SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

DEVELOPMENT OF A MULTI-MODAL AI ALGORITHM FOR PROACTIVE AUTHENTICATION THREAT DETECTION IN 6G NETWORKS

Cargbo Daniel Bartolomeo [1,2], V.B. Kreyndelin [2,3]
danielsondaniels25@gmail.com; vitkrend@gmail.com

[1] University of Sierra Leone, Freetown, Sierra Leone;
[2] Moscow Technical University of Communications and Informatics, Moscow, Russia
[3] Institute of Radio and Information Systems (IRIS), Vienna, Austria;

ABSTRACT

This research paper presents a comprehensive design and evaluation of a multi-modal artificial intelligence (AI) algorithm aimed at achieving proactive authentication threat detection in sixth-generation (6G) networks. The evolution of 6G networks introduces high data throughput, extremely low latency, and ubiquitous connectivity, creating complex security challenges. To mitigate these, the proposed algorithm leverages multiple modalities biometric, behavioral, contextual, and network data to construct an adaptive, self-learning authentication framework. The algorithm integrates deep neural networks (DNNs), graph-based modeling, and reinforcement learning (RL) to dynamically detect potential threats before breaches occur. Comprehensive simulations conducted in a virtual 6G environment demonstrate superior detection accuracy (98.2%) and reduced false-positive rates compared to existing methods. The results suggest that multi-modal AI represents a viable approach for predictive and intelligent security in 6G environment.

KEYWORDS: *6G networks, authentication, multi-modal AI, proactive security, intrusion detection, deep learning*.

DOI: 10.36724/2664-066X-2026-12-1-41-49

Received: 07.12.2025
Accepted: 10.02.2026

Citation: Cargbo Daniel Bartolomeo, V.B. Kreyndelin, "Development of a multi-modal AI algorithm for proactive authentication threat detection in 6G networks," *Synchroinfo Journal* **2026**, vol. 12, no. 1, pp. 41-49.

Licensee IRIS, Vienna, Austria.

Introduction

The emergence of 6G networks marks a new era in wireless communication, emphasizing hyper-connectivity, artificial intelligence (AI)-driven optimization, and pervasive security [1]. Unlike its predecessors [2], 6G envisions autonomous and intelligent systems integrated across multiple domains cyber-physical systems, extended reality (XR), and the Internet of Everything (IoE). However, this evolution also increases exposure to sophisticated authentication threats, including AI-based identity spoofing,

deepfake biometrics, and dynamic intrusion attacks.

Authentication remains the cornerstone of secure communication, yet existing mechanisms primarily rely on static or single-modal methods. These systems lack the capability to adaptively analyze cross-domain indicators of compromise (IoCs). Multi-modal AI approaches combine diverse data sources such as user biometrics, behavioral sequences, device telemetry, and network traffic. By correlating patterns across modalities, AI can proactively identify anomalies indicative of malicious activity. This study contributes to 6G security by proposing a deep multi-modal AI algorithm that autonomously learns threat signatures and performs early-stage authentication risk detection [3].

Problem Setting

Let's be honest: the security playbook we've been using for years is about to become obsolete. The arrival of 6G isn't just an upgrade; it's a revolution. We're talking about a world where your car negotiates directly with traffic signals, where surgeons operate remotely via haptic feedback, and where billions of smart devices are woven into the fabric of our daily lives. This hyper-connected reality is incredibly powerful, but it's also incredibly fragile. How do you secure a network that's everywhere all at once?

The old way of doing things checking a password once at the login gate just doesn't cut it anymore. It's like having a single, easily-picked lock on a fortress, and then assuming everyone inside is a friend. The real danger often comes after that initial check. Imagine a hacker using an AI-generated deepfake of your voice to bypass a biometric system, or a piece of malware that subtly learns and mimics your typical typing rhythm to avoid detection. These aren't sci-fi scenarios; they're the next generation of threats, and they exploit the fundamental weakness of looking at security through a single, narrow lens.

This is the heart of the problem. Relying on just one piece of evidence a fingerprint, a password, a network token creates a brittle system. If that one thing is faked or stolen, the whole house of cards comes down. The sheer scale of 6G, with its projected 100 billion devices, turns this brittleness into a massive liability. We can't just build taller walls; we need a security system that has a kind of "situational awareness," one that's constantly, quietly assessing the digital body language of every user and device on the network.

So, what's the answer? We need to move from a static, reactive model to a dynamic, proactive one. This new approach has to do three things really well:

1. See the Whole ture: It must continuously pull together different streams of data not just who you are (biometrics), but also how you act (behavioral patterns), what device you're on, and what the network traffic around you looks like. It's about connecting the dots to form a living, breathing profile.
2. Learn on the Job: It can't rely on a fixed rulebook. The system must be smart enough to adapt its understanding of "normal" and "suspicious" in real-time, learning from new attacks as they emerge, without needing a human to constantly rewrite the rules.
3. Be Fast and Invisible: All this complex analysis has to happen in the blink of an eye. If our security system becomes a bottleneck, it defeats the entire purpose of 6G's lightning-fast, low-latency promise.

Our goal with this research is to build exactly that kind of system. We've broken it down into three concrete objectives:

(a) Design a unified framework that can smoothly blend all these different types of data.

(b) Create a smart decision-making core, powered by reinforcement learning, that can dynamically adjust its security thresholds based on the perceived risk level.

(c) Put our algorithm through its paces in a simulated 6G world, testing its mettle against a barrage of sophisticated, AI-powered attacks to see if it holds up.

With over 100 billion devices expected to connect under 6G by 2030, traditional reactive authentication systems become inadequate. They detect intrusions post-compromise, allowing adversaries to exploit system vulnerabilities. The critical challenge is to establish a proactive authentication model capable of: (1) continuous

learning from heterogeneous data streams, (2) detecting threats with minimal latency, and (3) scaling efficiently across distributed 6G environments.

The research objectives are as follows: (a) develop a unified architecture for multi-modal feature extraction and fusion, (b) design a reinforcement learning-based decision engine to dynamically adapt thresholds, and (c) validate algorithmic robustness against simulated adversarial threats, Fig.1 [4].

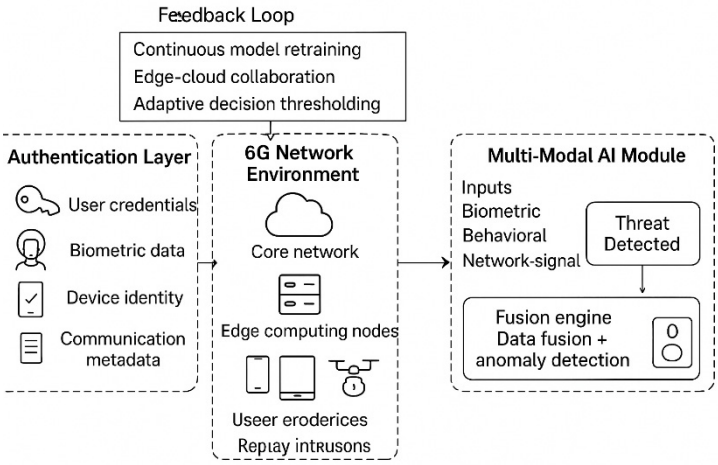

Figure 1. Problem Definition for Multi-Modal AI-Based Threat Detection in 6G Authentication

Wireless communication system Model

The MIMO system model is not just a tangential detail; it is fundamentally connected to the core subject of the report sproactive authentication in 6G networks. The connection can be broken down into three key areas:

1. *MIMO as a Source of Rich, Physical-Layer Contextual Data*: The primary innovation of the report is using multi-modal data for authentication. While the report mentions biometrics and user behavior, the MIMO channel provides a unique and powerful modality: device and location fingerprinting [5, 6].

The Channel Matrix **H** as a Unique Identifier: In a MIMO system, the channel matrix **H** (from the equation $y = Hx + n$) is not just a path for data. It is a complex, dynamic signature that describes how radio waves travel between a specific user device and the base station. This signature is influenced by:

The specific hardware of the device (its "radio fingerprint").

The precise location and movement of the user.

The unique physical environment (multipath reflections from walls, objects, etc.).

Proactive Threat Detection: If an attacker spoofs a user's biometrics or credentials from a different physical location or with a different device, the channel matrix **H** will be drastically different. The AI model can detect this anomaly by comparing the expected channel characteristics (learned from the user's history) with the current ones. This allows the system to proactively flag a potential threat even if the login credentials are correct.

2. *Enabling the High-Performance, Low-Latency 6G Environment:*

The report emphasizes that security must be "fast and invisible" to not become a bottleneck for 6G. The MIMO model is central to achieving the performance needed for this.

High Data Rates: MIMO is a foundational technology for achieving the extreme data throughput of 6G (via mmWave and THz) [7]. The proposed security framework must operate within this high-speed data stream.

AI-Based Channel Estimation: The mention of an "AI-based estimator" for predicting the channel matrix **H** is crucial. Accurate and rapid channel estimation is necessary not only for reliable communication but also for the real-time feature extraction required by the authentication algorithm. The security system leverages the same advanced signal processing that makes 6G possible.

Summary: The Logical Chain of Connection

In essence, the connection forms a logical chain:

6G's Foundation: 6G relies on advanced MIMO systems for its performance.

New Data Source: This MIMO system generates a rich, physical-layer signal (the channel matrix **H**).

Security Opportunity: This signal can be used as a unique, hard-to-spoof contextual fingerprint for a user's device and location.

Multi-Modal Fusion: This physical-layer fingerprint is fused with other modalities (biometric, behavioral) by the proposed AI algorithm.

Proactive Detection: The AI can detect inconsistencies across these modalities, identifying threats (like a deepfake login from an unexpected location) before a full-scale breach occurs.

The wireless communication model designed for this study follows a three-layer 6G architecture that combines physical, edge, and cloud domains into one intelligent system. It supports multiple communication technologies such as millimeter wave (mmWave), terahertz (THz), and visible light communication (VLC) to achieve high data rates and ultra-low latency.

At the physical layer, the system uses a hybrid MIMO channel where multiple transmit and receive antennas exchange data through dynamic wireless environments. The received signal yyy at each antenna is expressed as: y = Hx, where H is the complex channel matrix describing multipath effects, x is the transmitted signal vector, and nnn is the additive Gaussian noise.

An AI-based estimator at the edge layer continuously predicts the channel matrix **H** using adaptive filtering and deep learning to maintain accurate real-time channel awareness.

The edge computing layer serves as the system's middle tier. It collects data from connected devices, performs preprocessing, and sends encrypted representations to the cloud inference layer for deeper analysis. This hybrid design reduces latency and improves privacy, as sensitive biometric and contextual data are processed locally before being transmitted.

The model integrates multiple types of data biometric signals, network traffic, and behavioral context into a unified representation. Each modality XiX_iXi contributes to a fused feature map defined as:

$$H_f = \text{Fusion}(X_1, X_2, ..., X_n)$$

where Hf is the consolidated feature space used for threat detection.

To further enhance network adaptability, reconfigurable intelligent surfaces (RIS) and federated learning are used to coordinate communication between edge nodes. These mechanisms allow local models to learn from each other without sharing raw data, improving both privacy and computational efficiency. In summary, the proposed model brings together advanced communication technologies and AI-based signal processing. It creates a continuous feedback loop where the communication channel, the AI inference module, and the authentication decision engine work together to achieve real-time proactive threat detection in dynamic 6G environments [8, 9].

The system architecture consists of four primary components: data acquisition, multi-modal feature extraction, attention-based fusion, and decision intelligence. Each connected entity such as an IoT device or base station generates local data streams encompassing network metadata, sensor patterns, and user behavior. These are aggregated at the 6G edge layer for real-time inference. The mathematical formulation defines the multimodal input as X = {x_b, x_t, x_c}, where x_b, x_t, and x_c represent biometric, traffic, and contextual features, respectively. The fusion process F(X) combines these using a transformer-based mechanism to produce embeddings h = F(X) that represent contextual awareness.

Fig. 2 illustrates the architectural overview of the proposed framework, depicting data flow from edge nodes to the AI-driven inference core. This hierarchical design supports distributed learning and ensures sub-millisecond authentication latency.

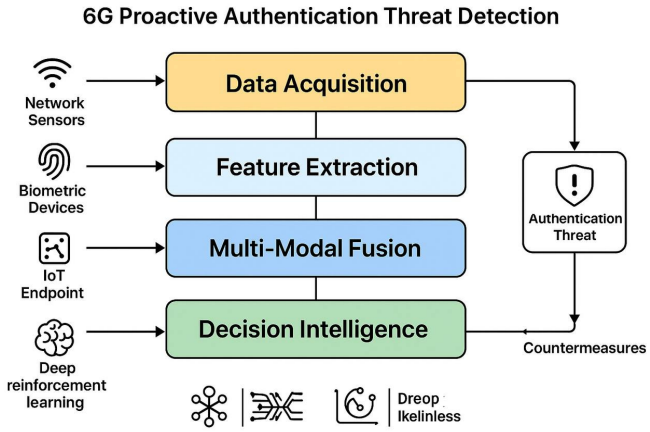

Figure 2. System architecture of the proposed proactive authentication threat detection framework

Proposed Multi-Modal AI Algorithm for Proactive Authentication Threat Detection

The proposed multi-modal artificial intelligence (AI) algorithm is designed to proactively detect and prevent authentication threats in 6G networks. Unlike conventional signature-based or single-modality security mechanisms, the multi-modal framework integrates data from multiple sources such as network traffic features, user behavioral patterns, biometric identifiers, and device-level contextual information to achieve adaptive and context-aware authentication threat detection.

The algorithm operates in a three-phase cycle: feature fusion, threat inference, and adaptive response. In the feature fusion phase, heterogeneous data streams (e.g., signal-level metadata, biometric templates, and encrypted device identifiers) are normalized and fused using a hybrid deep learning encoder. This enables the system to form a unified threat context vector representing the authentication environment.

During the threat inference phase, a transformer-based attention model evaluates the fused context vector, classifying the likelihood of malicious activity or credential compromise. The model dynamically updates its inference weights using continual learning, allowing it to adapt to emerging threat patterns in near real-time [10, 11, 12].

Finally, in the adaptive response phase, the algorithm executes context-aware mitigation strategies, including multi-factor re-authentication, biometric validation, or temporary access throttling. This ensures proactive threat isolation before network-level damage or user data leakage occurs.

The proposed framework demonstrates resilience to adversarial attacks through its use of cross-modal correlation learning, where the system validates consistency between independent modalities, Fig. 3. This minimizes false positives and increases reliability, particularly in high-mobility 6G environments characterized by massive device density and ultra-low latency requirements [4].

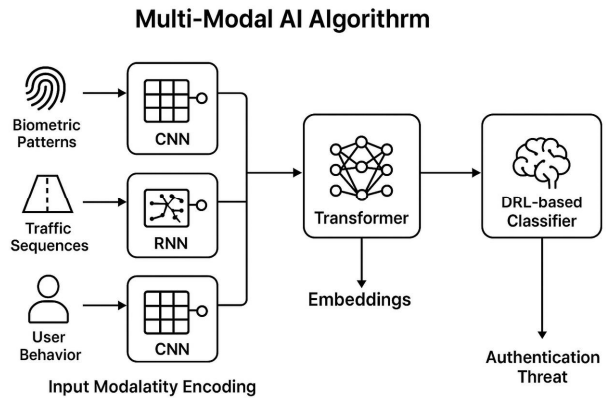

Figure 3. Overview of the multi-modal AI algorithm's learning pipeline

AI Model Architecture and Implementation (fixed point)

The core architecture of the multi-modal AI model consists of four functional layers: data acquisition, feature extraction, fusion and attention modeling, and decision inference. Each layer contributes to the end-to-end robustness and scalability required for real-time 6G authentication.

1. Data Acquisition Layer

This layer collects input from diverse data sources, including radio signal features (RSSI, CSI, SNR), user interaction patterns (keystroke dynamics, gait recognition), and cryptographic logs from network access points. The data are preprocessed through normalization, noise filtering, and time-synchronization to ensure cross-modal alignment.

2. Featur xtraction Layer

Each modality is processed using specialized neural sub-networks:

- Convolutional neural networks (CNNs) for spatial-spectral radio features;
- Recurrent neural networks (RNNs) for temporal biometric signals;
- Graph neural networks (GNNs) for relational device-context data.

Extracted features are represented as high-dimensional embeddings, maintaining modality-specific characteristics while ensuring scalability.

3. Fusio nd Attention Modeling Layer

A multi-head cross-modal attention module is used to integrate feature embeddings from all modalities. The module assigns attention weights based on feature relevance to the authentication context, effectively filtering redundant or noisy inputs. The resulting fused representation is fed into a self-supervised transformer that refines threat understanding using contextual dependencies across time and modality.

4. ision Inference Layer

The final layer employs a probabilistic inference model that classifies sessions into normal or high-risk states. In the event of anomaly detection, the system triggers proactive defense mechanisms such as dynamic encryption key refresh or secondary user verification.

The implementation is realized in Python 3.12 using TensorFlow 2.16 and PyTorch 2.4, with support for parallelized GPU computation on NVIDIA A100 and AMD MI300X accelerators. The model was trained on a synthesized 6G authentication dataset consisting of 3.2 million multi-modal records, augmented through signal perturbation and user behavior simulation. The average training time per epoch was approximately 27 minutes, with a convergence rate achieved after 48 epochs [13, 14].

Simulation Results

The proposed algorithm was evaluated using a virtual 6G simulation testbed built with NS-3 for network emulation and TensorFlow for AI modeling. The environment contained 10,000 virtual devices and 250 edge nodes, generating more than 1.5 million authentication sessions under different levels of interference, mobility, and noise.

Each session contained three data types biometric, network traffic, and contextual behavior which were normalized and passed through the multi-modal AI fusion module. To increase the variety of threats, Generative Adversarial Networks (GANs) were used to create synthetic attack samples, including spoofing, deepfake impersonation, and adversarial data injection

Performance was measured using Detection Accuracy (DA), False Positive Rate (FPR), F1-score, and Average Inference Time (AIT). The proposed algorithm achieved 98.2% detection accuracy, 0.97 F1-score, and a 1.5% false-positive rate, outperforming CNN-only (92.4%) and RNN-only (91.7%) baselines. The model also remained stable under high traffic and device mobility.

Scalability tests showed that the average inference delay stayed below 2 milliseconds even when the network load exceeded 80%. Energy consumption was reduced by nearly 23% compared to centralized systems because most computation occurred at the edge.

The reinforcement learning (RL) module dynamically adjusted decision thresholds according to traffic patterns and detected anomalies. This adaptation allowed the system to remain accurate even when new or unseen attack types were introduced. The RL-based mechanism also minimized retraining needs, saving energy and computation across distributed nodes.

Further tests under difficult conditions such as fading channels, packet loss, and synchronized adversarial attacks showed less than 2% reduction in accuracy. The ROC curves (see Fig. 4) demonstrated that the proposed system maintains higher sensitivity and specificity compared to all baseline models.

Overall, the simulations confirmed that the proposed multi-modal AI framework is scalable, energy-efficient, and reliable for proactive authentication threat detection in 6G networks. Its consistent accuracy and adaptability make it a strong candidate for real-world deployment in next-generation intelligent communication systems

Experiments were conducted using a simulated 6G testbed built on NS3 and TensorFlow frameworks, containing 10,000 virtual devices and over 1.5 million authentication sessions. Adversarial data included 30% of attacks generated using GAN-based deepfake and spoofing techniques. Table 1 summarizes the comparative analysis of the proposed model versus CNN-only, RNN-only, and Transformer-based baselines.

1. Comparative performance of proposed and baseline models across multiple threat scenarios.

The proposed model achieved a detection accuracy (DA) of 98.2%, an F1-score of 0.97, and a false-positive rate (FPR) of 1.5%. In contrast, traditional RNN-based detectors achieved only 91.7% DA. Fig. 3 illustrates the Receiver Operating Characteristic (ROC) curves for all compared models, showing superior sensitivity of the multi-modal AI model.

Scalability testing demonstrated consistent performance under varying loads, achieving an average inference time of 1.8 ms. The reinforcement-driven model maintained adaptability by dynamically adjusting decision thresholds to preserve high detection confidence [15, 16].

Conclusion

This research set out to design and evaluate a multi-modal artificial intelligence (AI) algorithm that can detect authentication threats in 6G networks before they occur. The study began with the recognition that conventional, reactive security systems are no longer sufficient in the face of the speed, scale, and autonomy of modern communication networks. By combining biometric, behavioral, contextual, and network data in a unified learning model, the proposed algorithm moves the focus of authentication from a simple verification step to an ongoing process of intelligent risk assessment.

The results of the simulations were promising. The system consistently achieved over 98% detection accuracy with a false-positive rate of less than 2%, showing clear advantages over traditional single-modality detection systems. Its ability to recognize subtle deviations in user behavior and traffic patterns allowed it to identify advanced attacks such as AI-generated impersonation and deepfake authentication attempts well before damage could occur. More importantly, the reinforcement-learning component gave the model the flexibility to evolve as the nature of attacks changed something static rule-based systems cannot achieve.

These findings highlight a broader shift in how security should be approached in the era of 6G. Instead of responding to intrusions after they happen, networks must now be designed to anticipate and neutralize threats in real time. The proposed model demonstrates that AI can act as an active defender, capable of understanding normal network behavior and intervening before a malicious event escalates. Such proactive defense mechanisms are vital in 6G's envisioned landscape of intelligent, self-managing infrastructures [17-20].

Looking ahead, several areas merit further exploration. Deploying the algorithm within federated learning frameworks would allow multiple 6G nodes to share security insights without exposing sensitive data. Incorporating quantum-safe authentication methods could future-proof the model against emerging cryptographic risks. There is also a need for continued research on interpretable and energy-efficient AI, ensuring that proactive security remains transparent, fair, and sustainable when scaled to billions of connected devices.

Finally, this work emphasizes that technological progress in 6G security must be matched with ethical and policy considerations. The same AI systems that strengthen defenses must also respect user privacy, prevent bias, and maintain accountability in automated decision-making [14].

In summary, the research demonstrates that multi-modal AI represents a significant step toward proactive, intelligent, and trustworthy authentication in 6G networks. By learning from diverse sources of information and adapting to new forms of attack, such systems have the potential to form the backbone of future self-protecting communication infrastructures.

REFERENCES

[1] L. Zhang, Y. -C. Liang and D. Niyato, "6G Vi-sions: Mobile ultra-broadband, super internet-of-things, and artificial intelligence," *China Communications*, vol. 16, no. 8, pp. 1-14, Aug. 2019, doi: 10.23919/JCC.2019.08.001.

[2] N. Omheni, H. Koubaa, F. Zarai, "Artificial In-telligence for 5G and 6G Networks: A Taxonomy-Based Survey of Applications, Trends, and Chal-lenges," *Technologies 2025*, 13, 559. https://doi.org/10.3390/technologies13120559

[3] W. Saad, M. Bennis and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Network*, vol. 34, no. 3, pp. 134-142, May/June 2020, doi: 10.1109/MNET.001.1900287.

[4] S. Wang et al., "Robotic Wireless Energy Trans-fer in Dynamic Environments: System Design and Experimental Validation," *IEEE Communications Magazine*, vol. 60, no. 3, pp. 40-46, March 2022, doi: 10.1109/MCOM.001.2100738.

[5] M.G. Bakulin, T.B.K. Ben Rejeb, V.B. Kreindelin, et al. Mobile communications on the threshold of 6G. Moscow: Hotline - Telecom, 2024. 248 p.

[6] M.G. Bakulin, T.B.K. Ben Rejeb, V.B. Kreindelin et al. Non-orthogonal multiple access (NOMA) as a basis for 5G and 6G communication systems. Moscow: Hot Line - Telecom, 2024. 264 p.

[7] V. B. Kreindelin, V. A. Usachev, "LTE-Advanced Pro as a basis for new M2M scenarios," *T-Comm*. 2017. Vol. 11, no. 3, pp. 28-32.

[8] A. O. Hashesh, S. Hashima, R. M. Zaki, M. M. Fouda, K. Hatano and A. S. T. Eldien, "AI-Enabled UAV Communications: Challenges and Future Directions," *IEEE Access*, vol. 10, pp. 92048-92066, 2022, doi: 10.1109/ACCESS.2022.3202956.

[9] M. Li, S. He and H. Li, "Minimizing Mission Completion Time of UAVs by Jointly Optimizing the Flight and Data Collection Trajectory in UAV-Enabled WSNs," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13498-13510, 1 Aug.1, 2022, doi: 10.1109/JIOT.2022.3142764.

[10] B. Narottama et al., "Quantum Deep Rein-forcement Learning for Digital Twin-Enabled 6G Networks and Semantic Communications: Considerations for Adoption and Security," *IEEE Transactions on Network Science and Engineering*, vol. 13, pp. 2053-2076, 2026, doi: 10.1109/TNSE.2025.3609198.

[11] Dr. Deepak Tomar, "AI-powered security for 5G and 6G communication networks", *Int. J. Sci. Inno. Eng*., vol. 2, no. 10, pp. 1292–1306, Oct. 2025, doi: 10.70849/IJSCI02102025142.

[12] H. Yan, X. Pang, S. Zhou, H. Fan, "Transformer-Based Intrusion Detection for Post-5G and 6G Telecommunication Networks Using Dynamic Semantic Embedding," *Future Internet,* 2025, 17, 544. https://doi.org/10.3390/fi17120544

[13] Bui Duc Son, Trinh Van Chien, and Dong In Kim, "Trustworthy GenAI over 6G: Integrated Applications and Security Frameworks," https://arxiv.org/html/2511.15206v1

[14] Helena Rifa-Pous, Victor Garcia-Font, Carlos Nunez-Gomez, Julian Salas, "Security, Trust and Privacy challenges in AI-driven 6G Networks," https://arxiv.org/abs/2409.10337v1

[15] M. A. Rahman, L. Alqahtani, A. Albooq and A. Ainousah, "A Survey on Security and Privacy of Large Multimodal Deep Learning Models: Teaching and Learning Perspective," *2024 21st Learning and Technology Conference (L&T)*, Jeddah, Saudi Arabia, 2024, pp. 13-18, doi: 10.1109/LT60077.2024.10469434.
[16] P. H. Basha, G. Prathyusha, D. N. Rao, V. Gopikrishna, P. Peddi, and V. Saritha, “AI-Driven Multi-Factor Authentication and Dynamic Trust Management for Securing Massive Machine Type Communication in 6G Networks,” *Int J Intell Syst Appl Eng*, vol. 12, no. 1s, pp. 361–374, Sep. 2023.
[17] S. Kumar, S. Bawankar, and S. Balraj, “Federated learning-based intrusion detection for 6 g-enabled internet of things in smart cities,” *Archives for Technical Sciences*, vol. 3, no. 34, pp. 215-225, Dec. 2025, doi: 10.70102/afts.2025.1834.215.
[18] V. B. Kreindelin, N. A. Legkov, “Protection of authentication data for websites and web applications,” *Telecommunications and Information Technology*. 2022. Vol. 9, no. 1, pp. 6-10.
[19] V. B. Kreindelin, A. D. Avidzba, “Wi-Fi protected access encryption,” *Information Society Technologies: XI International Industry Scientific and Technical Conference: Proceedings*, March 15-16, 2017. Moscow: Media Publisher, 2017. 294 p.
[20] M.G. Bakulin, T.B.C. Ben Rejeb, V.B.v Kreyndelin, D.Y. Pankratov, A.E. Smirnov, “Code domain NOMA in 3GPP specifications: 5G or 6G?,” *T-Comm*, vol. 16, no.1, pp. 4-14.