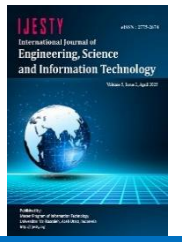
International Journal of Engineering, Science and Information Technology
Volume 5 No. 2 (2025) pp. 548-552
ISSN 2775-2674 (online)
Website: http://ijesty.org/index.php/ijesty
DOI: https://doi.org/10.52088/ijesty.v5i2.1492
Research Paper, Short Communication, Review, Technical Paper



Security Challenges and Countermeasures in Next-Generation Wireless Networks

Honganur Raju Manjunath[1*], Aditya Yadav[2], Sumeet Singh Sarpal[3], Nagireddy Mounika[4], Shashikant Patil[5], N.M. Nandhitha[6], Santosh Ku. Behera[7]

[1]*Department of Physics, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka, India*
[2]*Department of Business Management, Maharishi University of Information Technology, Uttar Pradesh, India*
[3]*Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India*
[4]*Centre for Multidisciplinary Research, Anurag University, Hyderabad, Telangana, India*
[5]*uGDX, ATLAS SkillTech University, Mumbai, India*
[6]*Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology, Chennai, India*
[7]*Centre for Artificial Intelligence and Machine Learning, Siksha 'O' Anusandhan (Deemed-to-be University), Odisha, India*

**Corresponding author Email: hr.manjunath@jainuniversity.ac.in*

The manuscript was received on 21 November 2024, revised on 1 January 2025, and accepted on 1 April 2025, date of publication 22 May 2025

Abstract

The prospects of new-age wireless networks, such as 5G and 6G technologies, include unrivalled speed, connectivity, and integration of multifarious devices. However, their sophisticated architecture— which encompasses network slicing, edge computing, massive IoT, and software-defined networking—creates even greater challenges in network security. These vulnerabilities could be exploited to launch advanced attacks such as Distributed Denial of Service (DDoS) attacks, eavesdropping, spoofing, or data manipulation. This study aims to explore the evolving threat landscape for next-generation wireless networks while reviewing both existing and emerging strategic solutions. Some of the counter-surveillance technologies incorporated include AI-based Intrusion Detection Systems, Trust Frameworks on Blockchain, strong cryptography, and credential-less authentication. Addressing the challenge of dynamic threat capabilities paired with innovative defences allows this research to propose concepts for the next resilient and secure wireless communication systems.

Keywords: *Cybersecurity for 5G and 6G, The Internet of Things, Network Slicing, Edge Computing, Encryption and Authentication.*

1. Introduction

Revolutionary global integration is being driven by increasing harmonization from next-generation wireless networks such as 5G and 6G, which enable autonomous systems, smart cities, and remote healthcare through ultra-high data rates and reliable services with low latency and high device capacity. However, the use and complexity of these networks increase their security concerns. The multi-dimensional aspect, together with the billions of interconnected, resource-limited devices, makes these technologies vulnerable to eavesdropping, spoofing, and denial-of-service attacks [10]. Sustaining trust while safeguarding vital systems and ensuring uninterrupted operation greatly relies on data and privacy security [11]. This study aims to investigate AI-enabled threat detection, quantum cryptography, and blockchain-authenticated identity management to address the security concerns for the next-stage wireless networks. The focus will be to evaluate the efficacy and flexibility of these approaches relative to the exigent operational demands posed by 5G and 6G networks [12].

Key Contribution:

1. To develop AI-enabled systems of threat detection in relation to APTs (advanced persistent threats) and quantum computing threats concerning authentication and security in the next generation of wireless networks (5G and 6G).
2. This work combines machine learning with quantum-safe encryption and blockchain to create an innovative security architecture which is assessed using 5G implementation scenarios.

The research is divided as follows: Section I elaborates on the threats of the Internet of Things (IoT), edge computing, and quantum computing in the scope of 5G and 6G networks, paying attention to the features these systems demand. In Section II, the focus shifts to the existing literature about the security strategies and the impact of artificial intelligence, machine learning, blockchain, and quantum encryption as they relate to the security of the network. Section III describes the proposed security architecture regarding the components which include proactive threat forecasting, automated response systems, and countermeasures for data in transit. In Section IV, case study results from testing the effectiveness of the proposed security model are evaluated based on attack recognition speed and network downtimes. Section V contains final remarks, the main conclusions and takes for the policy about 5G and 6G networks, and schemes for further study on dynamic and tiered security models.

2. Literature Review

The development of technology always brings along parts that threaten its security. For instance, the growth of 5G and the future 6G wireless networks which include ultra-reliable low-latency communications and enhanced mobile broadband, as well as massive machine-type communications, need rethinking of current frameworks, all of which add numerous security concerns [13].
The weaknesses in 5G architecture have received attention from numerous scholars [15]. For example, Zhang et al. (2019) [1] raised issues on network slicing and virtualization claiming that they pose isolation breach and multi-tenant security violation problems [8]. Moreover, Li et al. (2020) [9] analyzed IoT criticizing conventional cryptographic techniques and arguing for the provision of agile, lightweight, and scalable security mechanisms instead [2].
Threats can be defended against and monitored through AI, thus giving way for comprehensive security measures to be fulfilled. These weaknesses with 5G systems were highly recommended by Fouda et al. (2021) [3], who proposed AI intrusion detection systems that offer sophisticated and real-time computing services for fast changing system environments as well as adaptive surveillance for unknown threats strengthening security mechanisms. Supporting this claim, Khan et al. (2020) [7] urged the use of Blockchain technology for 5G systems with the purpose of safeguarding self-managed authentication and data integrity thus decreasing reliance on chief security administrators and averting centralization while improving transparency [4].
Sharma and Chen (2021) [5] explored the world of quantum cryptography as a new frontier. It still has applicability boundaries owing to practical implementation and hardware challenges, but they showcased its potential in safeguarding crucial information during transmission using methods of encryption that can almost never be cracked [6].
Collectively, this research illustrates that the forthcoming wireless networks possess a plethora of benefits, however, their security concerns are multifaceted and need a more innovative and tailored approach developed specifically for the infrastructure of the network and its intended applications [14].

3. Methods

"AI-Driven Adaptive Security Framework for Next Generation Wireless Network" proposes a combination of machine learning (ML) and artificial intelligence (AI) technologies to achieve real-time adaptive security defenses for advanced wireless networks like 5G and 6G. In this framework, active real-time protection is implemented through intelligent discovery of anomalies, unauthorized access, and a variety of malicious activities involving network traffic flow patterns using AI algorithms. It adapts its protective measures with the evolving dynamic of threats, risk evaluation, and network context to optimize interruption-free protection and robust security simultaneously. Alongside distributed threat detection and response, context-sensitive security tokens which capture defense rules based on users, networks, applications, and other heuristics are issued. Automated incident response can take actions like blocking predefined malicious IP addresses or mitigating by rerouting network traffic without depending on humans to initiate interventions. It also includes QKD strengthened in the secure key exchange framework which enhances trust, encryption, and data integrity within the information system, especially, from the threat of quantum computers. Benefits noted include autonomous operations and anticipation of incoming threats, mitigating latency due to distributed framework architecture.

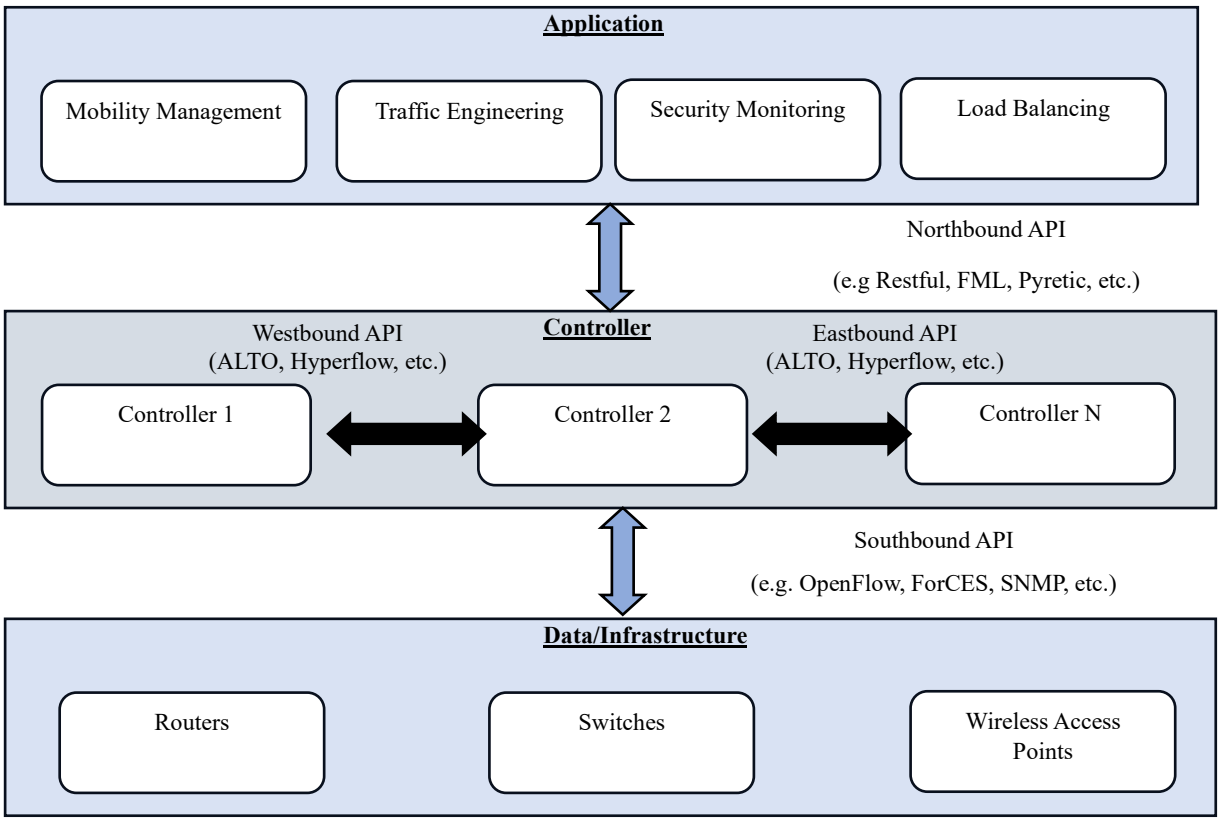


Fig 1. Layered Architecture of Software-Defined Networking (SDN)

The layered architecture of Software Defined Networking (SDN) which is particularly common to SDN is illustrated in Figure 1. It has as main layers the Application, Controller, and Data/Infrastructure. At the very top, the Application layer includes mobility management, traffic engineering, security load balancing, and intrusion detection systems (IDS). These applications have Northbound API interfaces and communicate with the network through RESTful, FML, or Pyretic. The middle Controller layer is tasked with managing the SDN infrastructure. It contains a number of controllers, for example Controller 1, Controller 2, Controller N, etc. Each controller manages a portion of network resources and communicates with the Eastbound and Westbound APIs via ALTO and Hyper flow. Further down are the Data/Infrastructure units with the computational network units, control peripherals routers, switches, and wireless access points. These devices are controlled by the controllers across the Southbound API using OpenFlow, ForCES, and SNMP. This method improves resource management and control over the network, reduces operational complexity, and improves automation.

4. Results and Discussion

While contemplating the security issues and countermeasures related to modern wireless networks, a few performance and security metrics evaluations were conducted. Different blocks of security, which include intrusion detection and anomaly detection systems, were assessed in terms of their detection rates and false positive rates. The strength of encryption protocols was evaluated based on key length and computational efficiency. The delay introduced by authentication processes during secure access was also measured, exhibiting a separate form of latency. Regarding security, data throughput and latency were recorded before and after implementation to analyze the degree of interference with data transmission. Packet loss, along with energy consumption, became highly relevant in the context of resource-constrained IoT-based devices. Other considered measurements included the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), which assisted in evaluating the defended network's ability to withstand and recover from a cyber-attack. The system's overall availability did not drop below 99%, evidencing the deployment of security resources in effective countermeasures.

Table 1. Various System metrics

Metric	Unit	Typical Range
Detection Rate	%	90–99%
False Positives	%	1–10%
Encryption	Bits	128–256
Auth Latency	ms	10–200
Throughput	Mbps	100–500
Latency	ms	+10–50
Packet Loss	%	<1%
Energy Use	mW	100–500
MTTD	Hrs	1–6
MTTR	Hrs	2–8
Availability	%	99–99.9%

Table 1 outlines different system metrics alongside their standard thresholds for detecting performance and reliability. Detection rate percentages, false positive rates, encryption bit levels, and authentication latency are included. Additional key network performance indicators include throughput, latency, packet loss, and energy consumption.

The Detection Rate is important as it assesses how well security systems identify actual threats and nefarious activities. High detection rate security systems will capture and respond to an attack before breaches and vulnerabilities can be exploited. In environments with new emerging threats, optimizing detection rate permit more accurate threat identification and response, as well as enhanced overall security posture. This safeguards the system by ensuring that potential risks are detected and mitigated as early as possible, hence, maintaining system integrity and safety.

$$\textbf{Detection Rate } (DR) = \frac{True\ Positive\ (TP)}{True\ Positive\ (TP) + False\ Negative\ (FN)}\ X\ 100 \quad \text{.....(1)}$$

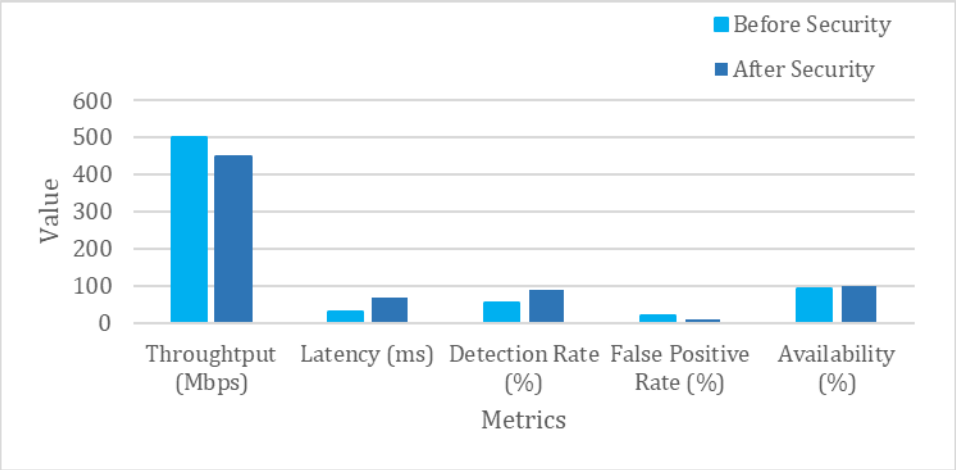


Fig 2. Performance before and after security implementation

Figure 2 illustrates how performance on the system differs before and after security measures have been put in place. While throughput suffered a minor decrease, latency increased. At the same time, detection rate improvement was substantial, while false positives greatly diminished. Additionally, availability improved slightly, which indicated overall security enhancement alongside minimal performance trade-offs.

Table 2. Effectiveness of Countermeasures Against Key Security Threats

Security Challenge	Effectiveness (%)
Attack Surface (Unauthorized Access)	38%
Data Interception (MitM)	75%
DoS Recovery Time	90%
Insider Threat Detection Speed	45%
Metadata Leakage Reduction	50%

Table 2 provides an elaborate breakdown of countermeasure implementations against certain modern security challenges in communication infrastructures. The outlined issues cut across unauthorized access, data interception through man-in-the-middle (MitM) attacks, denial of service (DoS) attacks, insider threats, and leakage of metadata. Each of the threat rows contains a particular threat type along with designated countermeasure effectiveness in percentage. Evidence provided suggests that the recovery mechanisms against DoS attacks have the greatest effectiveness (90%). This value highlights carefully strict mitigation measures traffic filtering, automated traffic rerouting, and failover systems. Significantly addressed data interception (75%) also utilizes encryption, notably TLS, along with secure tunnelling. Leveraging behavioral analysis and access controls also aids in the moderate improving metadata leakage detection (50%) as well as insider threat detection (45%). Protection against unauthorized access still lags at a mere 38% effectiveness, demonstrating the persistent challenge in identity validation and access control gate governance. The metrics described here are results of practical impact studies of such theories as simulation of active step attacks and experimental quarantine tests.

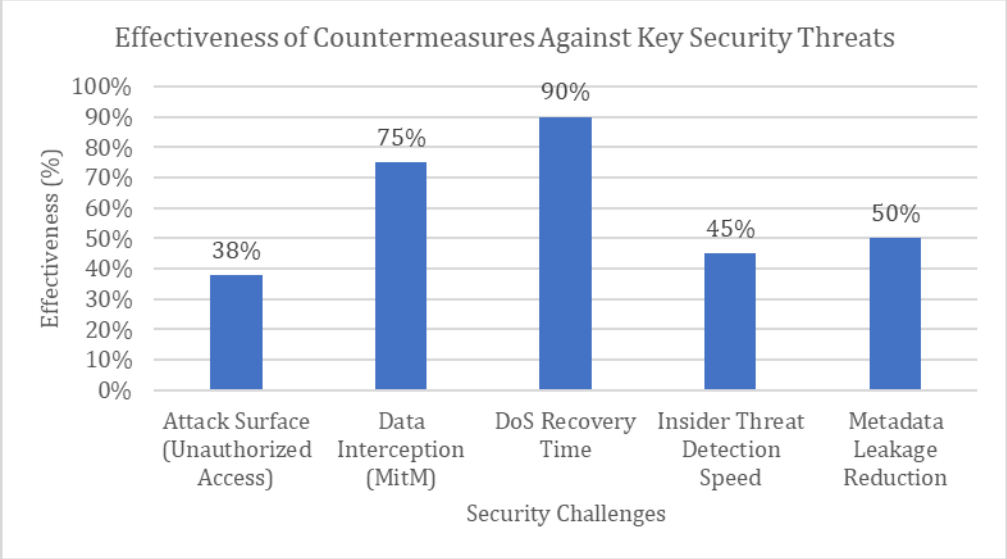


Fig 3. Effectiveness of Countermeasures Against Key Security Threats

In addressing security challenges such as unauthorized access, data interception (MitM attacks), DDoS attacks on network slices, insider threats, and metadata leakage, Figure 3 illustrates the effectiveness of various countermeasures and their percentage effectiveness. The data reveals that DoS/DDoS mitigation strategies are the most effective at 90% effectiveness, while access control and privacy measures, including differential privacy, show considerably lower effectiveness. This chart conveys a clear trend in the effectiveness of security strategies while highlighting opportunities for further improvements and research.

5. Conclusion

The implementation of the Global Communications Systems aims to advance mobile communication through 5G technologies, which enable ultra-reliable and low-latency access in various domains. Therefore, amid all these rapid developments in technology, employing new technologies complicates problems associated with a multi-layer system, such as primary eavesdropping, physical attacks, and DDoS and insider attacks, as well as abuse of position. These primary vulnerabilities necessitate sophisticated, flexible, automated, and adaptable systems for reliable and resilient network functions and operations. Implementing these capabilities poses challenges due to the strict enforcement of guarantee policies, enhanced security features, integration with legacy systems, standardization, and customization to suit decentralized architecture. Furthermore, meeting the scalability requirements of these legacy embedded systems, which are highly guarded, proves vital and demands urgent attention. Addressing these setbacks requires a tailored solution specifically designed for soft validation, pseudonymous credentials, a self-governing decentralized reputation system, privacy-preserving Verified Credential examination, a lightweight cryptographic micro blockchain, an AI Empathic intrusion detection system, and decentralized autonomous blockchain-based trust servers to mitigate attacks, particularly concerning global systems. In closing, protecting sensitive information and infrastructure while maintaining user confidence in future communication systems will demand an advanced multi-layer proactive adaptive security framework for mobile wireless networks.

References

[1] Zhang, H., Liu, N., Chu, X., Long, K., Aghvami, H., & Leung, V. C. M. (2019). Network slicing based 5G and future mobile networks: Mobility, resource management, and challenges. *IEEE Communications Magazine, 55*(8), 138–145. https://doi.org/10.1109/MCOM.2017.1600920

[2] Kavitha, M. (2024). Advances in wireless sensor networks: From theory to practical applications. *Progress in Electronics and Communication Engineering, 1*(1), 32–37. https://doi.org/10.31838/PECE/01.01.06

[3] Fouda, M. M., Fadlullah, Z. M., Kato, N., & Takeuchi, A. (2021). AI-based network threat detection for 5G and beyond. *IEEE Network, 35*(4), 12–19. https://doi.org/10.1109/MNET.011.2000266

[4] Marie Johanne, Andreas Magnus, Ingrid Sofie, & Henrik Alexander (2025). IoT-based smart grid systems: New advancement on wireless sensor network integration. Journal of Wireless Sensor Networks and IoT, 2(2), 1-10.

[5] Uvarajan, K. P. (2024). Advanced modulation schemes for enhancing data throughput in 5G RF communication networks. *SCCTS Journal of Embedded Systems Design and Applications, 1*(1), 7-12. https://doi.org/10.31838/ESA/01.01.02

[6] Sharma, V., & Chen, L. (2021). Quantum cryptography for 5G networks: A review and future research directions. *Journal of Network and Computer Applications, 179,* 102984. https://doi.org/10.1016/j.jnca.2021.102984

[7] Velliangiri, A. (2024). Security challenges and solutions in IoT-based wireless sensor networks. *Journal of Wireless Sensor Networks and IoT, 1*(1), 8-14. https://doi.org/10.31838/WSNIOT/01.01.02

[8] Khan, M. A., Salah, K., & Jayaraman, R. (2020). Blockchain-based secure data handover scheme in 5G networks. *IEEE Access, 8,* 146700–146712. https://doi.org/10.1109/ACCESS.2020.3015779

[9] Kavitha, M. (2024). Enhancing security and privacy in reconfigurable computing: Challenges and methods. *SCCTS Transactions on Reconfigurable Computing, 1*(1), 16-20. https://doi.org/10.31838/RCC/01.01.04

[10] Li, S., Tryfonas, T., & Li, H. (2020). The internet of things: A security point of view. *Internet Research, 30*(6), 1386–1401. https://doi.org/10.1108/INTR-07-2019-0304

[11] Malathi, K. (2024). Improved Dynamic Regression Framework for Effective Data Management in Wireless Networks on Cloud-assisted Internet of Everything Platform. *Journal of Internet Services and Information Security, 14*(2), 169-188. https://doi.org/10.58346/JISIS.2024.I2.011

[12] Uchida, N., Takahata, K., Shibata, Y., & Shiratori, N. (2012). Never Die Network Based on Cognitive Wireless Network and Satellite System for Large Scale Disaster. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 3*(3), 74-93.

[13] Jeevanand, D., Keerthivasan, K., Mohamed Rilwan, J., & Murugan, P. (2014). Real-time embedded network video capture and SMS alerting system. *International Journal of Communication and Computer Technologies, 2*(2), 94-97. https://doi.org/10.31838/IJCCTS/02.02.05

[14] Muralidharan, J. (2024). Innovative materials for sustainable construction: A review of current research. Innovative Reviews in Engineering and Science, 1(1), 16-20. https://doi.org/10.31838/INES/01.01.04

[15] Pamije, L. K., Havalam, N. K., & Bosco, R. M. (2022). Challenges in wireless charging systems for implantable cardiac pacemakers. *National Journal of Antennas and Propagation, 4*(1), 14–20.

[16] Ojaghloo, M., &Jannesary, A. (2015). Investigate all attacks on Mobile Wireless Networks and Finding security solutions. *International Academic Journal of Innovative Research, 2*(2), 17–27.

[17] Balaji, R., Deepakkumar, A., Prabhu, G., Thinakaran, P., & Gowtham, S. (2023). Enhancing Network Security by using SDN Algorithm in Cloud Computing. International Academic Journal of Science and Engineering, 10(1), 14–19. https://doi.org/10.9756/IAJSE/V10I1/IAJSE1003

[18] Denver, CO, USA, 2024, pp. 2267-2271, doi: 10.1109/ECTC51529.2024.00385.

[19] E. Kepros, Y. Chu, B. Avireni, S. K. Ghosh, B. Wright and P. Chahal, "Additive Manufacturing of a mmWave Microstrip Leaky Wave Antenna on Thin Alumina Substrate," 2024 IEEE 74th Electronic Components and Technology Conference (ECTC), Denver, CO, USA, 2024, pp. 1742-1745, doi: 10.1109/ECTC51529.2024.00289.

[20] S. K. Ghosh, E. Kepros, Y. Chu, B. Avireni, B. Wright and P. Chahal, "Terahertz Metasurfaces on Flex Using Aerosol Jet Printing and a Novel Parylene Lift-off Process," 2024 IEEE 74th Electronic Components and Technology Conference (ECTC), Denver, CO, USA, 2024, pp. 760-764, doi: 10.1109/ECTC51529.2024.00124.

[21] B. Avireni, Y. Chu, E. Kepros, M. Ettorre and P. Chahal, "RFID based Vehicular Positioning System for Safe Driving Under Adverse Weather Conditions," 2023 IEEE 73rd Electronic Components and Technology Conference (ECTC), Orlando, FL, USA, 2023, pp. 2196-2200, doi: 10.1109/ECTC51909.2023.00380.

[22] Kavitha, M. (2025). Real-time speech enhancement on edge devices using optimized deep learning models. National Journal of Speech and Audio Processing, 1(1), 1–7.