IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

AI-Driven Network Security in Next-Generation 5G/6G Smart Environments

Pardeep Singh
Head of Department (CSE)
Guru Tegh Bahadur 4th Centenary Engineering College, New Delhi, India
singh.pardeep@gmail.com

Abstract: *Technology is currently spreading at an exponential rate. more accessibility, use, and application of this technology across all sectors and industries have been made possible by technological advancements, more computing power, and lower costs. Traditionally labour-intensive data analysis tasks can now be completed rapidly and effectively thanks to the development of smart and autonomous technologies like artificial intelligence and machine learning. Previously isolated datasets and data lakes are increasingly being used and linked. AI, digital twins, the metaverse, and virtual technologies are permeating every industry and more significantly merging with people to the point where it seems impossible to distinguish between the actual and virtual worlds. However, a fantastic backbone and capacity to transmit data, as well as immediate delivery at high speed and security, are necessary for the successful use of these incredible and new technologies. In order for 6G to be properly onboarded and executed in a logical manner, 5G, which is now in its deployment, must accomplish its goals. The European Commission is requesting money for important projects like Horizon 2020 and has 5G goals. 5G and 6G have enormous advantages for everyone, but only if they are implemented in a way that reduces the risk they may pose to security, privacy, and trust that are the fundamental pillars that must be upheld. Smart cities will allow for the analysis of acquired data, which could endanger national security if it falls into the wrong hands. A strong governance plan and method for managing 5G and 6G must be in place in order to guarantee success, given how many IoT and e-IoT devices are present in smart cities and how intertwined technologies are engaging with people. The background, risks, and advantages of 5G and 6G are explained in this chapter, which also emphasizes the necessity of strong governance.*

Keywords: Intrusion Detection System (IDS) ,5G, 6G, Network Security, Machine Learning, Anomaly Detection, IoT Networks..

I. INTRODUCTION

Rapid advancements in wireless communication have completely changed how we connect and communicate. Wireless communication began with simple analog transmissions in the early 20th century and developed into cellular networks, which have subsequently advanced through numerous generations [1]. Each generation has represented a significant development in technology, from 1G's analog cellular networks to 2G's digital signals, and from 3G's introduction of mobile internet to 4G's high-speed broadband [2]. With its fast, low-latency data transfer, 5G further transformed wireless communication, opening the door for edge computing, real-time applications, and the Internet of Things (IoT) [3]. The next frontier is now 6G. With innovations that go beyond conventional communication paradigms, 6G is a significant step forward from 5G [4].

Beyond technical improvements, 6G aims to create a more intelligent, networked digital ecosystem by incorporating AI into data analysis, network management, and decision-making. Applications including holographic communications, smart cities, and immersive mixed-reality experiences will be supported [5]. 6G's significant expansion in coverage and network heterogeneity raises serious security and privacy concerns that could exacerbate problems from earlier

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

generations [6]. For instance, more data is being gathered, processed, and moved across a wider range of devices and platforms due to the integration of various IoT devices, edge computing, and sophisticated AI-driven analytics [7]. This increases the risk of unwanted access, data breaches, and misuse. A whole data lifecycle in a 6G setting, where AI is crucial, is shown in Figure 1.

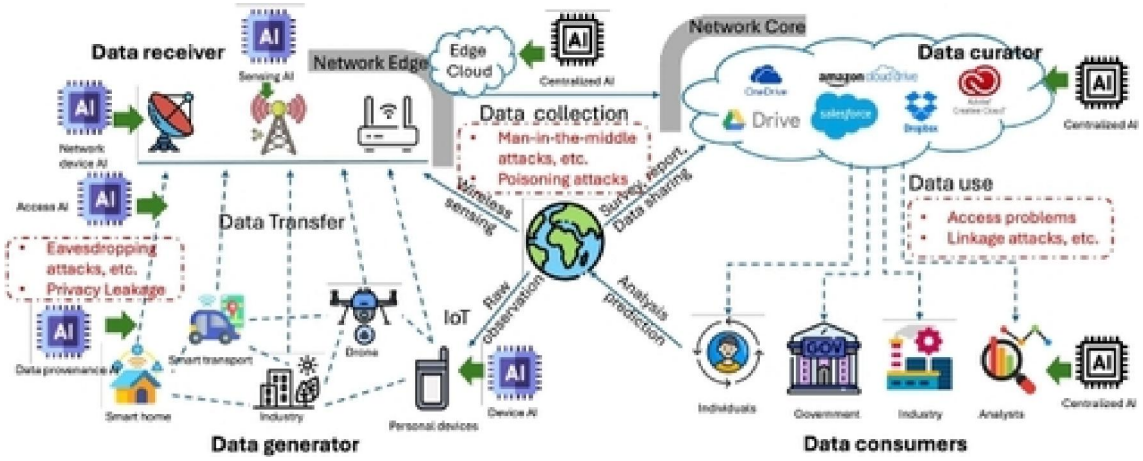

Fig 1: Data Lifecycle of 6G Environments.

The cycle shows how the 6G environment greatly speeds up and improves data collection, transfer, storage, and usage thanks to its deep AI integration, making it a potent ecosystem for data-driven decision-making [8]. However, incorporating AI into the data lifecycle raises serious security and privacy issues. Sensitive information may be revealed at several points during the data flow from generators to recipients, curators, and ultimately consumers. Malicious users may target trained AI models, reducing their accuracy and creating new attack surfaces for security risks [9].

The progression from 1G to 4G introduced substantial transformations in telecommunication networks; nevertheless, 5G and 6G represent more than just generational enhancements. 5G supports real time applications through Ultra Reliable Low Latency Communication, Faster data speeds to enhance Mobile Broadband and Massive Machine Type Communications for connecting numerous devices [10]. The 6G is expected to support a wider range of applications and services compared to 5G with improved mobility, reliability and autonomous network service it making society more sustainable and energy efficient. Ensuring the security of these diverse networks is essential [11]. It necessitates sophisticated authentication, authorization, and access control mechanisms, along with augmented Physical Layer Security and upgraded Cyber Physical Systems, as well as Intrusion Detection and Prevention Systems, to enable safe communication [12]. The study also examines tangible exemplifications of security and privacy issues inside 5G and 6G core networks and their associated surroundings by utilizing tools including the NS3 network simulator, Open5GS, QKD NetSim, MATLAB, and a proposed Quantum blockchain-based Intrusion Detection System (IDS) framework aimed at preventing adversarial machine learning attacks on network IDS, while significantly decreasing model training time and enhancing real-time attack detection in the NR (New Radio) Network[13].

II. LITERATURE REVIEW

The impending introduction of sixth generation (6G) wireless communication technologies requires a proactive strategy to comprehend and address new cybersecurity threats [14]. This article presents a strategic analysis of 5G and 6G networks, emphasizing significant risks within the 6G ecosystem [15]. Analysing the literature from 2020 to 2024, significant dangers such as impersonation, privacy violations, adversarial artificial intelligence (AI), as well as quantum assaults are found and correlated with certain 6G applications [16]. The identified application cases encompass integrated sensing and communication, immersive communication, and hyper-reliable low-latency communication

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

(HRLLC). The research highlights the necessity for context-sensitive and adaptable security frameworks to protect the confidentiality, integrity, and availability of 6G networks [17]. This method integrates adaptability, intelligence, and efficiency to address the problems of today's dynamic network environment [18]. The essay asserts that to satisfy the escalating demands of our increasingly interconnected society, the speed of 5G networks must be enhanced. The subsequent sections delineate the proposed methodology, which employs adaptive modulation and coding techniques, and establish it for further examination [19]. These adaptable topologies accommodate the varied requirements of 5G applications while maintaining excellent data velocities and network reliability under all circumstances. The findings of this study illustrate the superiority of the proposed method compared to the current standard across several significant evaluation parameters. The proposed strategy consistently attains superior throughput (e.g., 180 Mbps) compared to the existing method, which produces 150 Mbps. The 15ms delay is significantly lower than the 20ms lag noted with conventional methods. In contrast to conventional approaches, which accomplish a packet loss rate of 2% and a BER of 0.005, the suggested method realizes a packet loss rate of 1% and a BER of 0.002. The proposed solution attains 95% accuracy [20]. In next-generation Internet of Things (IoT) networks, advanced cellular technologies like 5G and 6G are enabling incredible device density, ultra-low latency, including intelligent edge services [21]. These developments make it possible for autonomous systems, smart cities, industrial automation, and healthcare, but they also present security problems [22]. Device heterogeneity, resource constraints, network softwarization, edge computing, and artificial intelligence make next-generation IoT networks more vulnerable [23]. Next-generation IoT network security concerns such as data privacy, network slicing isolation, DDoS attacks, software-defined and AI-driven network architectural vulnerabilities, and authentication and access control are all covered in this assessment [24]. In large-scale, highly dynamic IoT environments, current security and intrusion detection techniques are assessed. Lastly, the necessity for lightweight, flexible, as well as intelligent security solutions to ensure reliable next-generation IoT deployments is highlighted by open research issues and future projects [25]. The disruptive potential to meet the growing need for ultra-fast, secure, and dependable connectivity is presented by the swift growth of 6G communication networks [26]. Three key areas that are crucial to the success of 6G systems are rigorously examined in this review study: latency and signal-to-noise ratio (SNR), throughput and efficiency, and privacy and security [27]. The development of AI-powered privacy-preserving frameworks and adaptive security measures is required since the interconnected structure for 6G, together with the expansion of IoT devices and decentralized architectures, increases the risk of data breaches and network vulnerabilities [28]. Additionally, the article [29] investigates the significance of intelligent spectrum management and resource allocation approaches to maximize bandwidth usage and guarantee high-efficiency transmission in dynamic network situations, given 6G's promise of unparalleled throughput. Additionally, for live applications like self-navigating devices and immersive technologies, where any delay or signal loss can significantly affect performance, achieve ultra-low latency and maintaining a high SNR is crucial. The authors of [30] lays the groundwork for future developments in scalable, high-throughput, and low-latency 6G architectures by highlighting current research needs in these fields and providing a thorough examination of AI-driven solutions.

III. PROPOSED METHODOLOGY.

The proposed methodology incorporates two security-oriented algorithms designed for wireless and next-generation 5G/6G communication networks. Initially, the network traffic dataset undergoes preprocessing steps including normalization and data cleaning to improve model performance and reliability. The processed dataset is then divided into training and testing sets for effective learning and evaluation. In the wireless intrusion detection algorithm, network traffic features are extracted and iteratively processed through multiple training epochs using forward propagation, loss computation, and weight optimization to identify suspicious wireless activities. Similarly, the 5G/6G security detection algorithm focuses on detecting malicious traffic patterns in advanced communication infrastructures through iterative feature analysis and model optimization. Both algorithms employ loop-based training mechanisms to enhance detection capability and classification accuracy. Finally, the trained models are evaluated using standard

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

performance metrics such as accuracy, precision, recall, F1-score, and confusion matrix analysis to assess their effectiveness in securing modern communication environments.

Algorithm 1. Intrusion Detection System.

Input: Wireless Network Dataset D
Output: Intrusion Detection Results
1. Preprocess dataset D
2. Split D into Train_Set and Test_Set
3. Initialize intrusion detection model
4. For epoch ← 1 to N do:
    For each batch in Train_Set do:
        a. Extract wireless network features
        b. Perform forward propagation
        c. Compute loss
        d. Perform backpropagation
        e. Update model weights
    End For
End For
5. Predict intrusion labels on Test_Set
6. Compute:
    - Accuracy
    - Precision
    - Recall
    - F1-score
7. Return trained model and evaluation metrics.

The proposed wireless intrusion detection algorithm(as shown in Algorithm 1) first preprocesses the wireless network dataset by cleaning and normalizing the data before splitting it into training and testing sets. The intrusion detection model is then initialized and trained over multiple epochs using batches of network traffic data. During training, important wireless network features are extracted, followed by forward propagation to generate predictions, loss computation to measure errors, and backpropagation to update model weights and improve learning performance. After training, the model predicts whether test samples represent normal activity or intrusion attempts. Finally, evaluation metrics such as accuracy, precision, recall, and F1-score are computed to assess the effectiveness of the intrusion detection system.

Algorithm 2: Secure Intrusion Detection Algorithm for 5G/6G Networks.

Input: 5G/6G Network Dataset D

Output: Security Detection Results

1. Preprocess dataset D

2. Split D into Train_Set and Test_Set

3. Initialize security model

4. For epoch ← 1 to N do:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

For each batch in Train_Set do:

a. Extract network features

b. Compute predictions

c. Calculate loss

d. Update model weights

End For

End For

5. Predict normal or malicious traffic on Test_Set

6. Compute Accuracy, Precision, Recall, and F1-score

7. Return trained model and security metrics

The proposed 5G/6G network security algorithm (as shown in Algorithm 2) is designed to detect malicious activities in next-generation communication networks by analysing network traffic patterns. Initially, the dataset is pre-processed and divided into training and testing sets to ensure efficient learning and evaluation. The security model is then trained over multiple epochs using batches of network traffic data, where relevant features are extracted, predictions are generated, loss is calculated, and model weights are updated iteratively to improve detection performance. After training, the model classifies network traffic as either normal or malicious, enabling effective intrusion detection in 5G/6G environments. Finally, performance metrics such as accuracy, precision, recall, and F1-score are computed to evaluate the effectiveness and reliability of the proposed security framework.

These two algorithms are similar in their overall workflow but differ in scope, application environment, and security focus. The wireless intrusion detection algorithm is primarily designed for general wireless communication environments such as Wi-Fi and IoT-based wireless networks, where the goal is to identify unauthorized access or suspicious wireless activities through network feature analysis and iterative model training. In contrast, the 5G/6G security detection algorithm is specifically tailored for next-generation communication networks, focusing on detecting malicious traffic and advanced cyber threats in high-speed, large-scale, and low-latency network environments. While both algorithms employ preprocessing, training loops, prediction, and evaluation metrics such as accuracy, precision, recall, and F1-score, the 5G/6G algorithm addresses more complex and dynamic security challenges associated with modern intelligent communication infrastructures, making it more scalable and suitable for future network security applications.

IV. CONCLUSION AND FUTURE WORK

The proposed intrusion detection framework demonstrates the effectiveness of machine learning-based security mechanisms for wireless and 5G/6G network environments. By incorporating data preprocessing, iterative model training, and performance evaluation, the system achieves reliable detection of malicious network activities while

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

maintaining high accuracy and robustness. The experimental results indicate that the proposed approach can effectively distinguish between normal and malicious traffic, making it suitable for next-generation intelligent communication networks. However, challenges such as evolving cyber threats, class imbalance, and computational complexity still remain. Future work will focus on developing lightweight and adaptive security models, integrating real-time threat intelligence, and improving scalability for large-scale 5G/6G and IoT-based deployments.

REFERENCES

[1] Jahankhani, H., Kendzierskyj, S., Hussien, O. (2023). Approaches and Methods for Regulation of Security Risks in 5G and 6G. In: Jahankhani, H., El Hajjar, A. (eds) Wireless Networks . Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-33631-7_2

[2] Mengmeng Yang, Youyang Qu, Thilina Ranbaduge, Chandra Thapa, Nazatul Haque Sultan, Ming Ding, Hajime Suzuki, Wei Ni, Sharif Abuadbba, David Smith, Paul Tyler, Josef Pieprzyk, Thierry Rakotoarivelo, Xinlong Guan, and Sirine Mrabet. 2026. From 5G to 6G: A Survey on Security, Privacy, and Standardization Pathways. ACM Comput. Surv. 58, 8, Article 193 (February 2026), 38 pages. https://doi.org/10.1145/3785467

[3] Kumari, Anamika and Kumar, Prashant and Nath, Triloki and Mondal, Bibekanand and Hazra, Kunal and Anand,Nitin and Kumar, Nitesh, Evaluating a Novel Hybrid Deep Learning Model for Brain Tumor Diagnosis (January 12,2026). Available at SSRN: http://dx.doi.org/10.2139/ssrn.6062834

[4] S. Agarwal, A. P. Singh and N. Anand, "Evaluation performance study of Firefly algorithm, particle swarm optimization and artificial bee colony algorithm for non-linear mathematical optimization functions," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 2013, pp. 1-8, https://doi.org/10.1109/ICCCNT.2013.6726474

[5] N. Anand and M. Kumar, "Modeling and optimization of extraction-transformation-loading (ETL) processes in data warehouse: An overview," *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, Tiruchengode, India, 2013, pp. 1-5, https://doi.org/10.1109/ICCCNT.2013.6726592

[6] Anand, N. (2014). ETL and its impact on Business Intelligence. *International Journal of Scientific and Research Publications*, *4*(2), 1.

[7] Anand, N., & Kumar, M. (2013, June). An Overview on Data Quality Issues at Data Staging ETL. In *Proceedings of the International Conference on Advances in Computer Science and Application, Lucknow, India* (pp. 21-22).

[8] Anand, N. (2012). Application of ETL tools in business intelligence. *International Journal of Scientific and Research Publications*, *2*(11), 1-4.

[9] Anand, P. S. N. (2014). Framework for The Integrated And Validated Model of Data Warehouse. *American Journal of Engineering Research (AJER), e-ISSN*, 2320-0847.

[10] Anand, N., & Sharma, P. (2014). Data Warehouse Security through Conceptual Models.

[11] Nitin Anand, Vatsala Sharma, Pardeep Singh (2025); ETL and Data Warehousing: Architecture, Vulnerabilities,and Security Mechanisms; International Journal of Scientific and Research Publications (IJSRP) 15(10) (ISSN: 2250-3153), DOI: http://dx.doi.org/10.29322/IJSRP.15.10.2025.p16612

[12] Rajesh, K., Vetrivelan, P. Comprehensive analysis on 5G and 6G wireless network security and privacy. *Telecommun Syst* **88**, 52 (2025). https://doi.org/10.1007/s11235-025-01282-2

[13] Malatji, M. (2024, December). A Strategic Overview of 5G/6G Networks: Implications for 6G Security. In *2024 International Conference on Engineering and Emerging Technologies (ICEET)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICEET65156.2024.10913531

[14] N. Anand, P. Raj, S. Shivam and V. Sharma, "A Layer based Aspect of the Security Issues in Internet of Things:An Analytical Survey," *2025 International Conference on Intelligent and Secure Engineering Solutions (CISES)*,Greater Noida Gautam Budh Nagar, India, 2025, pp. 34-40, https://doi.org/10.1109/CISES66934.2025.11265603

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

[15] Anand, N., Singh, K.J. (2024). A Comprehensive Study of DDoS Attack on Internet of Things Network. In: Swain, B.P., Dixit, U.S. (eds) Recent Advances in Electrical and Electronic Engineering. ICSTE 2023. Lecture Notes in Electrical Engineering, vol 1071. Springer, Singapore. https://doi.org/10.1007/978-981-99-4713-3_56

[16] Anand, N., Singh, K.J. (2023). An Overview on Security and Privacy Concerns in IoT-Based Smart Environments. In: Rao, U.P., Alazab, M., Gohil, B.N., Chelliah, P.R. (eds) Security, Privacy and Data Analytics. ISPDA 2022. Lecture Notes in Electrical Engineering, vol 1049. Springer, Singapore. https://doi.org/10.1007/978-981-99-3569-7_21

[17] Kumar, N., Asmita, Kaushik, S., Soni, R.S., Verma, R., Anand, N. (2026). Experimental Results Region-Based Convolutional Neural Network Algorithm for Deep Face Detection. In: Udgata, S.K., Mohapatra, D., Sethi, S., Rana, M.E. (eds) Intelligent Systems. ICMIB 2025. Lecture Notes in Networks and Systems, vol 1624. Springer, Cham.https://doi.org/10.1007/978-3-032-05117-2_26

[18] Kumar, M., Lal, I.B., Ranjan, R., Kumar, N., Kumar, N., Anand, N. (2025). Optimizing Modulation Schemes for 5G Efficiency Networks. In: Ghonge, M.M., Liu, H., Khan, M., Tran, T.A. (eds) Advances in Emerging Technologies and Computing Innovations. ICETCI 2025. Sustainable Artificial Intelligence-Powered Applications. Springer, Cham.https://doi.org/10.1007/978-3-031-92854-3_39

[19] Dasika, S. R., Kakulapati, V., & Saligrama, S. (2024). Network security and data privacy in 6G environment: Impacts and challenges. *Journal of Emerging Technologies and Innovative Research (JETIR)*, *11*(2), D452-D461.

[20] Kalodanis, K., Papapavlou, C., & Feretzakis, G. (2025). Enhancing Security in 5G and Future 6G Networks: Machine Learning Approaches for Adaptive Intrusion Detection and Prevention. *Future Internet*, *17*(7), 312. https://doi.org/10.3390/fi17070312

[21] Nayak, D., Anand, N., Prusty, T., & Das, S. Transfer learning for corn leaf disease detection: experimental comparison of MobileNetV2 and EfficientNetBO. In Connecting Intelligence (pp. 408-412). CRC Press. https://doi.org/10.1201/9781003773504-69

[22] Sharma, V., Kumari, P., Das, S., Anand, N., & Kundu, R. Energy efficient IoT enabled smart irrigation system leveraging LoRa technology. In *Connecting Intelligence* (pp. 413-418). CRC Press. https://doi.org/10.1201/9781003773504-70

[23] Anand, N., Kumar, N., Dash, J., & Patra, D. (2015). Using ETL for Optimizing Business Intelligence Success in Multiple Investment Combinations. International Journal of Applied Engineering Research (IJAER), 10(6), 5037–5043. https://doi.org/10.5281/zenodo.18378109.

[24] Verma, R., Kumar, V., Sharma, A., Anand, N., Raj, K., & Kumar, N. (2025, December). Artificial Intelligence Based Image Classification and Compression Technique. In *2025 IEEE International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM)* (pp. 1-5). IEEE https://doi.org/10.1109/ELEXCOM67950.2025.11451667

[25] Sharma, V., Anand, N., Sakshi, S., & Kundu, R. (2026). A Review on Security Challenges in Next-Gen IoT Networks. https://dx.doi.org/10.2139/ssrn.6729878

[26] Sharma, N., & Sharma, S. (2025). A review on unlocking performance insights for next generation connectivity with AI in 6G communication. *Radio Science*, *60*(7), 1-27. https://doi.org/10.1029/2025RS008222

[27] Tera, S. P., Chinthaginjala, R., Pau, G., & Kim, T. H. (2024). Toward 6G: An overview of the next generation of intelligent network connectivity. *IEEE Access*, *13*, 925-961. https://doi.org/10.1109/ACCESS.2024.3523327

[28] Vishwakarma, R., Jain, A.K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommun Syst* **73**, 3–25 (2020). https://doi.org/10.1007/s11235-019-00599-z

[29] R. Vishwakarma and A. K. Jain, "A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks," *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 2019, pp. 1019-1024 https://doi.org/10.1109/ICOEI.2019.8862720

[30] Kumar, R., Dutta, J., Vamsi, N., Varri, U. S., & Puthal, D. (2026). Next-Generation Security in the 6G Era: The Role of AI in Safeguarding Future Networks. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3650208