initiates appropriate counter measures [18,19].

1.3 Detection of Man-in-the-Middle Attacks through Traffic Interception Analysis: The detection of unauthorized traffic interceptions and alterations, commonly referred to as Man-in-the-Middle (MitM) attacks, is a critical aspect of modern cybersecurity. Data analysis and threat intelligence play a pivotal role in identifying such security breaches. Wireshark, a widely used network protocol analyser, enables security professionals to export network traffic data into CSV files, facilitating further analysis using advanced tools such as Python, Excel, or Security Information and Event Management (SIEM) systems. These datasets serve as the foundation for various cybersecurity operations, including: Log Analysis – The systematic parsing and examination of network logs to identify potential security threats.

Threat Intelligence – The correlation of network events with known attack patterns, enhancing proactive defense strategies.

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

By integrating Wireshark's deep packet inspection capabilities with AI-driven security analytics, the proposed model ensures continuous, adaptive, and intelligent protection for emerging 6G networks. This study examines the integration of Artificial Intelligence (AI) and Machine Learning (ML) in building a resilient and secure 6G ecosystem, enhancing trust, ensuring reliability, and

acceleratingthe widespreadadoptionofnext-generation

communication technologies. [5,6].

2. Security Framework & Simulation Techniques:

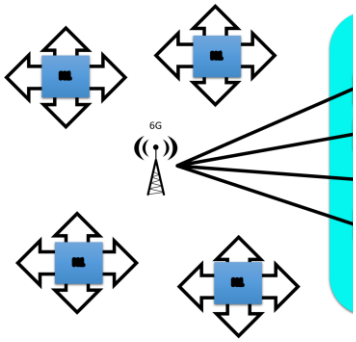


Figure 2:Node Organization of the Idealized 6G Layer

This illustration depicts a complex interconnected ecosystem comprising multiple nodes, devices, and servers linked to the 6G tower. The proposed security layer ensures real-time monitoring and threat assessment to safeguard the network against cyber threats.

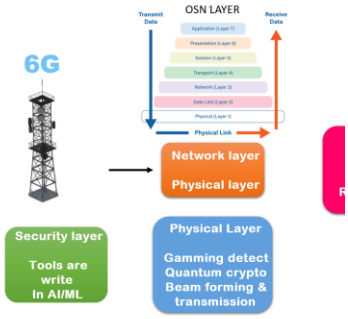


Figure 3*:* Security tool design using IDS and IPS for the above connection

2.1 This diagram illustrates the integration of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) within the 6G security architecture, strengthening its capacity to detect, analyze, and mitigate potential threats effectively.

AI-Driven Cybersecurity Framework for 6G Networks: Leveraging Wireshark 4.4.3 for Advanced threat Detection: The rapid evolution of 6G networks necessitates robust and intelligent security mechanisms to counter emerging cyber threats. This study presents a

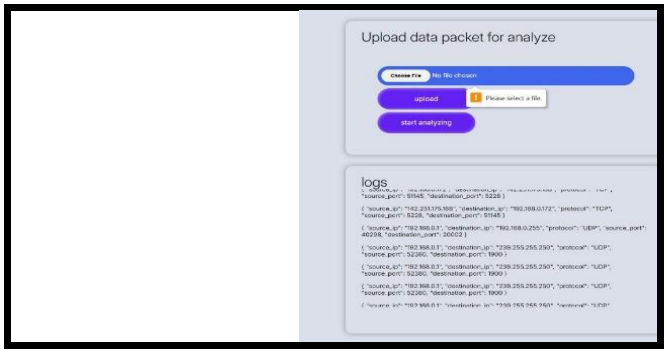
Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

comprehensive security framework that integrates **Wireshark 4.4.3**, a sophisticated network packet analyser, as a core component for network monitoring and threat detection. By enabling the real-time capture and in-depth inspection.



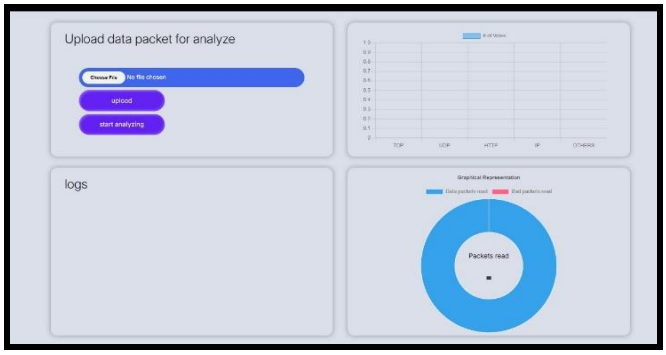


Figure 4: Log analysis and network traffic in packet transfer using Intrusion detection system

Wireshark plays a critical role in various cybersecurity operations, including:

Intrusion Detection – Identifying suspicious traffic patterns and anomalies indicative of security breaches.

Malware Analysis – Examining network packets to detect malicious payloads and known malware signatures

Network Forensics – Investigating security incidents by analysing captured network traffic to reconstruct attack timelines.

Protocol Analysis – Evaluating network protocols to identify misconfigurations and vulnerabilities that may be exploited.

Man-in-the-Middle (MitM) Attack Detection – Detecting unauthorized interception, alteration, or rerouting of network traffic.

To enhance data analysis and threat intelligence capabilities, Wireshark facilitates the export of network traffic data into CSV files, enabling further analysis through advanced computational tools such as Python, Excel, and Security Information and Event

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Management (SIEM) systems. These datasets serve as critical resources for: **Log Analysis** – Parsing and scrutinizing network logs to identify irregularities and potential security threats.

Threat Intelligence – Correlating network activity with known attack patterns to facilitate proactive defense mechanisms.

By integrating Wireshark's deep packet inspection capabilities with **AI-driven security analytics**, the proposed framework ensures continuous, adaptive, and intelligent protection for 6G networks. Through the application of Artificial Intelligence (AI) and Machine Learning (ML), this approach enhances network resilience, fosters trust and reliability, and accelerates the widespread adoption of secure and robust next-generation communication technologies. This paper explores the intersection of AI and cybersecurity in the context of 6G networks, emphasizing the necessity of intelligent, data-driven threat detection models to mitigate evolving cyber risks effectively [12,17].

By combining Wireshark for real-time monitoring and CSV analysis for in-depth investigation, security teams can quickly detect and respond to attacks.

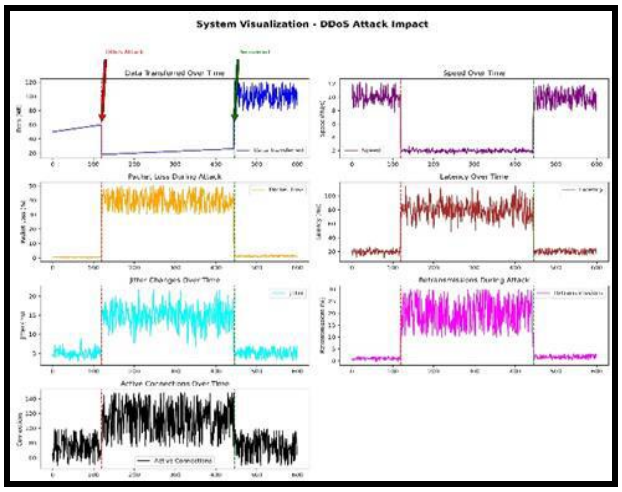


Figure 5: Simulation result transfer 10Gb file to another device using 6G Tower

Table 1:Different usage of wireshark and CSV analysis

Security Goal	Wireshark Use	CSV Analysis
Threat Detection	Capture live traffic, detect anomalies	Analyse logs for abnormal patterns
Malware Analysis	inspect packet payloads for malware signatures	Correlate attack patterns with known threats
DDoS Mitigation	Identify excessive traffic sources	Find attack trends over time
Incident Response	Save PCAP evidence	Cross-reference logs with external threat databases

Received: August 07, 2025

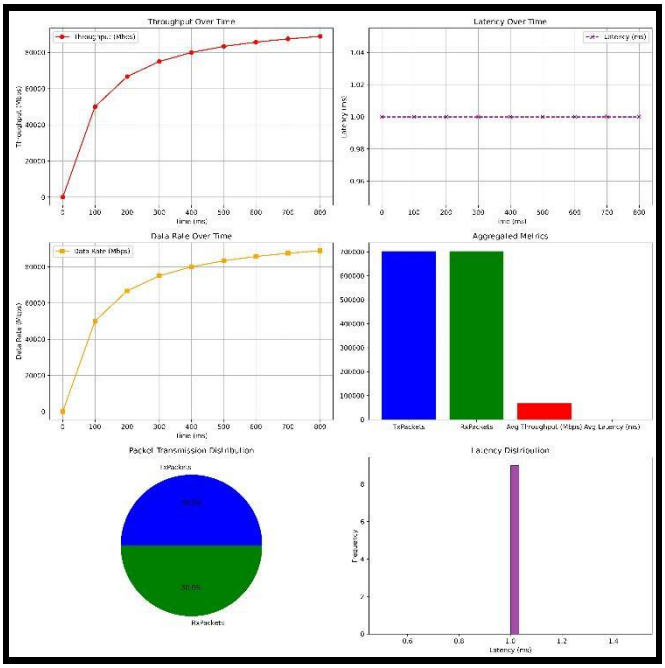
International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3. Section II: Simulation Result based on to transmit data packets through 6G tower to another device:

Transmitted Packets Over Time (Graph 1): This graph comprises six sets of subgraphs, with the upper-left section specifically tracking the number of packets transmitted by the client node over time. The x-axis represents time in seconds, while the y-axis denotes the total number of packets sent. The red line follows a linear upward trajectory, indicating a steady and consistent rate of packet transmission.With the same sequence graph depicts the data rate increases in the same manner which transmits the data packets and received the packet with the same rate. The upper right graph shows the latency between both the graph, indicates by purple graph is linear, a stable and constant transmission rate. Received Packets Over Time (Middle Graph) This graph tracks the number of packets successfully received by the server node over time. The purple line also increases linearly, matching the transmitted packets. Reliable transmission: No packet loss. Consistent transmission rate: The number of sent and received packets follows a steady trend. High-speed communication: Even at 100 Gbps data rate, throughput remains stable at 70 Mbps. Minimal degradation: The slight drop in throughput is expected in real networks due to minor timing



Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 6: Simulation result transfer 10Gb file to another device using 6G Tower

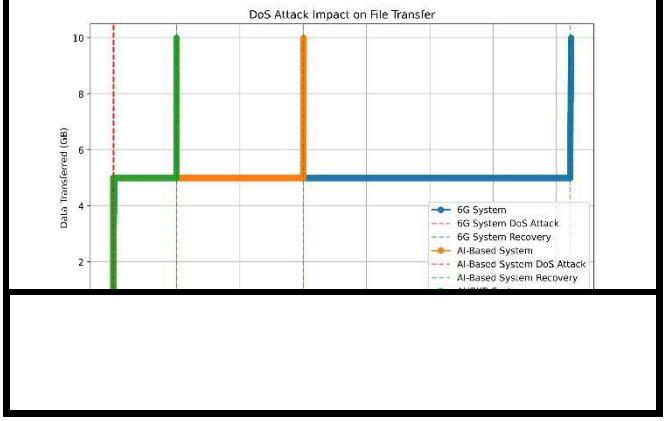


Figure7: Proposed attack in 6G wireless network system

The image illustrates a DoS attack affecting three different systems. Each system was in the process of transferring a 10GB file, with 50% of the transfer completed before the attack. The recovery and completion times varied across the systems:

- **System 1 (standard): 6,175 seconds**
- **System 2 (AI/ML-enhanced): 75 seconds**
- **System 3 (AI/ML with QKD integration): 25 seconds**

Simulation result based on 6G with AIML:

To propose the 6G network using AIML (supervised and unsupervised data set), simulate and drive by CSV files and Wireshark, a sophisticated network packet analyser, as a core component for network monitoring and threat detection. By enabling the real-time capture and in-depth inspection of network traffic, Wireshark plays a critical role in various cybersecurity operations.

Leveraging AI-driven security analytics, the proposed framework delivers continuous, adaptive, and intelligent protection for 6G networks. By integrating Artificial Intelligence (AI) and Machine Learning (ML), this approach strengthens network resilience, fosters trust and reliability, and accelerates the adoption of secure and robust next-generation communication technologies. This paper explores the convergence of AI and cybersecurity within the 6G landscape, underscoring the critical need for intelligent, data-driven threat detection models to effectively counter evolving cyber risks. By utilizing Wireshark for real-time monitoring and CSV analysis for in-depth investigation, security teams can swiftly detect and respond to potential attacks. [19,20].

Throughput and data rate around **500 Gbps** (half of the first). Latency is slightly higher **(~0.5 ms).**

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Packet distribution remains **50-50.**

Suggests a similar network but with half the bandwidth.

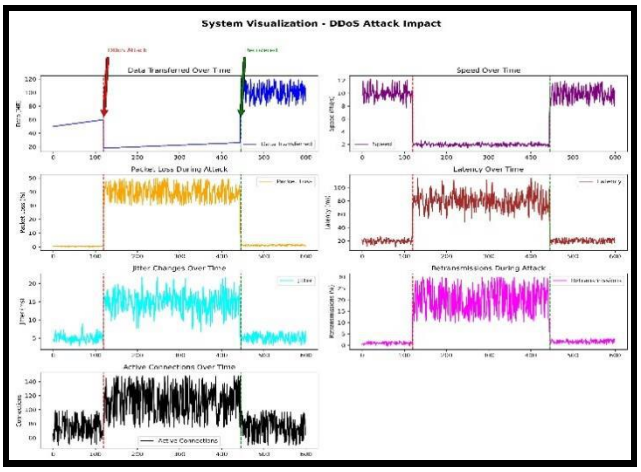


Figure 9: Proposed DDOS attack in 6G with AIML

Speed	**500Gbps**
Latency	**0.5ms**
Packet	**1mb**
Completi	**0.16s**
Throughput Over Time	**This represents the rate of successful data**

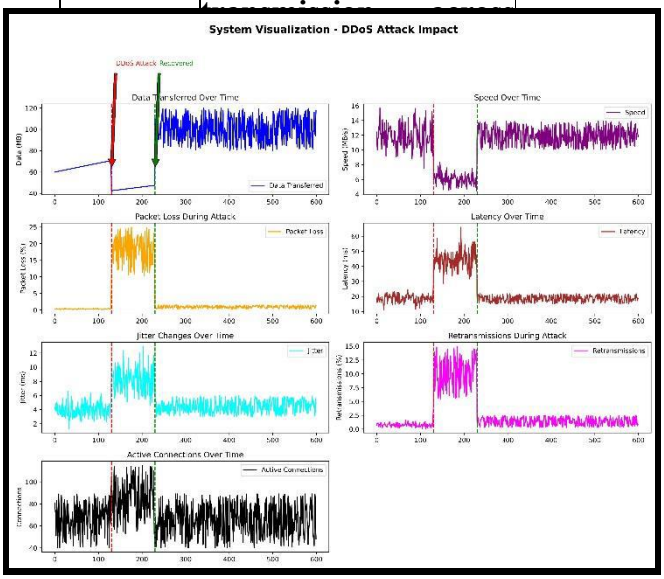


Figure 10: Proposed DDOS attack in 6G with AIML

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

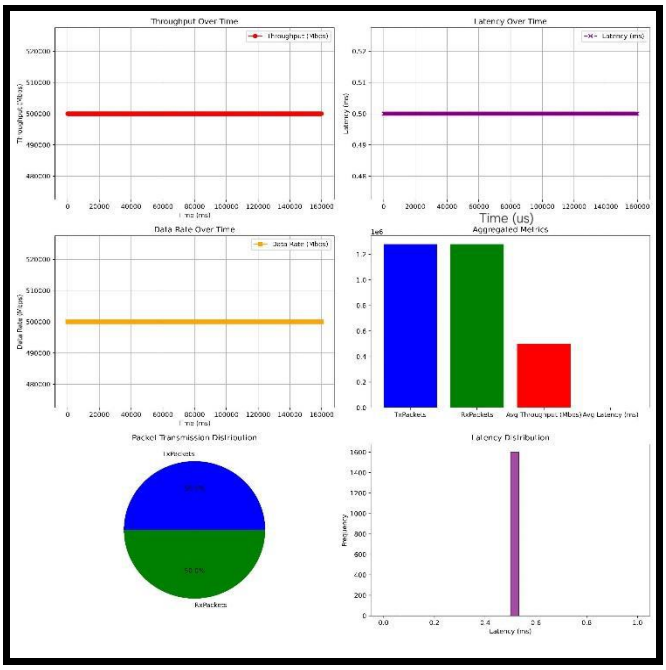


Figure 11: The observation in graph 2 indicates 6G with AI/ML and quantum cryptography.

Table 2: Simulation analysis 6G parameter with AIML Quantum distribution

Speed	1Tbps
Latency	0.1ms
Packet size	10MB
Completion .	0.8s
Throughput Over Time	This illustrates the speed of successful data transmission across the network,

Feature	System 1 (Weakest)	System 2 (Moderate)	System 3 (Strongest)
Recovery Time	**3 min 25 sec** (205s)	**1 min 40 sec** (100s)	**39 sec** (Fastest)
Data Transfer Impact	Severe drop (60-80%)	Moderate drop (40-50%)	Minimal drop (20%)
Speed Reduction	Major slowdown (50-80%)	Moderate (40%)	Minimal (30%)
Latency Increase	2.5x to 4x increase	2x increase	1.5x increase
Jitter Increase	High fluctuation (3x-4x)	Moderate fluctuation (2x)	Small fluctuation (1.3x)
Packet Loss (%)	Severe (10-50%)	Moderate (5-10%)	Minimal (3-7%)
Retransmissions	High (5-15%)	Moderate (3-8%)	Low (2-6%)
Active Connections	High fluctuation (bot activity)	Moderate increase	Slight increase (controlled bots)
Attack Resilience	Weak (high distortion, long recovery)	Moderate (some distortion, faster recovery)	Strong (fastest recovery, minimal disruption)

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 4: Comparative analysis of 6G ,6G AIML and post quantum cryptography

3.3 To model AI enabled security measures for 6G wireless network: AI-enabled security in 6G wireless networks leverages machine learning and deep learning to provide adaptive, real-time

threatdetectionintrusio preventio and authenticati

enhancement. By analyzing multi-modal network and device data, these models ensure high accuracy, low latency, and robustness against evolving cyberattacks, while being optimized for edge deployment to maintain scalability, energy efficiency, and secure communication.[30].

For designing an **AI-enabled security model for 6G wireless networks**, the key parameters to consider can be grouped into **performance**, **efficiency**, and **robustness** aspects: **Performance Metrics**

- **Accuracy (%)** – Correct classification of normal vs malicious activities.
- **Latency (ms)** – Time to detect and respond to threats
- **Precision & Recall** – Ability to avoid false positives and false negatives.
- **F1 Score** – Balance between precision and recall.
- **Model Size (MB)** – Suitability for edge and mobile devices.

Accuracy (%) represents the proportion of correctly classified

3.3 instances, indicating the model's capability to distinguish between within the 6G environment.

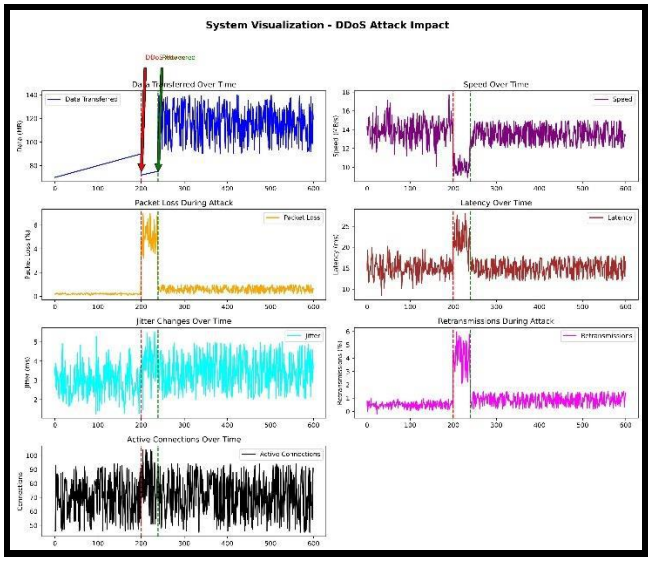


Figure 12: The observation in graph 2 indicates 6G with AI/ML

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and quantum cryptography.

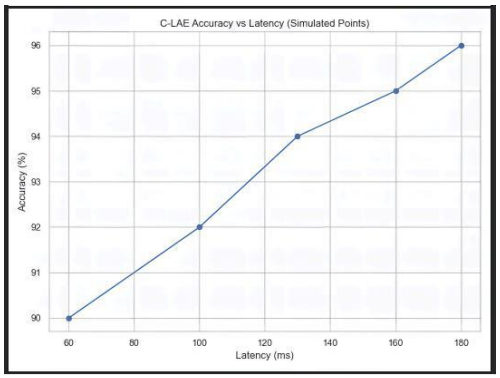


Figure 13:C-LAE Accuracy vs Latency (Simulated)

Latency (ms) – Time to detect and respond to threats,Latency (ms) – Represents the time taken by the AI-enabled 6G security model to detect and respond to potential threats, where minimal latency is critical to maintaining real-time protection and meeting the ultra-low delay requirements of 6G communication systems.

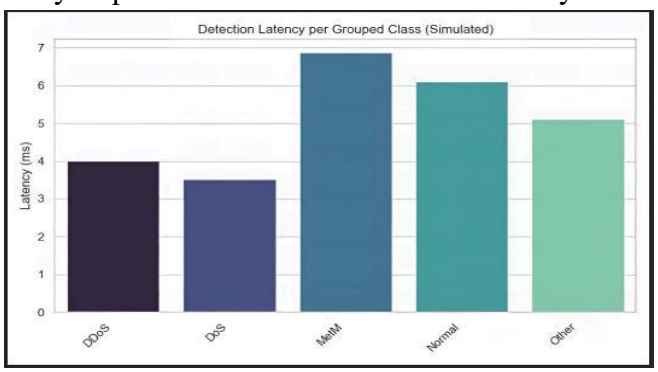


Figure14: Detection latency per grouped class(DDoS, DoS,MitM and other)

The simulated figure depicts detection latency (ms) across five network traffic classes: DDoS, DoS, MitM, Normal, and Other. Latency varies notably among categories, with *MitM* showing the highest value (~7.0 ms), about 75% greater than *DoS* (~4.0 ms), due to the complexity of detecting subtle packet manipulations and cryptographic interceptions. *Normal* traffic (~6.0 ms) also incurs higher latency, reflecting the challenge of distinguishing benign from borderline anomalous events. The *Other* category (~5.0 ms) likely reflects additional verification steps for heterogeneous signatures. *DDoS* (~4.0 ms) and *DoS* (~3.5 ms) exhibit the lowest latencies, benefiting from clear, high-volume traffic patterns that facilitate rapid classification [30,31]

3.3.1 C-LAE Precision Precision vs Recall in Grouped Classes: – For the Centralized–Lightweight Anomaly Estimator (C-LAE) applied in AI-enabled 6G security, precision and recall can be evaluated for grouped traffic classes such as Distributed Denial of Service (DDoS), Denial of Service (DoS), Man-in-the-Middle (MitM), Normal, and Other. Precision

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

indicates the proportion of correctly identified instances within each class among all detections assigned to that class, while recall measures the proportion of actual instances of that class correctly detected by the model [33]. This grouped-class analysis enables a detailed assessment of C-LAE's detection performance across diverse network threat categories, ensuring that the model maintains both accuracy and reliability in multi-class 6G security environments.

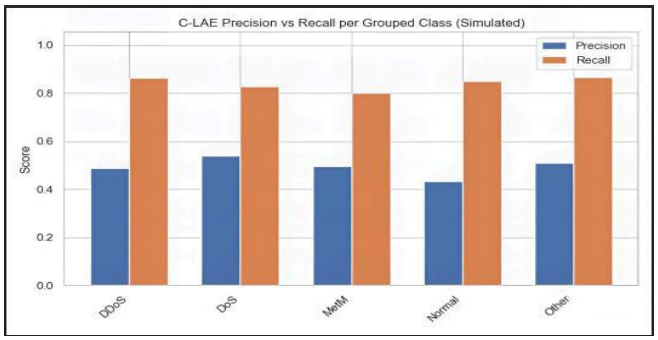
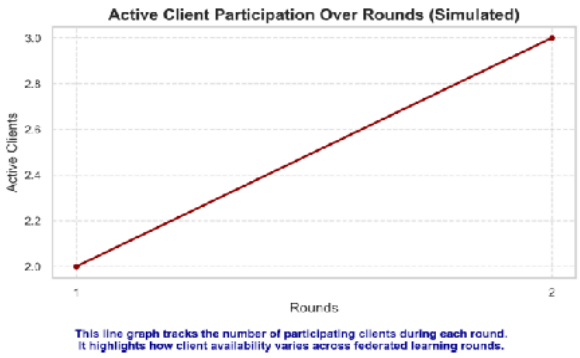


Figure 15: C-LAE precision vs Recall Grouped class *(* (DDoS, DoS,MitM and other)

3.3.2 Active Client Participation in Rounds – In the context of AI-enabled security for 6G wireless networks, active client

participation in rounds refers to the proportion of available network clients (e.g., edge devices, IoT nodes, or base stations) that actively contribute to the model's training or update process during each communication round. Higher participation enhances model diversity and detection accuracy by incorporating a wider range of local threat data, while lower participation may reduce detection robustness but can help minimize communication overhead and latency.



Graph 15: Active client participation over Rounds

Federated vs Centralized Accuracy (Simulated*)"* illustrates a comparative analysis of model accuracy between Federated Learning and Centralized Learning over multiple training rounds. The x-axis represents the number of training rounds (2, 4, 6, 8, and 10), while the y-axis denotes the corresponding model accuracy, measured in percentage (%).In the case of

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Centralized Learning (depicted by the orange line with circular markers), the model begins with an accuracy of approximately 70% at round 2. The accuracy steadily increases, reaching around 80% by the 10th round. This indicates a consistent yet moderate improvement in performance across training iterations [32].

Conversely, Federated Learning (represented by the blue line with circular markers) initiates at a slightly lower accuracy of about 65% at round 2. surpassing the centralized model by round 6 with an accuracy of nearly 77%. By round 10, the federated model achieves an accuracy close to 90%, indicating superior scalability and learning efficiency over time.

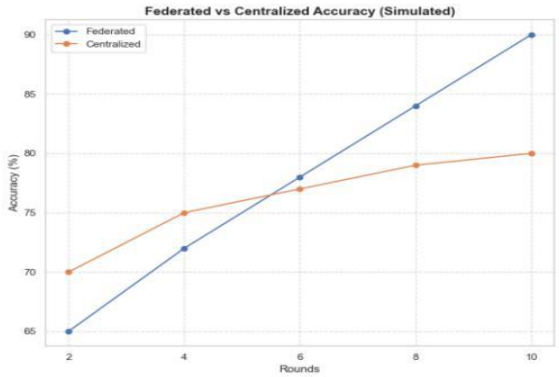
3.3.4 Client Contribution to Global Model – In AI-enabled 6G security, client contribution refers to how much each device's local data and updates influence the overall global security model, affecting its accuracy and ability to detect diverse threats effectively.

Graph 16: Client contribution to Global model The graph compares the accuracy (%) of Federated Learning and Centralized Learning models over multiple training rounds, simulating their performance in AI-

convergence, and privacy advantages compared to traditional centralized learning methods.

enabled security for 6G wireless networks.X-axis

(Rounds)**:** Represents the number of training iterations (2 to 10). Y-axis (Accuracy %): Shows the model's accuracy in detecting security threats in the network.

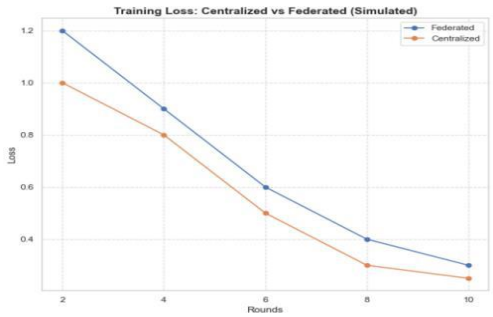


Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)



Graph 17:Federated vs Centralized Learning Accuracy Performance with training loss.

3.3.5 Federated vs Centralized Learning Performance in AI-enabled 6G Security

The first graph compares the accuracy (%) of Federated and Centralized learning models over multiple training rounds (2 to 10). Initially, the centralized model achieves higher accuracy (~70%) at round 2 compared to the federated model (~65%). However, as training progresses, federated learning

demonstrates superior performance, surpassing the centralized model around round 6 and reaching approximately 90% accuracy by round 10. In contrast, the centralized model improves steadily but plateaus around 80%. This indicates that federated learning offers better scalability and learning efficiency for AI-enabled 6G security applications.

The second graph presents the training loss for both models across the same rounds. Training loss, which measures model error, decreases for both methods, but federated learning consistently achieves lower loss values at each round. By round 10, the federated model attains a loss near 0.2, outperforming the centralized model's loss around 0.3. This further confirms federated learning's enhanced capability to optimize model parameters and generalize from distributed data sources while preserving privacy[31] Together, these results highlight federated learning as a promising approach for AI-enabled security in 6G wireless

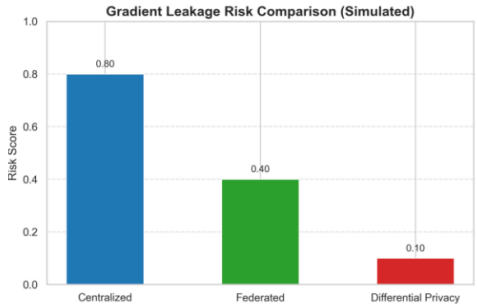


Figure 18: Gradient leakage risk Comparison (centralized, Federated and differential Privacy)

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The graph illustrates the gradient leakage risk across three machine learning paradigms for 6G security. Centralized learning shows the highest risk (0.80) due to all data being processed centrally, increasing privacy vulnerability. Federated learning reduces this risk to 0.40 by keeping data on devices and sharing only model updates. Differential privacy achieves the lowest risk (0.10) by adding noise to data or gradients, greatly enhancing privacy. This progression highlights improved privacy protection from centralized to federated learning, and further with differential privacy techniques.

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); Application Interface", December2020 ETSI GS QKD 014, "Quantum Key Distribution (QKD);
2. Protocol and data format of REST-based key deliveryAPI", February 2019
3. ETSI GS QKD 015, "Quantum Key Distribution (QKD);Control Interface for Software Defined Networks", March 2021 ITU-T Y.3803, "Quantum key distribution networks - Key management", December 2021.
4. P. Kela and T. Veijalainen, “Cooperative action branching deep reinforcement learning for uplink power control,” in Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit),2023.
5. M. Ylianttila, R. Kantola, and A. Gurtov, “6g white paper: https://arxiv.org/abs/2004.11665.
6. 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
7. Shah, H., & Fatangare, S. (2020). Review on the Integration of Artificial Intelligence and 6G Communications.
8. I. Union, “IMT traffic estimates for the years 2020 to 2030,” Report ITU, vol. 2370, 2015.
9. Ahammed, T. B., Patgiri, R., & Nayak, S. (2022). A vision on the artificial intelligence for 6G communication. ICT Express.

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

10. 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.
11. Tan, J., Xue, R., & Shi, Y. (2022). Exploration and Application of AI in 6G Field. arXiv preprint arXiv:2207.13382.
12. Letaief, K. B., Shi, Y., Lu, J., & Lu, J. (2021). Edge artificial intelligence for 6G: Vision, enabling technologies, and applications.
13. IEEE Journal on Selected Areas in Communications, 40(1), 5-36.
14. 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.
15. 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,
16. 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
17. 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 /
18. Tariq, M. R. Khandaker, K.-K. Wong, M. A. Imran, M.
19. Bennis, and M. Debbah, "A speculative study on 6g," IEEE Wireless Communica tions, vol. 27, no. 4, pp. 118- 125, 2020.
20. ETSI GS QKD 014, "Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API", February 2023.
21. ETSI GS QKD 015, "Quantum Key Distribution (QKD); Control Interface for Software Defined Networks", March 2024
22. I TU-T Y.3803, "Quantum key distribution networks - Key management", December 2023
23. Y. Wu et al., "AI and Machine Learning for 6G Wireless Security: Challenges and Solutions", IEEE Network, 2023.
24. M. Chen et al., *"Deep Learning-Based Intrusion Detection for 6G Networks: A Survey"*, IEEE Communications Surveys & Tutorials, 2022.
    a. Z. Ning et al., *"Artificial Intelligence-Empowered
25. Cybersecurity in 6G: Challenges, Techniques, and Future Directions"*, IEEE Internet of Things Journal, 2023.
26. Q. Yang et al., "Federated Learning for 6G: Applications, Challenges, and Future Directions", IEEE Wireless Communications, 2022.

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

27. K. Bonawitz et al., "Towards Federated Learning at Scale: System Design", Proceedings of Machine Learning and Systems (MLSys), 2019.
28. L. Lyu et al., "Privacy and Robustness in Federated Learning: Attacks and Defenses", IEEE Transactions on Neural Networks and Learning Systems, 2023.
29. C. Dwork et al., "The Algorithmic Foundations of Differential Privacy", Foundations and Trends in Theoretical Computer Science, 2014.
30. M. Abadi et al., "Deep Learning with Differential Privacy", ACM CCS, 2016.
31. R. Shokri et al., "Membership Inference Attacks Against Machine Learning Models", IEEE Symposium on Security and Privacy, 2017.
32. M. Peng et al., "Edge Intelligence for 6G Networks: Challenges and Solutions", IEEE Wireless Communications, 2023.
33. Y. Mao et al., "A Survey on Mobile Edge Computing for 6G: K. Matsuda et al., "Field Demonstration of Real-time 14
    a. Tb/s 220 m FSO Transmission with Class 1 Eye-safe 9- Fundamentals, Applications, and Challenges", IEEE IoT Journal, 2022.
34. aperture Transmitter," Optical Fiber Communications Conference and Exhibition (OFC), San Francisco, CA,USA, 2021, pp. 1-3 https://gtr.ukri.org/projects?ref=45364 [4] ITU-T Y.3800,
35. "Overview on networks supporting quantum key distribution", October 2023.
36. ETSI GS QKD 004, "Quantum Key Distribution (QKD); Application Interface", December 2023.

Received: August 07, 2025