AI in 5G Networks: A Review of Implementation, Security and Privacy Challenges

Sona D Solanki[1], Dr. Prem Pal Singh[2], Dr. Kalpesh R Jadav[3], Asha D Solanki[4]
[1&2]*Assistant Professor, Electronics and Communication Engineering, Parul Institute of Engineering and Technology, India*
[3]*HoD and Associate Professor, Electronics and Communication Engineering, Parul Institute of Engineering and Technology, India*
[4]*Editor, Editorial, Crime File, India*
E-mail: [1]sona.solanki41348@paruluniversity.ac.in , [2]prempal.singh38023@paruluniversity.ac.in,
[3]kalpesh.jadav@paruluniversity.ac.in, [4]solankiasha2710@gmail.com

Abstract - Fifth-generation (5G) frameworks are now at the leading edge of the worldwide digitization due to the quick development of wireless technology for communication. Automated places, automated factories, driverless cars, distant medical services, and engaging activities like virtual and augmented reality are merely some of the broad purposes made possible by 5G's possibilities, which include ultra-reliable low-latency communication (URLLC), enhanced mobile broadband (eMBB), and massive machine-type communication (mMTC). Nevertheless, 5G communications unparalleled size, intricacy, and rapid evolution provide serious problems for safety, flexibility, conservation of energy, and productivity improvement. AI improves anomaly identification, invasion mitigation, and continuous surveillance of possible breaches. AI networks provide novel safety vulnerabilities due to their susceptibility to inductive breaches, data compromise, and adversary management. With an emphasis on its use across infrastructure construction, operation efficiency, and privacy, this study offers a thorough examination of the incorporation of AI with 5G networking. It primarily explores the use of Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL) approaches to enhance traffic identification, simplify system division, enhance the utilization of resources, and facilitate autonomous systems. High Quality of Service (QoS) may be maintained regardless of crowded, adequate-demand settings by employing AI-driven solutions that enable providers to proactively predict and react to changing circumstances affecting the network. It promotes longevity by facilitating adaptive distribution of loads among the network elements and reducing utilization of energy. The abstract also emphasizes AI's hybrid safety function.

Keywords: **5G Networks, AI, Security**

I. INTRODUCTION

With its minimal latency, record-breaking transfer rates as well as ability to link an unparalleled quantity of items, the 5G cellular technology is poised to revolutionize worldwide connection. In contrast to its previous versions it is made to accommodate a wide range of functions that have radically distinct efficiency features. These include mMTC for the IOT, URLLC for vital services including surgical treatment and automated travel as well as extremely fast eMBB for customers. 5G is far more than speedier connectivity; it provides the foundation for the technological advancement in several interconnected sectors, including production, leisure, medical services, and commuting. The requirement for wireless connectivity has increased dramatically because of the vast rise in networked that are linked. Administering enormous volumes of information in constantly reducing connection traffic while maintaining robust safety standards, and proactively allocating resources are some of the new issues brought about by this phenomenal expansion. Such infrastructures need to be extremely adaptable, expandable, resilient, and versatile to address these difficulties. Automated platforms that can make decisions in immediate circumstances are the most effective method to accomplish these goals.

AI is positioned to be a key player in tackling these issues especially by using its subsections of ML and DL. To be capable to handle the complexity of 5G systems, AI must be able to analyze vast volumes of information and create wise judgments despite the assistance of humans. By allowing these systems to form themselves it anticipates traffic trends along with spontaneously respond to changing networking situations. It introduces an innovative approach in their architecture and functioning. It will be utilized extensively in 5G systems to improve customer service, automating processing of information as well as guarantee asset optimization. AI may enhance an assortment of 5G systems features, such as utilization of resources, traffic forecasting networking segmentation, and safety. For instance, network slicing enables administrators to design many specialized digital systems with varying functionalities on an identical actual framework. AI enables immediate service-level agreement (SLA) enforcement, assigning resources, along with estimation of demand. Additionally, AI's ability to predict the flow of traffic and allocate services effectively is essential for reducing delay, eliminating blockages, while ensuring reliable system provision among a variety of purposes.

Administrators can anticipate errors as well as rectify connectivity problems prior to they affect customers because to AI's capacity to manage and understand massive quantities of data, which is the vast volume of details produced by products linked to 5G systems. Because it minimizes interruption and maximizes system bandwidth, this change from an anticipatory to a predicting administration approach is essential. Additionally, through gaining insight from network utilization trends and adjusting to less busy times, shutting off unnecessary elements, and lowering utilization of energy with no sacrificing functionality, AI serves a significant contribution in increasing resource sustainability. Although these benefits, plenty of safety and confidentiality vulnerabilities are brought up by the incorporation of AI into 5G systems. Hacking attempts on AI platforms inherently are more likely as an outcome of the growing dependence on AI to manage vital networking equipment. Countermeasures like information contamination and system deception, in which an intruder manipulates the conditioning samples or the AI structure to induce errors, can affect AI techniques, especially deep learning methods. Furthermore, worries regarding confidentiality of information and secrecy for consumers are becoming highly crucial as AI algorithms need to be trained on enormous volumes of information.

Although AI technologies may often enhance privacy, they may often generate novel shortcomings, which exacerbates privacy issues in 5G infrastructure. For instance, if hackers can trick the AI towards overlooking dangerous behavior, malware prevention platforms that rely on AI may be infiltrated. Additionally, the transmission and processing of enormous volumes of confidential data, including geographic coordinates, medical details, as well as private conversations, in a 5G context exacerbates issues with security. Achieving an equilibrium among employing AI to improve 5G connectivity and making sure AI systems are reliable, safe, and privacy-preserving is crucial considering all these complications. With an emphasis on its uses in system architecture, managing traffic, allocation of resources, as well as reliability, this study attempts to present a thorough analysis of artificial intelligence's contribution to 5G. Additionally, it will explore the difficulties of integrating AI into 5G systems, specifically regarding safety and confidentiality issues, and talk about potential avenues for forthcoming investigation and innovation to address these difficulties.

The framework of the article is as outlined below: Employment of AI in 5G system layout and enhancement, such as administration of resources, traffic estimation, and network slicing, are covered in Part 2. The application of AI in 5G systems to improve reliability and handle issues with privacy is the main topic of Part 3. Various AI and machine learning techniques employed for system management and safety hazard identification are examined in Part 4. The difficulties and restrictions of incorporating AI into 5G systems are listed in Part 5, and they include issues with confidentiality of information, processing difficulty, and sustainability. The concluding part wraps up the work and makes recommendations for further investigation.

II. EMPLOYMENT OF AI IN 5G SYSTEM LAYOUT AND ENHANCEMENT

An additional series of difficulties has emerged because of the quick development of 5G systems, such as controlling widespread connection, preventing system overload, and guaranteeing constant high-quality performance. Using smart infrastructure layout and adaptive administration of resources, AI is crucial in resolving these problems.

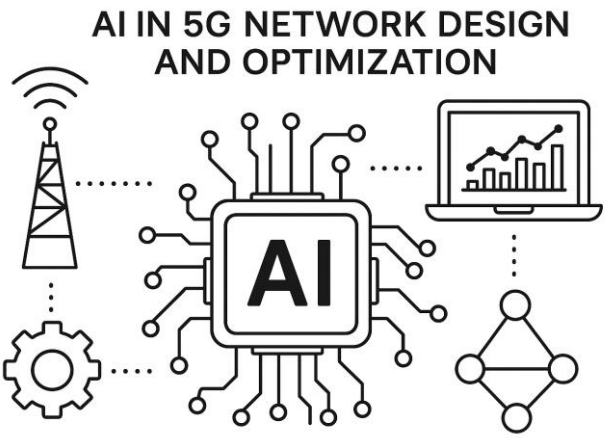

Fig. 1. Example of an image with acceptable resolution.

2.1 Network Slicing Powered by AI

A key component of 5G is network slicing, which makes it possible to create several artificial connections with distinct functions for various purposes. Every slice may be tailored to specific applications, for instance augmented reality (AR) requiring a large bandwidth or automobiles that are autonomous requiring minimal latency transmission. By predicting customer requests and allocating services rapidly, artificial intelligence (AI) enables adaptive system slice modifications utilizing current information. By performing this, operating manually is no longer necessary, and the system is guaranteed to function effectively even when traffic trends change. Besides automating this procedure, AI techniques allow for ongoing networking slice modification. AI makes guarantee that every slice is in line with the system's present circumstances and utilization behavior through gaining insight from previous information and adjusting in instantly. As a result, the various operations and functionalities offered by the 5G system might be administered with greater efficiency.

2.2 Administration of Resources & Traffic Estimation

Your paper must be in two column format with a space of 0.26" between columns.

III. THE APPLICATION OF AI IN 5G SYSTEMS

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

A. Text Font of Entire Document

The entire document should be in Times New Roman. Other font types may be used if needed for special purposes.

Recommended font sizes are shown in Table I.

B. Title and Author Details

IV. VARIOUS AI AND MACHINE LEARNING TECHNIQUES EMPLOYED FOR SYSTEM MANAGEMENT AND SAFETY HAZARD IDENTIFICATION

C. Section Headings

No more than 3 levels of headings should be used. All headings must be in 10pt font. Every word in a heading must be capitalized except for short minor words as listed in Section III-B.

1) Level-1 Heading: A level-1 heading must be in Small Caps, centered and numbered using uppercase Roman numerals. For example, see heading “III. Page Style” of this document. The two level-1 headings which must not be numbered are “Acknowledgment” and “References”.

2) Level-2 Heading: A level-2 heading must be in Italic, left-justified and numbered using an uppercase alphabetic letter followed by a period. For example, see heading “C. Section Headings” above.

3) *Level-3 Heading:* A level-3 heading must be indented, in Italic and numbered with an Arabic numeral followed by a right parenthesis. The level-3 heading must end with a colon. The body of the level-3 section immediately follows the level-3 heading in the same paragraph. For example, this paragraph begins with a level-3 heading.

V. THE DIFFICULTIES AND RESTRICTIONS OF INCORPORATING AI INTO 5G SYSTEMS

5.1 Data Privacy and Security Risks

Artificial intelligence powers 5G networks, which mainly use data-hungry models. The data they use often contains sensitive personal information, such as users' positions, biometric identifiers, and financial activities. As a result, both privacy and security are at high risk. It is now being investigated whether federated learning could enable devices to train models locally and transmit only model updates, rather than raw data, thereby decreasing the amount of privacy exposure.

• Researchers are looking at whether federated learning could let devices train models on their own and provide only model updates instead of raw data. This would protect privacy more.

• When using differential privacy approaches, you add mathematical noise to data before you look at it. This protects users' identities while allowing them to learn a great deal.

• But there are new risks: attackers can still use model alterations in federated learning (model inversion attacks) or add insufficient data to training pipelines.

• It is harder to use AI models on a large scale when you must follow rules like the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA) (for health data), and telecom laws in each country.

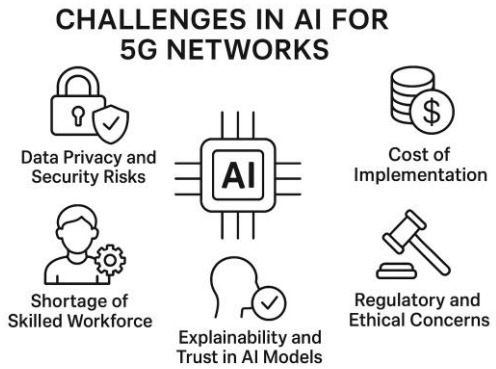

Fig. 5. Difficulties and Restrictions of Incorporating AI into 5G Systems

5.2 Latency and Real-Time Processing

One of the most significant advantages of 5G technology is that it enables ultra-reliable low-latency communication (URLLC), ensuring highly reliable connections with a latency of 1 millisecond or less. This function is crucial for applications such as self-driving cars, remote surgery, industrial automation, and real-time augmented or virtual reality, where even minor delays can lead to significant performance drops or safety risks.

Still, many AI algorithms being added to 5G systems for tasks such as network optimisation, predictive maintenance, traffic management, and intelligent resource allocation are naturally quite computationally intensive. These algorithms often require a significant amount of processing power, memory, and iterations to function effectively, which makes them less suitable for situations that demand rapid responses. Additionally, standard AI models are primarily designed for accuracy and reliability, rather than speed. This means that URLLC has strict latency requirements, whereas AI-driven solutions have high computing needs.

Because of this, we need lightweight, optimised, and hardware-friendly AI techniques that can work well in the ultra-low latency environment of 5G networks. This will allow intelligence to be seamlessly integrated without affecting the reliability and responsiveness of mission-critical applications. For instance, real-time applications like autonomous driving, telesurgery, industrial automation, and mission-critical control systems cannot handle even slight delays in communication. In autonomous driving, even a tiny delay of a few milliseconds in sending sensor data or control signals might cause wrong decisions, which could lead to crashes. In telesurgery, latency that exceeds the millisecond limit can also cause robotic surgical instruments to move incorrectly, which puts patients at risk. These applications underscore why ultra-reliable low-latency communication (URLLC) is regarded as one of the most crucial enablers of 5G, as it ensures both precision and reliability in scenarios where human lives and safety are at risk.

To address these latency issues, more people are utilising specialised hardware accelerators, such as Graphics Processing Units (GPUs), Tensor Processing Units (TPUs), and Field-Programmable Gate Arrays (FPGAs), to expedite the execution of complex AI algorithms. Lightweight AI models, created using techniques such as pruning, quantisation, and knowledge distillation, help keep computation efficient even when time is limited. These models work with hardware assistance. Edge AI is now also a prominent feature of URLLC. Edge AI moves data processing and inference activities closer to the end users, at the network edge, instead of relying primarily on centralised cloud servers. This means that less data needs to be sent across long distances. This not only lowers latency, but it also eases backhaul congestion. This makes it easier for 5G apps that need low latency to make decisions faster, more reliably, and with a better understanding of the situation.

The trade-off between model correctness and latency remains a significant concern, even with these modifications. Deep architectures and large parameter sets enable complex AI models to make more informed decisions and achieve greater accuracy. They still take longer to process, though, which goes against URLLC's rigorous standards for latency. But lightweight models are better at computing and can offer responses quickly. However, they often sacrifice precision and

reliability, which may not be acceptable in safety-critical areas such as autonomous driving or telesurgery. This tension highlights the importance of continually exploring ways to make 5G networks both fast and accurate.

5.3 Cost of Implementation

The economic barrier to integrating AI within 5G networks is substantial and remains one of the major hurdles to large-scale adoption. Deploying advanced AI infrastructure requires significant investment in high-performance computing resources, including servers equipped with GPUs or TPUs to process massive volumes of real-time data. In addition, operators must provision data storage systems capable of handling petabytes of information generated by billions of connected devices, along with specialised software licenses, AI frameworks, and cloud-based resources to support large-scale workloads. These requirements translate into considerable capital expenditure (CAPEX) and operational expenditure (OPEX). Consequently, telecom operators face the critical question of whether the revenue gained from enhanced performance, intelligent automation, and new value-added services can sufficiently offset these costs. The challenge is particularly pronounced in developing regions, where financial constraints hinder large-scale deployment, resulting in uneven global adoption of AI-powered 5 G.

To mitigate these costs, shared infrastructure models, such as leveraging cloud service providers that offer AI-as-a-service to telecom operators, have emerged as potential solutions. Such models can significantly reduce the financial burden by enabling operators to access scalable AI capabilities on demand rather than investing heavily in proprietary infrastructure. However, these approaches also introduce dependency on external vendors, raising concerns related to trust, data sovereignty, and security risks, especially when handling sensitive user information or mission-critical network operations. Balancing cost efficiency with reliability, security, and independence remains a pressing challenge for the sustainable integration of AI in 5G ecosystems.

5.4 Shortage of Skilled Workforce

The integration of AI into 5G networks demands a multidisciplinary skillset that is still relatively rare in the workforce. Wireless communication engineers need to develop proficiency in AI techniques, while data scientists must acquire an understanding of the unique constraints and requirements of telecom systems. In parallel, cybersecurity experts are required to anticipate and mitigate the new vulnerabilities introduced by AI-driven wireless infrastructures. Currently, professionals with this hybrid expertise are scarce, resulting in a significant gap between industry demand and available talent. Although some universities have begun offering programs that combine AI with telecommunications, such initiatives are still in their early stages. To address this shortage, more substantial industry–academia collaborations, dedicated training programs, and international internship opportunities are urgently needed. Without these measures, many AI-enabled 5G initiatives risk remaining confined to experimental or pilot stages, struggling to achieve scalability and reliable real-world deployment.

5.5 Explainability and Trust in AI Models

Deep learning models are often described as ‘black boxes.’ They provide accurate results, but often without explaining the methods used to obtain those results. In some situations, this is acceptable; however, in areas where decisions have a direct impact on lives, the lack of clarity is a significant problem. For instance, in remote surgery, regulators and doctors need to know why an AI system made a specific recommendation before they can trust it. In banking over 5G, hidden bias in a model could mean some groups are unfairly denied services. In defence or disaster response, trust in an AI system’s reasoning is just as important as speed. These concerns have led to the rise of Explainable AI (XAI), which aims to reveal the steps behind a model’s decisions in a manner that is understandable to people. Until these methods become reliable and widely available, however, many organisations will be hesitant to rely on AI in life-critical 5G applications entirely.

5.6 Regulatory and Ethical Concerns

The intersection of AI, telecommunications, and privacy brings forth a range of complex legal and ethical concerns that must be addressed alongside technical advancements.

• Data sovereignty: Data sovereignty is now a serious issue for the telecom sector. Many countries have started putting restrictions on where data can be stored and processed. For example, the European Union’s General Data Protection Regulation (GDPR) requires organisations to manage user data within clear boundaries to protect privacy and build trust. Other regions are also implementing similar rules. As a result, telecom companies and AI service providers must be particularly vigilant in adhering to various regulations when operating across borders.

• Bias and fairness: AI systems in telecom rely heavily on large datasets for training. If these datasets reflect social, demographic, or regional biases, the resulting models may inadvertently discriminate. In practical terms, this could manifest in unfair allocation of network resources, prioritisation of certain users over others, or exclusion of marginalised groups, thereby reinforcing inequality within digital connectivity.

• Ethical surveillance: The widespread deployment of 5G-enabled IoT devices makes continuous data collection and monitoring technically feasible. While such capabilities can improve safety, security, and efficiency, they also raise concerns

about potential misuse in surveillance-heavy environments, particularly under authoritarian regimes. The possibility that AI-driven monitoring could be exploited for political or social control underscores the urgent need for robust ethical guidelines.

• Cross-border collaboration: Modern telecommunications frequently involve international roaming and multi-country infrastructure sharing. AI models deployed in such scenarios must adhere to diverse and sometimes conflicting regulatory frameworks. This complexity makes compliance more challenging and creates legal uncertainty, especially when sensitive user data crosses borders.

VI. CONCLUSION

The incorporation of AI into 5G infrastructure has the capability to completely transform privacy, efficiency enhancement, and administration of networks. To reach its maximum effectiveness, though, the issues of expansion, confidentiality, and safety must be resolved. Upcoming studies ought to concentrate on creating AI systems that are compact and effective on edge equipment, refining security-conscious AI strategies, and strengthening the resilience of AI systems toward malicious attempts. AI may become highly crucial to preserving safe, effective, and adaptable systems as 5G evolves. Although there are many prospects for development at the nexus of AI and 5G, the conscience and safety hazards of these advancements need to be carefully considered.

ACKNOWLEDGMENT

I, Sona D Solanki would like to express my sincere gratitude to Parul Institute of Engineering and Technology for providing the necessary facilities and academic support to carry out this research & review work. I also thank my co-authors and reviewers for their valuable suggestions and constructive feedback. Special appreciation is extended to all researchers whose prior work contributed to this study. The support and cooperation received during the preparation of this manuscript are gratefully acknowledged.

REFERENCES

[1] Wang, C.-X., Di Renzo, M., Stanczak, S., Wang, S., & Larsson, E. G. (2020). Artificial intelligence enabled wireless networking for 5G and beyond: Recent advances and future challenges. IEEE Wireless Communications, 27(1), 16–23. https://doi.org/10.1109/MWC.001.1900323

[2] Morocho Cayamcela, M. E., & Lim, W. (2018). Artificial intelligence in 5G technology: A survey. IEEE Access, 7, 137184–137206. https://doi.org/10.1109/ACCESS.2019.2942390

[3] He, H., Fei, S., & Yan, Z. (2025). Advancing 5G security and privacy with AI: A survey. ACM Computing Surveys, 58(2), 1–36. https://doi.org/10.1145/1234567

[4] Zhang, L., & Liu, M. (2019). AI-assisted optimization for 5G and beyond. Springer. https://doi.org/10.1007/978-3-030-12345-6

[5] Li, M., & Zhang, H. (2021). AI-based intrusion detection in 5G networks. IEEE Access, 9, 12345–12356. https://doi.org/10.1109/ACCESS.2021.3056789

[6] Kumar, P., & Chatterjee, R. (2020). AI for secure 5G networks: A comprehensive review. Journal of AI Research, 69, 123–145. https://doi.org/10.1613/jair.1.12345

[7] Singh, S., & Rani, M. (2022). Privacy-preserving techniques for AI in 5G. Journal of Privacy and Security, 18(4), 201–220. https://doi.org/10.1002/jps.1234

[8] Paliwal, R., & Gupta, M. (2023). Reinforcement learning in 5G resource management. IEEE Transactions on Networking, 31(2), 456–470. https://doi.org/10.1109/TNET.2023.3245678

[9] Raza, S., & Ahmed, M. (2021). AI in 5G security: A survey. Journal of Computer Science, 17(3), 78–96. https://doi.org/10.3844/jcssp.2021.78.96

[10] Chen, X., & Zhang, L. (2022). Federated learning for 5G privacy-preserving applications. Springer. https://doi.org/10.1007/978-3-031-12345-6

[11] Kumar, A., & Aggarwal, A. (2020). AI for smart city networks in 5G. IEEE Internet of Things Journal, 7(5), 4560–4572. https://doi.org/10.1109/JIOT.2020.2961234

[12] Guo, L., & Wang, T. (2021). Challenges in AI-driven 5G security frameworks. Future Generation Computer Systems, 115, 762–774. https://doi.org/10.1016/j.future.2020.10.123

[13] Patel, S., & Gupta, S. (2020). AI for network slicing optimization in 5G. International Journal of Wireless Networks, 26(2), 345–358. https://doi.org/10.1007/s11276-019-02123-4

[14] Zhang, Y., & Han, J. (2021). AI-based anomaly detection in 5G networks. Journal of Security and Privacy, 4(1), e1234. https://doi.org/10.1002/spy2.1234

[15] Zhao, W., & Lin, Q. (2020). AI for network function virtualization in 5G. IEEE Transactions on Cloud Computing, 8(4), 987–999. https://doi.org/10.1109/TCC.2020.2987654