iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VII **Month of publication:** July 2025

DOI: https://doi.org/10.22214/ijraset.2025.73375

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

Private 5G Network: Security, Challenges, and Comparison with Wi-Fi

Manish Kumar[1], Anuj Kumar[2]
AMD India,

Abstract: ***As Indian industries embrace digital transformation, there is an escalating demand for wireless connectivity that delivers not just speed but also reliability, security, and customizability. While public 5G networks have introduced improvements in latency and bandwidth, they often fall short in meeting the specialized needs of enterprises due to shared infrastructure and limited control. This paper investigates the emerging landscape of private 5G networks in India, detailing their architecture, deployment models, regulatory frameworks, and practical use cases across verticals such as manufacturing, healthcare, logistics, and mining. The study highlights how private networks enable real-time operations, support edge computing, and provide enterprise-grade quality of service through localized spectrum and standalone configurations. A comparative analysis with public 5G and next-generation Wi-Fi standards demonstrates the technical and operational advantages of private deployments. This paper exploresspectrum sharing challenges, policy implications and the evolving role of telecom operators in enterprise-led 5G initiatives. By capturing ongoing trends and research directions, this work offers a comprehensive view of how private 5G can act as a catalyst for India's next wave of industrial innovation.***

Keywords: Private 5G, Wi-Fi, Private 5G Deployment, Security, Public 5G

I. INTRODUCTION: THE NEED FOR PRIVATE 5G NETWORKS

With the ongoing digital transformation in sectors like manufacturing, healthcare, education, and logistics, Indian enterprises increasingly demand robust wireless networks. The volume of connected devices is growing rapidly, and traditional networks often struggle to deliver the desired level of performance, security, and control.

While public 5G has ushered in higher data speeds and improved latency compared to its predecessors, it is not always suitable for enterprise-specific applications. Congestion, shared infrastructure, and unpredictable quality of service often make public 5G less ideal. In contrast, private 5G networks allow organizations to build and manage their own infrastructure, tailored to specific operational requirements. This leads to improved data privacy, seamless integration with critical applications, and better control over network performance.

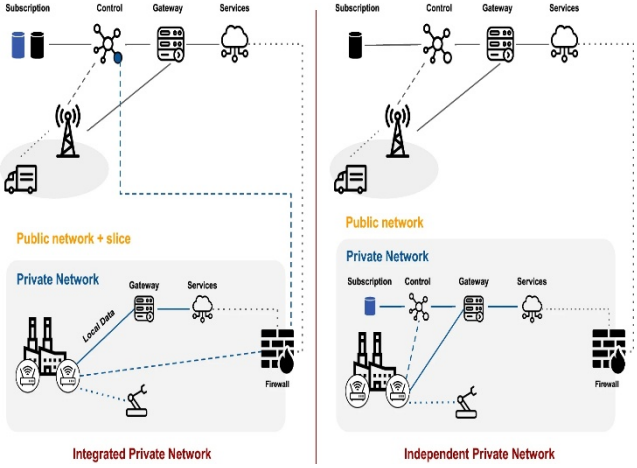


Fig 1. Public vs Private Network Needs[1]

II. ARCHITECTURE: PRIVATE 5G NETWORKS

A private 5G network mirrors the essential structure of a standard public 5G network, it is specifically designed to be deployed, owned, and operated by a private entity—such as a manufacturing company, hospital, or university—within its premises. These networks built to serve the specific operational needs of the organization, providing enhanced control, security, and performance.

The primary components of a private 5G network include:

1) *User Equipment (UE):* This refers to all endpoints that access the network, such as smartphones, IoT sensors, wearable medical devices, smart cameras, AR/VR headsets, and autonomous machinery. Each device connects to the network wirelessly via 5G radios.
2) *Radio Access Network (RAN):* Comprising base stations or small cells, the RAN facilitates wireless transmission between UEs and the core network. In a private 5G context, the RAN is deployed on-site and can be configured to provide optimized coverage for a particular environment, be it indoors, underground, or spread across a campus.
3) *5G Core (5GC):*Core network is responsible for user authentication, mobility management, traffic routing, and policy enforcement. The private 5GC may be implemented on-premises, at the edge, or hosted on a private or public cloud platform, depending on latency requirements and data governance policies.
4) *Edge Computing Infrastructure:* One of the standout features of private 5G is its synergy with edge computing. Data generated by sensors and devices can be processed at or near the source, reducing the time it takes for insights to be generated and actions to be taken. This is especially useful in time-critical operations such as machine control, emergency response, and automated inspection.
5) *Network Management and Orchestration Tools:* These tools provide a centralized interface for configuring, monitoring, and managing network resources. Features such as real-time analytics, fault management, performance optimization, and security monitoring are essential for ensuring continuous service availability and quality.

Private 5G networks can be deployed in either of the following two architectural models:

- *Standalone (SA):* This model operates completely independently of public networks. It uses its own RAN and core components, offering full control over every aspect of the network, from device registration to traffic routing and data security. This is ideal for organizations with stringent security, reliability, or customization needs.
- *Non-Standalone (NSA):* In this model, the private network relies partially on an existing public 4G/5G infrastructure—typically for core network functions—while deploying its own RAN. Customization and Security may be limited but it allows faster deployment leading to cost savings.

Hybrid configurations are also gaining popularity, where part of the network is owned and operated privately, and other elements are managed through collaboration with telecom service providers.

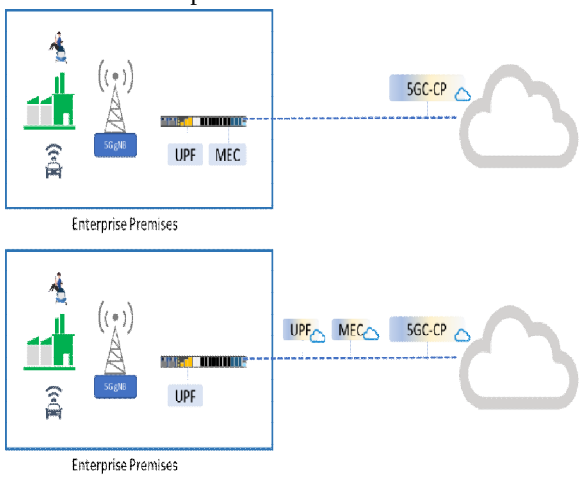


Fig 2: Architecture of a Private 5G Network [1]

III. DEPLOYMENT MODELS

Deployment models for private 5G vary significantly based on enterprise size, operational goals, regulatory conditions, and spectrum availability. Below are the primary models observed in practical deployments [1]:

1) *Locally Licensed Spectrum*

In this model, enterprises directly obtain spectrum licenses from the regulatory authority. In India, the Department of Telecommunications (DoT) allocates spectrum in high-frequency bands such as 26 GHz for industrial and enterprise usage. This model gives full control to the organization, ensuring robust performance and minimal interference.

2) Network Slicing

Here, a mobile network operator (MNO) offers a dedicated "slice" of its public 5G infrastructure to an enterprise. Though not fully isolated, the slice is logically segregated, allowing the enterprise to operate its services with agreed-upon service level agreements (SLAs). This approach is beneficial for companies that cannot invest in full infrastructure.

3) Neutral Host Networks

In shared environments such as airports, stadiums, or business parks, a third-party service provider deploys a neutral host network. Multiple enterprises can use the same physical infrastructure, reducecosts, and promote resource efficiency. This is particularly effective for medium-scale enterprises or startups.

4) Hybrid Model

A hybrid model combines private and public network assets. For example, an enterprise may run its core network while using public RAN infrastructure or vice versa. This model balances flexibility with cost savings and is suitable for operations spread across multiple locations.

5) Cloud-based Private 5G

Some deployments use cloud-hosted 5G cores, where the control and user planes are virtualized and managed remotely. This approach lowers capital expenditure and facilitates easier scalability, making it ideal for tech-driven startups and SMEs.

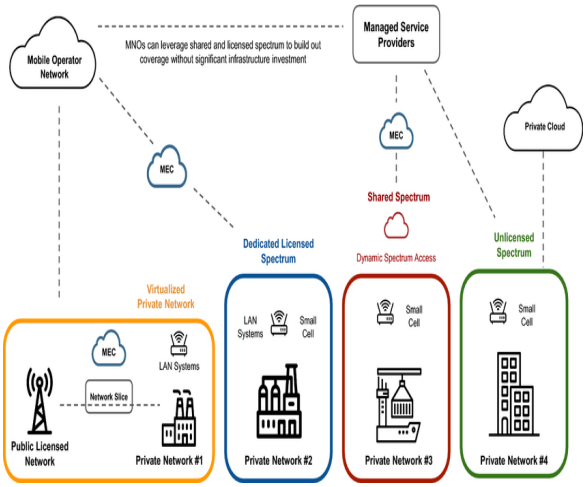


Fig 3: Deployment Models of Private 5G [1]

IV. USE CASES

1) Manufacturing [8]

The manufacturing sector is undergoing a shift towards automation, where real-time communication and control are critical. Private 5G supports seamless connectivity for robots, assembly lines, and control systems. Its ultra-low latency ensures timely coordination among automated mobile robots, while high reliability facilitates predictive maintenance and quality assurance through real-time sensor feedback.

2) Healthcare

In medical facilities, private 5G enables secure, high-speed connections between various critical devices. It supports applications such as remote diagnostics, wireless telemetry, and video-assisted surgeries. With improved bandwidth and low latency, healthcare professionals can access patient data and imaging tools quickly, enhancing both diagnostics and care delivery.

3) Logistics

Efficient planningrelies on uninterrupted, coordinated operations. Private 5G enables communication among automated guided vehicles (AGVs), IoT-enabled inventory systems, and drones for stock verification. These features help reduce human errors and accelerate the movement and tracking of goods within large distribution centers or warehouses.

4) Energy and Utilities

Power grids and utility networks require consistent monitoring and rapid decision-making. Private 5G provides a reliable link between remote equipment, substations, and control centers. This ensures real-time data transmission for fault detection, load balancing, and operational safety, even in isolated regions.

5) Mining

Mining operations occur in remote and harsh conditions where public networkstend to underperform. Private 5G ensures robust connectivity for underground machinery, enabling automation of drilling and hauling systems. It also improves worker safety by supporting connected wearables and surveillance systems that monitor hazardous environments.

6) Public Transportation

Private 5G enhances operational efficiency in public transport hubs like airports, metro stations, and bus depots. It facilitates intelligent surveillance, crowd management, and real-time passenger information systems. Additionally, it supports contactless ticketing and efficient interconnectivity between transport control systems and IoT infrastructure. Private 5G networks help factories automate operations using real-time data. AMRs, sensor-based quality checks, and predictive maintenance tools all rely on dependable, low-latency connectivity.

V. RESEARCH DIRECTIONS

Private 5G is an active research area. Current focuses include:

1) Using AI and ML to manage network traffic and detect anomalies.
2) Integrating with TSN to support time-sensitive industrial processes.
3) Exploring advanced security protocols.
4) Developing systems ready for 6G enhancements.
5) Promoting open interfaces through O-RAN to reduce costs.

VI. COMPARISON WITH PUBLIC 5G NETWORKS

Feature	Private 5G	Public 5G
Ownership	Enterprise-managed	Operator-managed
Control	Full	Limited
Security	Higher, on-site	Dependent on operator
Customization	Extensive	Standardized
Latency	Predictable	Variable

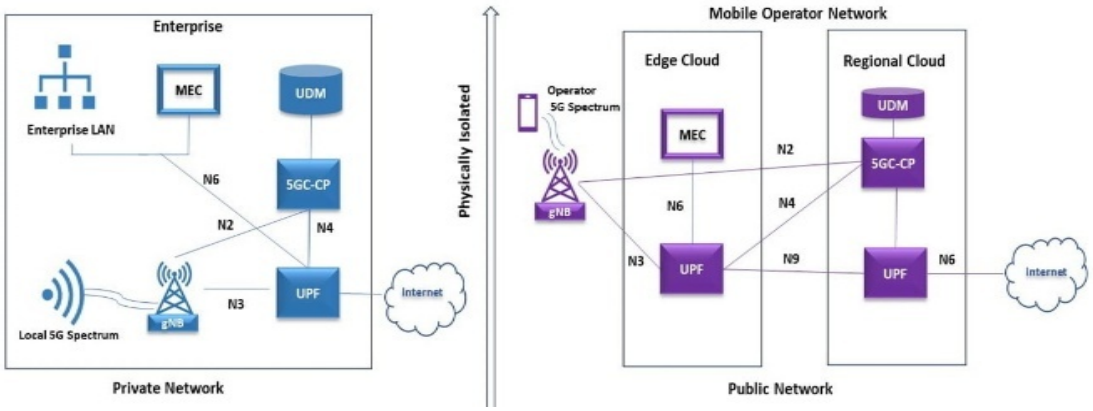


Fig 4: Comparisonbetween Private and Public 5G networks [1]

VII. COMPARISON WITH WI-FI

Wi-Fi 6 and its successors have brought significant performance improvements in terms of throughput and multi-user handling. Wi-Fi 7 further enhances this with multi-link operation, deterministic latency, and wider channels. However, Wi-Fi still operates in unlicensed bands, making it prone to interference, especially in urban or industrial areas with many overlapping networks. [3-5]

Private 5G, by contrast, operates in a licensed or locally managed spectrum, offering enterprises greater predictability and control. It provides robust support for mobility, which is vital for use cases like autonomous mobile robots and connected vehicles. Moreover, private 5G networks are inherently more secure due to SIM-based authentication and enterprise-specific policy control.

For mission-critical environments—such as smart manufacturing, healthcare diagnostics, and logistics—private 5G ensures more consistent latency, broader coverage, and enforceable SLAs. While Wi-Fi remains ideal for general office settings and non-critical applications, the deterministic nature of 5G makes it preferable for real-time industrial operations.

Feature	Private 5G	Wi-Fi 6/7/8
Spectrum	Licensed or shared	Unlicensed
Interference	Low	High in dense networks
Mobility	Seamless handovers	Limited handover support
QoS	Guaranteed via 3GPP standards	Best-effort, with some QoS in Wi-Fi 7
Security	Carrier-grade encryption, SIM-based	WPA3, user-managed

VIII. SECURITY

In private 5G networks, security measures are crafted to align closely with the operational and regulatory needs of the enterprise. Unlike public networks, where security mechanisms are standardized and controlled by the service provider, private 5G allows organizations to implement tailored security protocols that address unique vulnerabilities and data governance priorities.

Key components of private 5G security include robust identity and access management, strong encryption for over-the-air and backhaul communication, and complete isolation of user and control planes. These networks also facilitate local data processing, reducing exposure to external networks and potential breaches.

Security responsibilities are shared among the enterprise IT/security teams, system integrators, and technology vendors. Potential risks include data interception, misconfigured network components, software vulnerabilities, and insider threats. To counter these, best practices such as role-based access control, network segmentation, regular patching, threat intelligence sharing, and adherence to zero-trust frameworks are increasingly adopted.

Given the evolving threat landscape, many organizations also employ real-time intrusion detection and prevention systems (IDPS), perform periodic penetration testing, and enforce strict compliance with standards such as ISO/IEC 27001 or 3GPP security specifications.

IX. CHALLENGES: PRIVATE 5G DEPLOYMENT

Deploying a private 5G network presents a unique set of challenges that must be addressed to ensure successful adoption and long-term sustainability.

1) Spectrum**:** Access to spectrum remains one of the most significant barriers. Regulatory policies around spectrum allocation for private use are still evolving in many countries, including India. While some bands have been earmarked for enterprises, the licensing process can be time-consuming, and availability may vary by region, making it difficult for businesses to plan network rollouts.
2) Cost**:** The financial investment required for deploying private 5G can be substantial. Costs include not only the acquisition of spectrum and network hardware but also integration with existing IT infrastructure, network planning, and operational support. For small and mid-sized enterprises, these expenses can be prohibitive without viable financing or partnership models.
3) Expertise**:** Building and maintaining a private 5G network requires specialized skills in radio frequency (RF) engineering, cybersecurity, network orchestration, and device integration. There is a growing demand for professionals trained in 5G technologies, and many enterprises face difficulty finding or developing the required talent internally.
4) Compliance**:** Enterprises must ensure that their private 5G networks adhere to national telecom regulations and international standards. This includes lawful interception capabilities, data protection policies, and secure access controls. Noncompliance leads to legal penalties and security vulnerabilities.
5) Integration with Legacy Systems**:** Many enterprises operate on a legacy infrastructure that may not be readily compatible with 5G. Integrating these systems with a modern private network often requires custom solutions, adding further complexity and cost.
6) Vendor Lock-in and Interoperability: Selecting technology providers that support open standards and multi-vendor environments is crucial to avoid being tied to a single vendor ecosystem, which could limit flexibility and increase long-term costs.

X. SHARED SPECTRUM AND POLICY IN INDIA

Enterprises are allowed to deploy private network using both shared spectrum and licensed spectrum by Indian Department of Telecommunications. This move aims to accelerate digital transformation in sectors such as manufacturing, logistics, and healthcare.

Shared bands, particularly in the 5 GHz and 6 GHz range, offer a cost-effective alternative to licensed spectrum. These bands are unlicensed, meaning they are open to use by multiple users under specific power and interference guidelines. While Wi-Fi networks have historically operated in these frequencies with superior results, private 5G brings a new level of sophistication and demand for stability.

Deployment and Operation in the shared spectrum comes with its own set of hurdles. The risk of interference is high, especially in dense urban areas or environments with many overlapping networks. Private 5G solutions deployed in shared bands must therefore employ intelligent spectrum management tools and interference mitigation strategies to maintain performance.

Furthermore, clarity is still needed on long-term spectrum policy, particularly around pricing, licensing duration, and interference resolution protocols. Greater regulatory certainty will encourage more enterprises to invest in private networks and drive innovation in spectrum sharing techniques.

XI. ROLE OF MOBILE NETWORK OPERATORS (MNOS)

Mobile Network Operators (MNOs) are in a pivotal position as enterprises increasingly explore private 5G deployments. Traditionally focused on mass-market consumer services, MNOs are now adapting to serve enterprise verticals that demand customized, high-performance networks.

On the one hand, MNOs can become key enablers by providing managed private 5G services, leasing spectrum, and offering end-to-end integration support. This model benefits enterprises by lowering the barrier to entry, especially for those lacking in-house expertise or infrastructure.

On the other hand, some enterprises prefer full ownership and control of their networks, positioning MNOs more as competitors than partners leading to evolving service offerings and business models by telecom operators to stay relevant. Partnerships with system integrators, cloud providers, and hardware vendors can help MNOs expand their reach into enterprise markets.

Private 5G also presents a revenue diversification opportunity for MNOs, allowing them to offset declining consumer margins through high-value enterprise contracts. However, doing so requires investment in network slicing, resolute enterprise teams, and new operational frameworks.

XII. INTEGRATION WITH PUBLIC 5G

Private 5G networks do not have to function in isolation. Many enterprises choose to integrate their private networks with public 5G infrastructure, creating hybrid environments that offer the best of both worlds resulting in resource optimization, broader coverage leading to seamless mobility.

For instance, a manufacturing plant may use a private 5G setup for on-site operations while relying on public 5G for remote maintenance or logistics coordination. Similarly, healthcare facilities might use private 5G within hospital premises and switch to public 5G for home monitoring of patients.

However, such integration demands robust policy control, secure handover mechanisms, and well-defined network boundaries to protect sensitive data. The use of dual SIM devices, multiple access points, and service-based architecture helps in achieving a smooth transition between private and public domains.

Challenges in this model include ensuring data sovereignty, avoiding SLA violations, and mitigating vulnerabilities introduced by the public network. Hence, network segmentation, encryption, and coordinated management systems are crucial for maintaining the integrity of hybrid deployments.

XIII. CONCLUSION

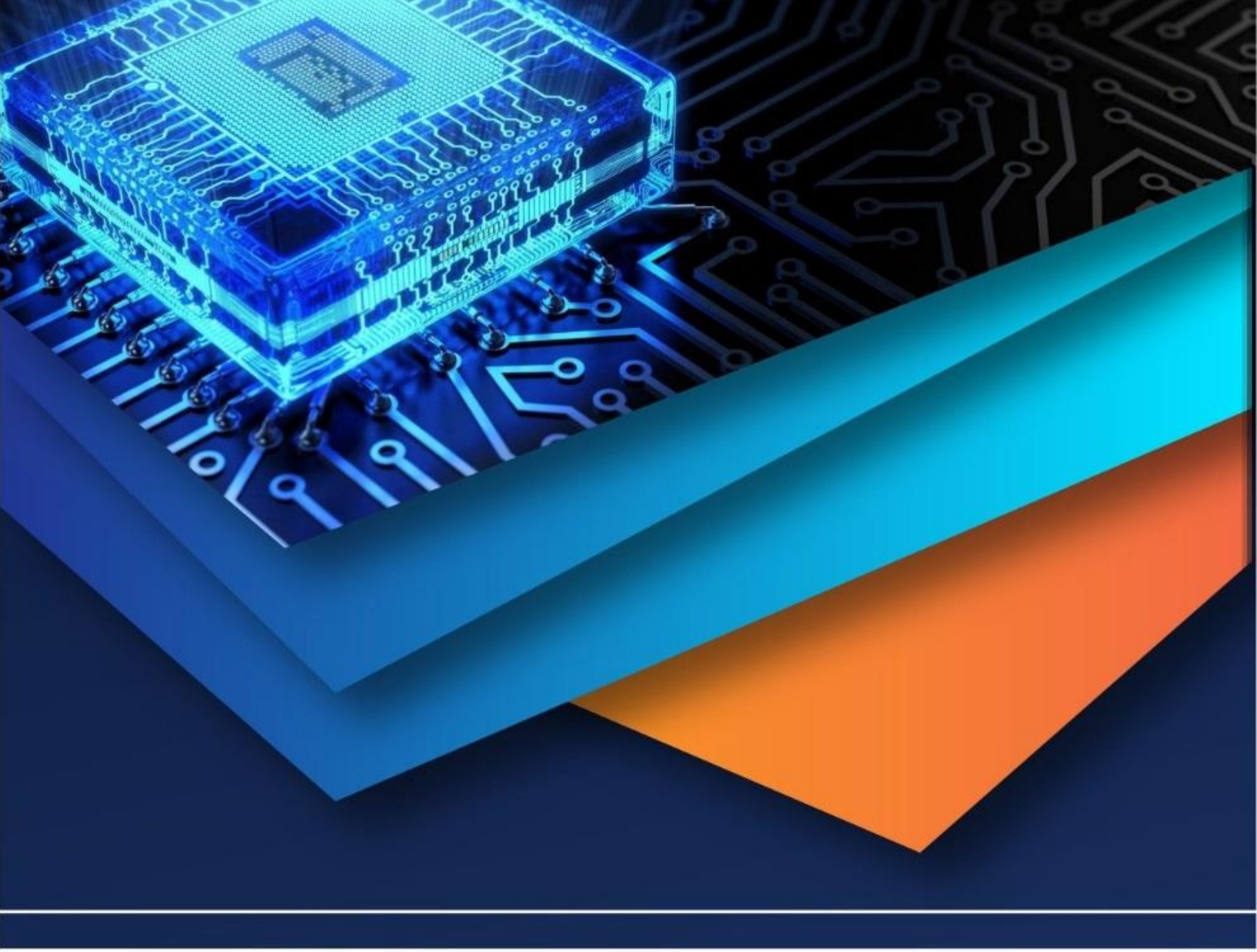
Private 5G networks will play a transformative role in determining the digital infrastructure of Indian enterprises. By offering dedicated connectivity with low latency, enhanced security, and high configurability, these networks provide a strong foundation for mission-critical applications across various sectors. Unlike public networks, private 5G solutions grant organizations full control over deployment and performance, which is essential for time-sensitive and data-intensive operations.

Through a detailed examination of deployment models, spectrum access strategies, and integration pathways, this paper underscores that a tailored approach—aligned with enterprise needs and regulatory realities—is essential for successful implementation.

The comparison with public 5G and advanced Wi-Fi standards further illustrates the unique value proposition of private networks, especially in industrial and automation-heavy environments. As spectrum policies in India continue to evolve, and as interest in AI-driven orchestration and O-RAN grows, enterprises must also prepare for technical, financial, and operational challenges. Looking ahead, private 5G stands not merely as a network upgrade, but as a strategic enabler of digital transformation, competitiveness, and long-term innovation across India's enterprise ecosystem.

REFERENCES

[1] Prasad Honnavalli, Sivaraman Eswaran. 2022, Private 5G networks: a survey on enabling technologies, deployment models, use cases and research directions. ResearchGate
[2] Tezcan Cogalan, Daniel Camps-Mur. 2022, 5G-CLARITY: 5G-Advanced Private Networks Integrating 5GNR, Wi-Fi, and LiFi. IEEE Conf
[3] TS 23.501, System Architecture for the 5G System. 3GPP Release 15
[4] TS 33.501, 5G Security architecture and procedures for 5G System 3GPP Release 15
[5] Cailian Deng, Xuming Fang, 2020. Wi-Fi 7: New Challenges and Opportunities. IEEE Conf
[6] Shivam Chauhan, Arpit Sharma, 2021. A Review on Wi-Fi 7 Use Cases. IEEE Conf
[7] Wi-Fi 7. https://www.qualcomm.com/products/technology/wi-fi/wi-fi-7
[8] 5G for Connected Industries and Automation. https://5g-acia.org/
[9] Shared & unlicensed spectrum LTE/5G network ecosystem. https://www.snstelecom.com/shared-spectrum



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY