Towards Sustainable 5G Networks: Addressing Security, Environmental, and Deployment Challenges

Mohsin Mubeen Abbasi[1], Syed Muhammad Daniyal[1*], Sarmad Saud[2], Noman Bin Zahid[1], Muhammad Kashif[3], Hayyan Qasim[1]

[1]Faculty of Engineering Science and Technology, Iqra University, Karachi, Pakistan
mohsin.abbasi@iqra.edu.pk, syed.daniyal@iqra.edu.pk, noman.zahid@iqra.edu.pk, hayyan.58806@iqra.edu.pk

[2]Director, Global Technical Services & Support, USA
saud@rapidai.com

[3]Faculty of Engineering Science and Technology, Indus University, Karachi, Pakistan
m.kashif@indus.edu.pk

Corresponding Author: syed.daniyal@iqra.edu.pk

Abstract: The development from first-generation (1G) to fifth generation (5G) mobile networks has paved the way for improved connectivity, bandwidth, and latency. But the deployments of 5G have also posed many security concerns, architectural obstacles, and environmental sustainability issues. The current body of literature focuses on performance optimization or individual security solutions. Still, there is a need for a critical study of the lack of models that can simultaneously tackle the security, sustainability, and deployment challenges. This paper examines the most important potential threat vectors in the 5G environment, such as Software-Defined Networking (SDN) vulnerabilities and Network Function Virtualization (NFV) vulnerabilities, mobile cloud threats, multi-domain trust issues, IoT-based attack surfaces, and the environmental impact of large-scale infrastructure. We would like to propose a holistic solution to mitigate attacks based on SDN, NFV, Machine Learning (ML)-based intrusion detection, Mobile Cloud Computing (MCC), and blockchain-based decentralized trust management. A conceptual evaluation model is created to make comparisons between these approaches with respect to four dimensions – security effectiveness, scalability, latency sensitivity, and energy efficiency. The main features of the present invention are: (1) providing a systematic analytical comparison of the emerging 5G security mechanisms; (2) matching security objectives with the sustainable networking goals; and (3) a conceptual evaluation framework to validate multi-layered 5G protection strategies. Results show that the orchestration of intelligence in the deployment of secure and eco-friendly 5G networks hinges on the ability to manage trust in a decentralized manner, design energy-efficient networks, and integrate privacy-preserving distributed intelligence, including federated learning.

Keywords: Sustainable 5G, Machine Learning Security, Environmental Sustainability, Software-Defined Networking (SDN), NFV, Blockchain.

I. INTRODUCTION

Fifth generation (5G) communication systems are a paradigm shift in telecommunications, which is a radical change from the old mobile networks. The 3 main areas of the 5G are ultra-reliable low-latency communication (URLLC), enhanced mobile broadband (eMBB), and massive machine-type communication (mMTC), all of which will be instrumental to critical applications in smart cities, autonomous transportation, industrial Internet of Things, and healthcare [1]. All of this is transformative, but the architecture of 5G will pose challenges for virtualization, cloud-native deployment, network slicing, and distributed control.

The basic elements of 5G are different from its predecessors, and it is based on Software-Defined Networking (SDN), Network Function Virtualization (NFV), Mobile Cloud Computing (MCC), and edge computing [2]. These technologies provide greater scalability and resource optimization but also add to the attack surface. Distributed denial-of-service (DDoS) attacks, virtualization exploits, signaling storms, and cross-domain trust violations are emerging types of threats that are harder to protect against using perimeter-based security defenses.

Another challenge with a parallel interest is environmental sustainability. The increase in base stations, small cells, and edge nodes significantly increases energy use and CO2 emissions. Also, tons of electronic waste and habitat destruction with huge infrastructure. Energy-efficient orchestration and infrastructure planning that takes a more environmentally conscious approach is key to the sustainable implementation of 5G [3].

A. Research Gap

The existing literature mainly focuses on SDN, NFV, MCC, IoT security, and on detection based on ML techniques independently, without considering the interaction among them in multi-domain 5G environments. Decentralized trust mechanisms and privacy-preserving techniques, such as blockchain and federated learning, are very little talked about with environmental sustainability objectives. The fragmentation of the 5G comes with a major research gap: how to build a comprehensive, secure, and sustainable 5G architectural model that covers technological, environmental, and operational aspects.

B. Contributions

This paper contributes to filling this gap by introducing the following:

(1) A clear and comprehensive examination of the threats to 5G from SDN/NFV vulnerabilities, mobile cloud security, multi-domain trust threats, IoT-based threats, and environmental deployment impacts.

(2) Comparing and Contrasting SDN, NFV, MCC, and ML-based Security Mechanisms, highlighting the trade-off of Security, Scalability, Latency, and Energy consumption.

(3) An integrated security and sustainability solution that integrates ML-driven threat detection, blockchain-based decentralized trust management, and energy-saving edge-cloud orchestration.

(4) conceptual evaluation model for the effectiveness, scalability, latency effects, and energy efficiency of the proposed framework.

(5) Recognition of existing constraints and research avenues to build smart, sustainable, and 6G network ecosystems.

The challenges and threat models in 5G networks are presented in Section II. The rest of this paper is organized as follows: Section II presents challenges and threat models in 5G networks. A comparative analysis of enabling technologies is given in Section III. A discussion of mitigation solutions is included in Section IV. In 5G security, blockchain and federated learning are explored in Section V. The limitations and future directions are presented in Section VI.

II. CHALLENGES IN 5G NETWORKS

A. SD-WAN and NFV Vulnerabilities

While Software-Defined Networking (SDN) focuses on control and permits dynamic programmability, the centralized controller architecture makes the centralized controller a high-value attack target [4]. An SDN controller that has been compromised has the potential to disrupt an entire network slice, alter flow rules, and make the network unusable. Some of the biggest risks are denial-of-service attacks on the controller and exploitation of the application programming interfaces (APIs). NFV also eliminates the need for dedicated hardware, but the lack of isolation between virtual machines may lead to configuration flaws and cross-tenant security issues [5]. Hypervisor integrity and access-control policies are critical to the security of an NFV environment. Additionally, SD-WAN deployments add bandwidth constraints, latency variations, man-in-the-middle threats, and interoperability issues on the way to the data [3].

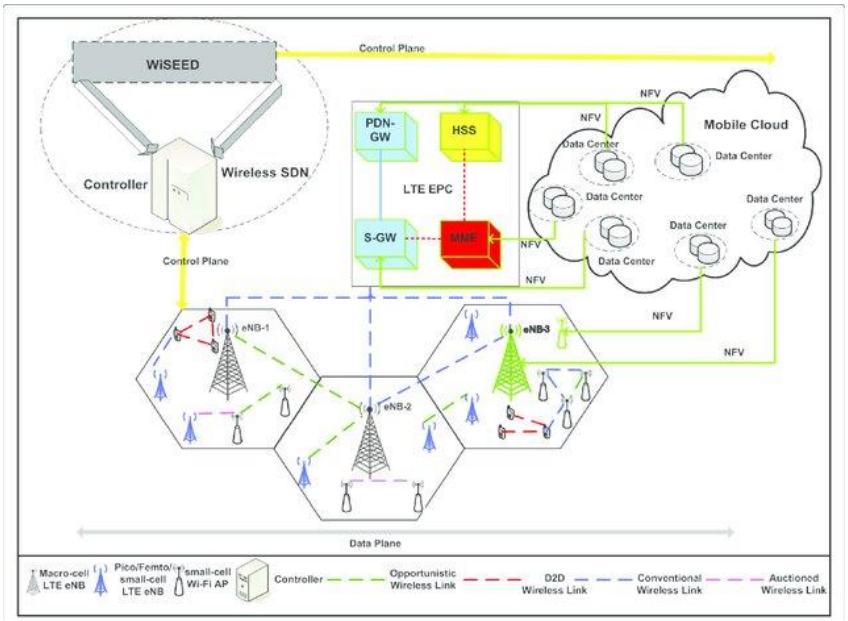

Figure 1. SDN-enabled LTE and Cloud Integration via NFV

B. Mobile Cloud Computing Threats

Mobile Cloud Computing (MCC) is an approach that would allow for storing and processing the applications of the 5G network in a scalable way; however, it presents several security challenges [6]. Multi-tenant cloud systems introduce the possibility of resource contention and data leakage between users. The adversary can attack data centers through the mobile network, targeting Radio Access Technology (RAT), while Cloud Radio Access Networks (C-RAN) can, in part, counter such attacks, but they can still suffer single points of failure scenarios. Bad traffic injections can also affect the overall network throughput and performance. As the mobile and cloud paradigms converge, they demand strong service-level security controls, virtualization-based isolation, and robust encryption.

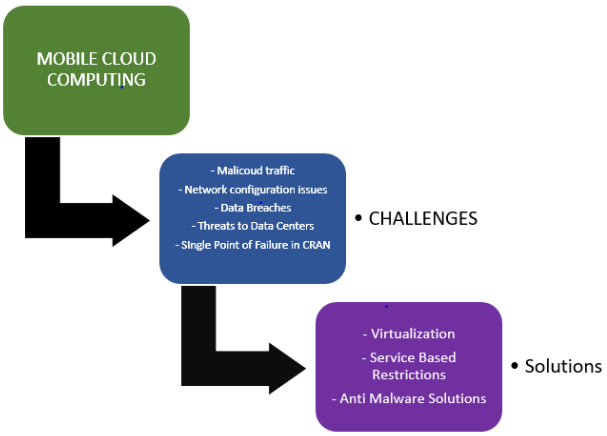

Figure 2 Mobile cloud Computing

Figure 2. Mobile Cloud Computing Challenges and Solutions

C. Multi-Domain Trust Challenges

Novel trust threats arise in modern 5G multi-domain environments, which are enabled by SDN/NFV capabilities, cloud RAN, and distributed control, that go beyond traditional networking paradigms [7]. The two types of trust risks are important: multi-tenant trust relationships, where both parties have their own interests, and distributed environment security risks that are related to the security of the network and its distributed components, owned by various entities [8]. The threats are magnified in 5G, as different network elements are controlled by different decentralized actors, leaving no centralized control and allowing malicious actors to take advantage of that. The threats to trust relate to unauthorized access to resources, identity spoofing in different administrative domains, and policy inconsistencies between network operators.

D. Network Channel and Privacy Challenges

5G networks use common SDN interfaces instead of generation-specific protocols, reducing the effort required by possible attackers [9]. Persistent interference is caused by the coexistence of multiple network technologies operating at overlapping frequencies. Moreover, the mobility of nodes makes inter-network collaboration difficult, especially when moving between networks. There are some efforts to solve these problems with interference management strategies using ML [10].

Threats to user privacy include Semantic information attacks, timing attacks, and boundary attacks to location privacy. IMSI-catching attacks using rogue base stations are a key concern for 5G deployments [11]. Unlike previous generations, 5G operators aren't in total control of infrastructure components and rely on Communication Service Providers (CSPs). This shared governance model poses challenges to the synchronization of privacy policies between Virtual MNOs, CSPs, and network infrastructure providers. 5G's cloud-based data storage and NFV capabilities take away physical data limits and additionally reduce the operator's control over data residence.

E. IoT-Based Challenges

In a secure environment, evaluating 5G in secured configurations is essential when deployed with IoT to safeguard the confidentiality, integrity, and availability (CIA triad) of the transmitted data [12]. Validation of digital signatures, end-to-end encryption, and authentication are critical. Several IoT devices have limited memory and processing power, and shifting these tasks to fog/edge layers by security-as-a-service mechanisms is a potential mitigation measure [13]. Besides, the volume of data produced in 5G-IoT systems is huge, which poses scalability challenges to intrusion detection systems and traffic anomaly analysis systems.

F. Environmental and Ecosystem Challenges

The large-scale deployment of 5G infrastructure base stations, small cells, and transmission towers incurs high environmental costs, including deforestation, land use changes, and electromagnetic interference with wildlife habitats [14]. High-frequency transmissions in the 3 GHz to 300 GHz range are estimated to contribute to bird mortality, with annual figures reported in the range of 250 to 500 million globally [16]. International bodies, including the UN and WWF, have begun raising awareness and establishing compliance frameworks. Energy consumption is further exacerbated by the low-power device category requirements of 5G NR

(e.g., Cat-M1), which must balance ultra-high speed with power efficiency constraints. With 5G expected to surpass one billion users and connected device counts projected to exceed 50 billion, energy-conscious network design is a fundamental sustainability imperative [15].

III. COMPARATIVE ANALYSIS OF 5G SECURITY MECHANISMS

In this section, a cross-comparative evaluation of the 5G security-enabling technologies (SDN, NFV, Mobile Cloud Computing, and threat detection based on ML) is presented. Technology is assessed in a variety of dimensions: security benefit, primary limitation, energy impact, and scalability. This summary is captured in Table 1, which outlines the comparison of the different technologies, including those discussed in Section V on blockchain and federated learning.

A. SDN-Based Security

Centralized traffic monitoring and fast policy enforcement are made possible by SDN. It is a single pane of glass visible, making it easier to detect volumetric and policy violation attacks. The central controller is a single point that is easy to compromise, though. If a controller is successfully attacked, then entire network slices can be disrupted. High controller redundancy, hardening of authentication data, and anomaly-based controller monitoring are therefore required for SDN-based security.

B. NFV-Based Virtualization Security

With NFV, there is no need for any proprietary hardware, and deployed agility is increased. But if isolation of the VMs is not sufficient, cross-tenant data leakage attacks and lateral movement attacks can be made possible. Hypervisor integrity and access control are key factors in NFV environments to ensure security. SDN's distributed approach to function deployment is its comparative advantage, mitigating, not eradicating, single points of failure.

C. Mobile Cloud Computing (MCC) Security

While MCC provides scalable compute and storage offloading, it also opens data up to remote access vulnerabilities and multi-tenant exploitation. Virtualization-based isolation offers better tenant separation, but it's not a complete solution against insider threats or lateral movement in shared environments. MCC has the greatest scalability compared to the other technologies but requires more energy costs and privacy exposure than SDN and NFV.

D. ML-Based Threat Detection

Using machine learning for traffic behavioral analysis is more effective than using rules in detecting zero-day attacks. But these ML models are power hungry, need huge representative training sets of data, and are vulnerable to adversarial input tampering. While SDN or NFV provides scalable detection, ML-based IDS provides adaptive detection at moderate scalability, with moderate overhead in terms of energy consumption during operation, and the need for powerful data pipelines.

Table 1: Overview of Threat Models in 5G enabling technologies.

Technology	Security Threat	Limitation	Energy Impact	Scalability
SDN [17]	Centralized monitoring	Controller attack risk	Moderate	High
NFV [18]	Flexible deployment	VM isolation risk	Moderate	High
MCC [19]	Cloud scalability	Privacy concerns	High	Very High
ML-based IDS [20]	Adaptive detection	Data-intensive; adversarial vulnerability	High	Moderate
Blockchain	Decentralized trust	Throughput & latency overhead	High	Moderate
Federated Learning	Privacy-preserving AI	Communication cost	Moderate	High

IV. INTEGRATED SECURITY SOLUTIONS FOR 5G

A. Securing SDN and NFV Deployments

The vulnerabilities that are identified in SDN and NFV are attempted to be solved by exploiting the complementary capabilities of both technologies. The southbound APIs of SDN allows for real-time reallocation of resources and monitoring of traffic, while NFV provides a basis for dynamically deploying cloud-native security functions closer to the edge of the network [20]. User-plane integrity is provided by end-to-end encryption. Centralized policy enforcement with SDN gives global traffic visibility, and C-RAN and edge computing decrease signaling overheads of high-density UE environments [21]. Virtual network slices can be provisioned in a selective manner to handle flash traffic in the overloaded areas. For secure radio interface key management, use of cryptographic key exchange protocols like Host Identity Protocol (HIP)-based

Protocols must be implemented.

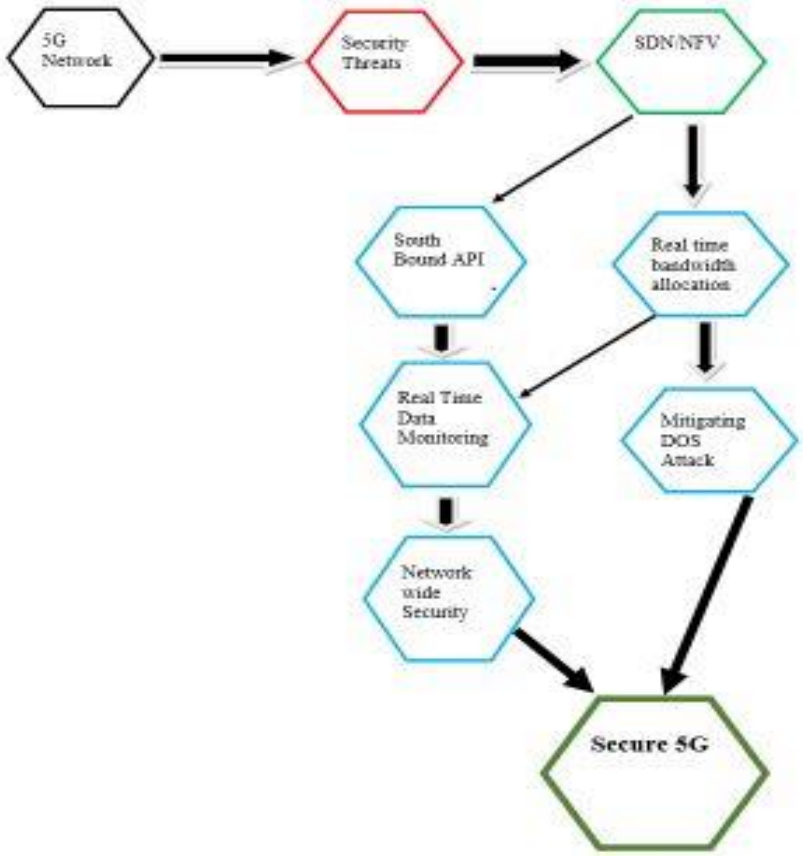

Figure 3. Solution using SDN & NFV for Secure 5G

B. Secure Mobile Cloud Computing

Virtualization-based isolation, tweaked encryption methods, and smart load balancing are key areas of focus for security solutions in MCC environments. Virtual Machine (VM) based isolation allows for separation between users on shared cloud resources. Service-based access controls should apply “least privilege” with cloud-connected endpoints. Systems that have been trained on known patterns and attacks, and especially attack classes for the HX-DOS, are more effective in detecting attacks than generic rule-based systems. Cloud-based or on-premises client-side anti-malware solutions add to endpoint security. The MCC security framework should include energy-efficient data integrity mechanisms for storing, lightweight compromise-resistant outsourcing mechanisms, and public provable data possession schemes [22].

C. ML-Based Threat Detection Framework

Compared to static signature-based intrusion detection, ML-based intrusion detection is a major step forward. The system can be trained with a set of curated threat data to detect anomalous deviations from normal network activity by matching network behavior with known digital signatures [23]. For 5G environments that produce huge packet volumes, it is crucial to maintain detection accuracy throughout dataset curation and model refresh cycles. Secure traffic baselines should be created using encrypted traffic protocols such as HTTPS, SSH, and SFTP on mobile clients, further augmenting training datasets [24].

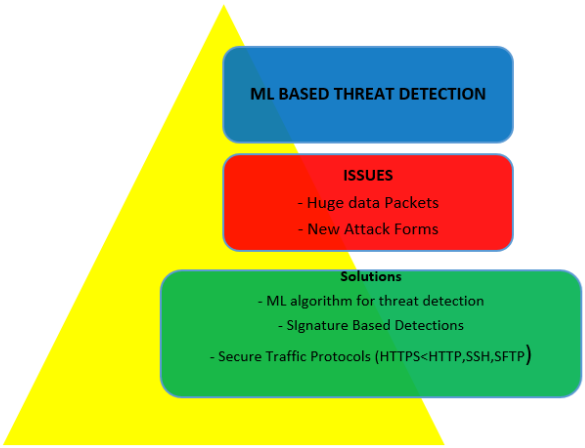

Figure 3 ML Based Threat Detection

Figure 4. ML Based Threat Detection

D. Privacy Mitigation Framework

Three-level coordination is a key factor in ensuring privacy protection in 5G. Government agencies, with the support of international organizations like the UN or the EU, are responsible for implementing data privacy laws [25]. Industry entities such as standards bodies like 3GPP, ETSI, and ONF create and publish best-practice privacy principles [26]. From the user's perspective, the concepts of privacy by design and transparency frameworks guarantee that users' expectations are translated into network architectures [27].

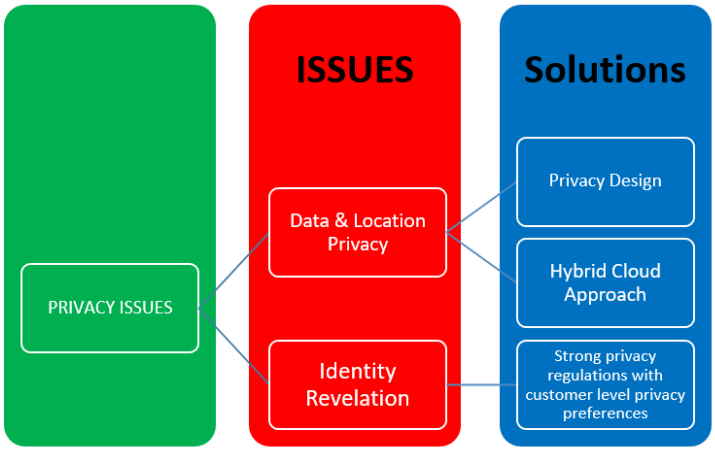

Figure 4 Mitigating Privacy Issues

Figure 5. Mitigating Privacy Issues

V. BLOCKCHAIN AND FEDERATED LEARNING FOR 5G SECURITY

By making it possible to achieve decentralized authentication, tamper-evident audit logging, and transaction validation without depending on a central authority, blockchain technology enhances trust management in multi-domain 5G environments. Smart contracts can be used for enforcing network slicing policies and for securing the allocation of the resources to the tenant(s). This decentralized architecture directly addresses threats to multi-domain trust outlined in Section II.C.

Although blockchain is a key element in decentralizing data management, Federated Learning (FL) complements it by enabling the process of model training without sharing individual users' raw data with the central servers, while preserving privacy and promoting the growth of shared intelligence. The training of intrusion detection models in FL is performed collectively by the edge devices while avoiding sensitive information leakage in 5G-IoT deployments. AI can be used in conjunction with blockchain and FL to support decentralized coordination of security, as well as ensuring the integrity of the models and data. Together, the combination will provide a strong and resilient solution that will help to minimize single points of failure, privacy disclosure and distributed intelligence edge of the 5G network.

Recent studies have shown that post-quantum cryptographic solutions can have an additional layer of security for 5G infrastructure based on blockchain against threats of future generations [28, 29]. It is noted that with the evolution of such ideas, there is a potential path for security evolution for 5G to 6G, the quantum-resistant cryptography and blockchain-federated architectures.

VI. CONCLUSION

This paper covered a complete analytical review of security, deployment, and environment challenges in 5G networks. This study builds on the work done piecemeal in previous studies and combines all of the above components into a coherent unit of security and sustainability. By comparing the security benefits that each technology provides to the others, no single technology can provide all the security benefits on its own – the ultimate security benefits can only be achieved through coordinated orchestration strategies. The proposed framework is designed to tackle three closely coupled aims: Adaptive threat detection using ML-based IDS, decentralized trust management through blockchain, and energy-conscious deployment through edge-cloud orchestration. The conceptual evaluation model developed in this study can serve as a foundation for conducting empirical studies. There are some limitations in the present study. First, the comparison is not validated by real-world experiments, which hampers generalizability. Secondly, ML detection systems have computational requirements that can cause scalability issues when traffic is heavy. Thirdly, blockchain integration imposes latency and throughput overheads, which need to be measured on the deployed system. The following are proposed for future research: (1) prototype implementation and quantitative benchmarking of the proposed framework, (2) integration with 6G architectural standards, (3) development of energy-efficient AI security models that offer detection accuracy along with being energy-efficient, (4) empirical evaluation of federated learning convergence in a heterogeneous IoT-5G environment, and (5) investigation of quantum-resistent cryptographic integration in decentralized trust management systems. Intelligent automation, environmental responsibility, and open multi-stakeholder governance are essential design principles to ensure secure and sustainable 5G evolution.

REFERENCES

[1] Khan, N. A. (2022). 5G Network: Techniques to Increase Quality of Service and Quality of Experience. Int. J. Comput. Netw. Appl., 9, 476-496.

[2] Imam-Fulani, Y. O., et al. (2023). 5G frequency standardization, technologies, channel models, and network deployment. Sustainability, 15(6), 5173.

[3] Alimi, I. (2025). 5G Fixed Wireless Access: Revolutionizing Connectivity in the Digital Age. Springer Nature.

[4] Ahsan, M., et al. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning. Journal of Cybersecurity and Privacy, 2(3), 527-555.

[5] Bertsekas, D., & Gallager, R. (2021). Data networks. Athena Scientific.

[6] Dangi, R., et al. (2021). Study and investigation on 5G technology: A systematic review. Sensors, 22(1), 26.

[7] Attaran, M. (2023). The impact of 5G on the evolution of intelligent automation and industry digitization. J. Ambient Intell. Humanized Comput., 14(5), 5977-5993.

[8] Ahmed, S. F., et al. (2024). Toward a secure 5G-enabled internet of things: A survey. IEEE Access, 12, 13125-13145.

[9] Kandhro, I. A., et al. (2025). Network security attack classification: leveraging machine learning methods. Int. J. Electronic Security and Digital Forensics, 17(1-2), 138-148.

[10] Ahmad, I. A. I., et al. (2024). Emerging 5G technology: A review of its far-reaching implications. World Journal of Advanced Research and Reviews, 21(1), 2474-2486.

[11] Siddique, W. A., et al. (2024). Big data analytics for 6G-enabled massive Internet of Things. In Low-Power Wide Area Network for Large Scale IoT, pp. 177-202. CRC Press.

[12] Tyokighir, S. S., et al. (2024). New developments and trends in 5G technologies. Bulletin of Electrical Engineering and Informatics, 13(1), 254-263.

[13] Sangeetha, S., et al. (2024). Smart performance optimization of energy-aware scheduling model for 5G green communication systems. The Journal of Engineering, 2024(2).

[14] Ahmad, I. A. I., et al. (2024). 5G deployment strategies: Challenges and opportunities. World Journal of Advanced Research and Reviews, 21(1), 2428-2439.

[15] Jatoi, F., Masood, A., & Daniyal, S. M. (2025). A novel call routing optimization in an in-direct sales environment.

[16] Lin, X. (2025). The bridge toward 6G: 5G-Advanced evolution in 3GPP Release 19. IEEE Communications Standards Magazine, 9(1), 28-35.

[17] Yousuf, W. B., et al. (2024). Novel Prognostic Methods for System Degradation Using LSTM. IEEE Access.

[18] Yang, M., et al. (2024). From 5G to 6G: A survey on security, privacy, and standardization pathways. arXiv:2410.21986.

[19] Munteanu, C., et al. (2025). Catch-22: Uncovering Compromised Hosts using SSH Public Keys. 34th USENIX Security Symposium.

[20] Noor, K., et al. (2025). A review of machine learning and transfer learning strategies for intrusion detection in 5G. Mathematics, 13(7), 1088.

[21] De Soete, M. (2025). SSH. In Encyclopedia of Cryptography, Security and Privacy, pp. 2517-2517. Springer, Cham.

[22] Prasad, P., Mohammad, T., & Sainio, P. (2024). Enhancing Security in SDN-based IP Multicast Systems.

[23] Samson, A. (2024). Assessing SDN-based Access Control System Effectiveness.

[24] Shakil, M. H., et al. (2025). Exploring Innovations and Security Enhancements in Android Operating System. Spectrum of Engineering Sciences, 3(2), 472-495.
[25] Ali, W. J., et al. (2024). Auctisafe: Building a robust and reliable auction system. IEEE KHI-HTC, pp. 1-6.
[26] Faheem, M. Y., et al. (2019). Ultra-low power small size RF Transceiver module for 5G/LTE applications. ICEEST, pp. 1-6.
[27] Moiz, S., et al. (2024). Unveiling the arsenal of user data protection tools and practices. IEEE KHI-HTC, pp. 1-7.

Submitted: 19th Oct 2025; Accepted: 1st July 2026;