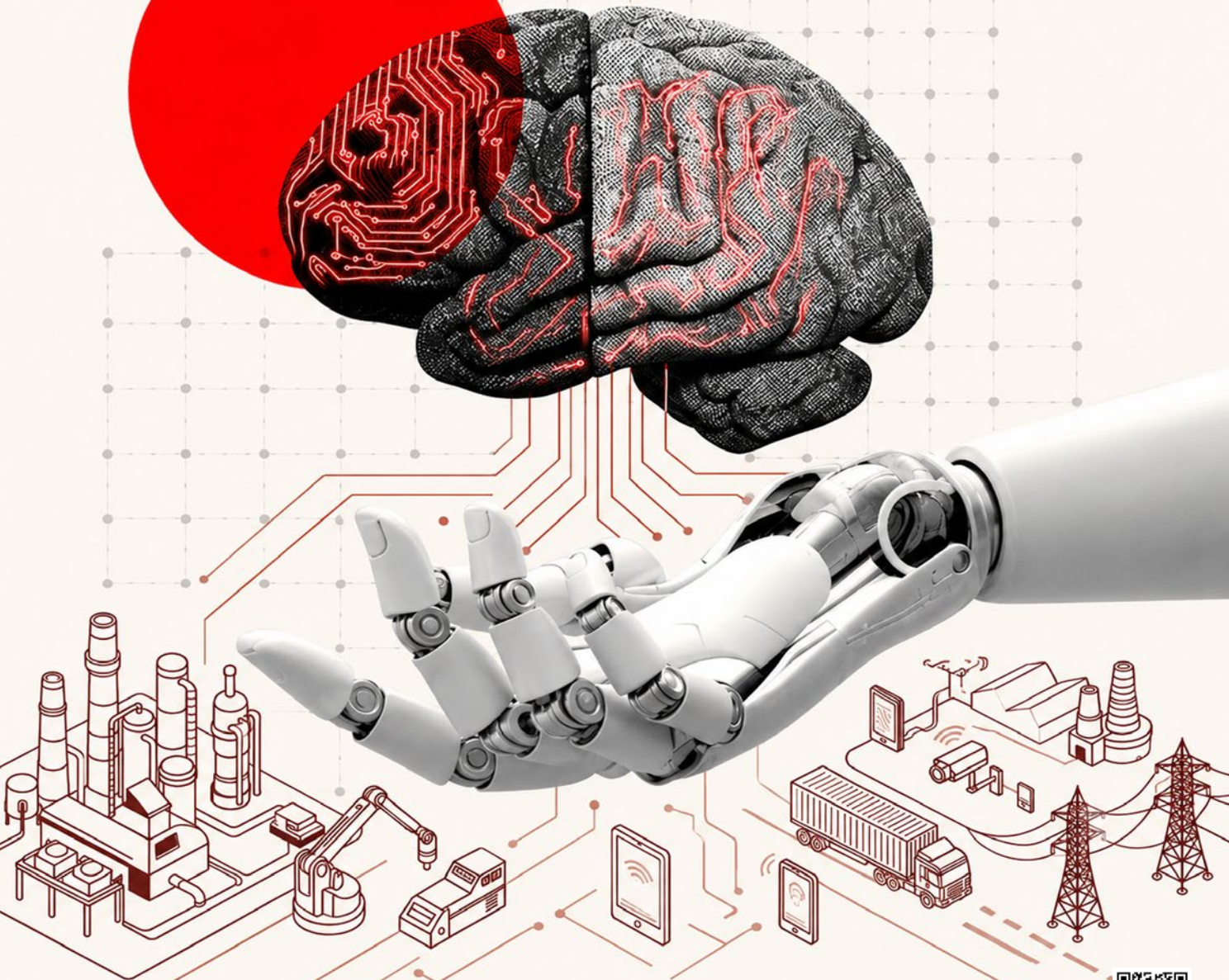


The skinny network

Low-power networks are quietly becoming the nervous system running industrial operations, connecting sensors, machines, and AI with unprecedented efficiency.





APEEJAY SCHOOL

Sector 15, Faridabad | Affiliated to CBSE | Estd. in 1972



Foundation For Lifelong Learning Starts Here



KEY HIGHLIGHTS



Value-based holistic education



State-of-the-art infrastructure



Safe & secure campus



Curriculum aligned with NEP 2020



Focus on experiential and competency-based learning



Spectacular competitive exam results with students placement in National and international Universities

AWARD & RECOGNITION

Ranked No.1 in 'Faridabad Leaders' category by Times School Survey 2025



For admission enquiry, please contact:

Apeejay School, Sector 15, Faridabad, Haryana

Admission Helpline Number:

+91-8826 074 074, +91 9599 105 614

Email: skool.ms.fbd@apj.edu

CONNECT WITH US



FACEBOOK



INSTAGRAM



When it comes to higher recall, **TRUST PRINT.**



That's the power of print. In addition to **70% higher recall**, according to neuroscience research it's proven that print content is **21% easier to understand** and more memorable than digital media. That is why, print content connects with our brain more efficiently and effectively. So, choose to read newspapers.

INS

THE INDIAN NEWSPAPER SOCIETY

EDITORIAL

MANAGING EDITOR: Thomas George
CONSULTING GROUP EDITOR: Ibrahim Ahmad
EDITOR: Shubhendu Parth
CONSULTING EDITOR: Pradeep Chakraborty
CONTRIBUTING EDITOR: Pratima Harigunani
ASSISTANT EDITOR: Ayushi Singh
SUB EDITOR: Manisha Sharma
SR. MANAGER DESIGN & COVER DESIGN: Vijay Chand

HEAD - AI TRANSFORMATION & CONTENT STUDIO: Sudesh Prasad
VICE PRESIDENT RESEARCH: Anil Chopra

MANAGER CYBERMEDIA LABS: Ashok K Pandey

LARGE BUSINESS CONVENTIONS & PROJECTS

CONFERENCE PRODUCER: Ajay Dhoundiyal

BUSINESS SOLUTIONS & SALES

GM - BUSINESS SOLUTIONS: Rajnish Jamur
SR MANAGER: Ajay Dhoundiyal (North)
SR MANAGER: Sudhir Arora (North, East)
SR. MANAGER: Anita Swamy (South)

MARKETING & ALLIANCES

SR MANAGER: Ajay Dhoundiyal

EVENTS, OPERATIONS & COMMERCIALS

GM - EVENTS OPERATIONS & PROJECT: Ankit Parashar
CREATIVE DESIGN: Sunali
SR. MANAGER - ONLINE AD OPERATIONS: Suneetha B S
SR. MANAGER - COMMERCIAL & MIS: Ravi Kant Kumar
MANAGER - COMMERCIAL & ADMIN: Ashok Kumar

DISTRIBUTION & GROWTH:

GM - DISTRIBUTION & GROWTH: Prateek Malik
SR. MANAGER - INSTITUTIONAL SUBSCRIPTION: Sudhir Arora
SR. MANAGER - INSTITUTIONAL SUBSCRIPTION: C. Ramachandran (South)
SR. MANAGER - AUDIENCE GROWTH: Alok Saxena
EXECUTIVE - AUDIENCE SERVICE: Kusum Sharma
MANAGER - CREATIVE OPERATIONS: Suraj Singh
SOCIAL MEDIA EXECUTIVE: Amit Bhardwaj, Priyanshi Goyal
SEO TEAM: Neha Joshi, Chandan Kumar Pandey
PRESS CO-ORDINATOR: Rakesh Kumar Gupta

OUR OFFICES

GURGAON (CORPORATE OFFICE)

Cyber House
B-35 Sector-32, Gurgaon, Haryana - 122 003
Tel: 0124 - 4237517, Fax: 0124 - 2380694

BENGALURU

205-207, Shree Complex (Opposite RBANMS Ground)
#73, St John's Road, Bengaluru - 560 042
Tel: +91 (80) 4302 8412, Fax: +91 (80) 2530 7971

MUMBAI

INS tower, Office No. 326, Bandra Kurla Complex Road,
G Block BKC, Bandra East, Mumbai - 400051
Mobile: +91 99694 24024

INTERNATIONAL

Huson International Media
President, 1999, South Bascom Avenue, Suite 1000,
Campbell, CA95008, USA
Tel: +1-408-879 6666, Fax: +1-408-879 6669

Voice&Data is printed and published by Pradeep Gupta on behalf of Cyber Media (India) Ltd, D-74, Panchsheel Enclave, New Delhi - 110 017, and printed by him at M/s Archana Printers, D-127, Okhla Industrial Area, Phase-1, New Delhi 110020. Editor: Shubhendu Parth

For subscription queries, please email: subscriptions@cybermedia.co.in or send a WhatsApp message to 9289870545.

All Payments Favoring: CYBER MEDIA (INDIA) LTD
Distributors in India: IBH Books & Magazines Dist. Pvt. Ltd, Mumbai.
All rights reserved. No part of this publication be reproduced by any means without prior written permission from the publisher
Corporate Website: www.cybermedia.co.in
www.ciol.com (India's #1 IT Portal)

June 2026

[CONTENTS]

COVER STORY 24

The skinny network

Low-power networks are quietly becoming the nervous system running industrial operations, connecting sensors, machines, and AI with unprecedented efficiency.



INDUSTRY SPEAK

08 Browser-first work exposes endpoint security gaps

11 India's connectivity risks: Subsea cables and satcom gaps

14 Gaming's tax reckoning redraws industry boundaries

[TECHNOLOGY]

32 From rulebooks to reasoning: Telecom's next shift

35 Teaching wireless networks to think for themselves

38 When networks turn green, strategy follows suit

[COMMENTARY]

58 The 5G building code is being written in DAS

61 Campus networks face a test beyond bandwidth limits

66 Data quality: The bedrock of AI observability

NEWS ANALYSIS

16 Telcos and ISPs: New defensive wall against World Cup scams

TELECOM TALK



20 Telecom's sustainability shift moves from edge to core

LT. GEN. DR. SP KOCHHAR

USE CASE

45 AI + IoT + Cloud = Preventive healthcare by 2030

INTERVIEW



48 "AI sprawl is becoming the biggest enterprise risk now"

PRASANNA ARIKALA

FOCUS

52 The death of the network perimeter is rewriting security

REPORT

68 From storage box to data control tower for enterprises

72 Brain chips, AI, and virtual worlds to reshape work by 2050

REGULARS

06 Voicemail

07 Opening Note

74 Postscript

[NEXT ISSUE]



MAY 2026

Scan QR Code
& Subscribe now...



SEND YOUR FEEDBACK FOR US
TO SERVE YOU BETTER...

For **subscription queries**, please email:
subscriptions@cybermedia.co.in or
send a WhatsApp message to **9289870545**.

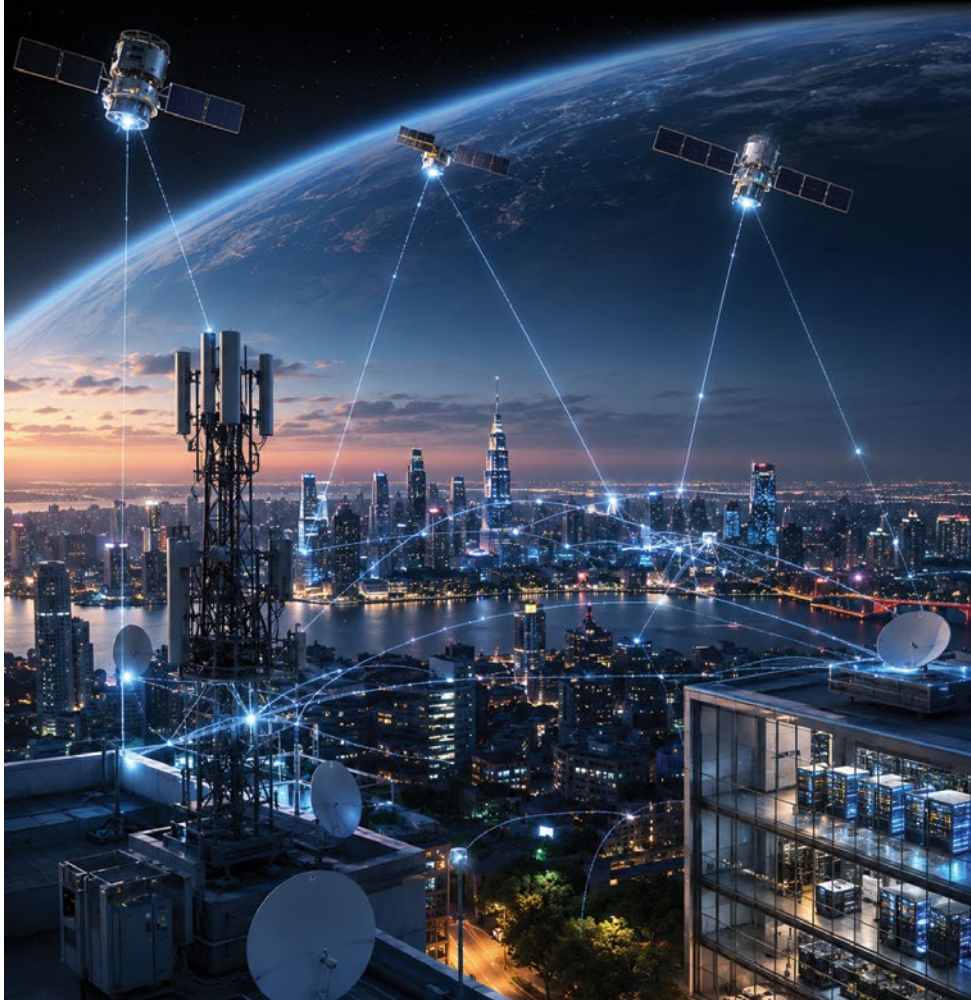
You can also write to
Reader Service Executive, **VOICE&DATA**,
Cyber House, B-35 Sector 32,
Gurgaon-122 003, Haryana
Tel: 9953150474, 7993574118



Share your views at vndedit@cybermedia.co.in

NEXT
ISSUE

SATCOM-TERRESTRIAL CONVERGENCE



For any query: ajaydh@cybermedia.co.in



SHUBHENDU PARTH [OPENING NOTE]

The AI era demands networks that think

India's telecom industry has spent the last few years building one of the world's largest digital infrastructure platforms. More than 4.78 lakh 5G sites are now operational, 5G users have crossed 250 million, and forecasts suggest that nearly 970 million Indians will be using 5G by 2030. Yet the boardroom conversation is changing. The challenge is no longer coverage. It is monetisation.

For decades, telecom networks were designed to transport data as efficiently as possible. Bandwidth, reliability and speed were the measures of success. Artificial Intelligence (AI) is now rewriting that equation. The next generation of networks will be expected not only to move data but also to support real-time computation, inference and decision-making. This is the AI and network transformation dilemma confronting operators worldwide.

The business implications are significant. Industry estimates suggest that 20% to 30% of upcoming telecom infrastructure investments could increasingly be directed towards AI-ready data centres, edge computing facilities, high-capacity fibre networks and specialised routing architectures. The reason is simple: traditional networks were built for human communications, while AI workloads are built around machine-to-machine interactions occurring at extraordinary scale.

Legacy TCP/IP-based networks can tolerate minor delays and occasional packet loss. AI environments cannot. Large language models and agentic AI systems require enormous data exchanges between GPUs, storage systems and applications, often within microseconds. This is driving demand for lossless networking technologies such as RDMA over Converged Ethernet (RoCE) and advanced optical fabrics capable of supporting high-performance AI clusters.

The shift is already visible in India. Bharti Airtel's plans for 56 edge data centres and its participation in a proposed 1 GW AI-ready digital infrastructure ecosystem in Visakhapatnam reflect a growing emphasis on compute. Reliance Jio is pursuing similar ambitions through large-scale AI infrastructure investments, including the 168 MW AI-enabled data centre project in Jamnagar. The emerging battleground is no longer connectivity alone. It is compute capacity, data gravity and AI readiness.

Edge computing will play a defining role. Applications such as autonomous mobility, industrial automation, digital payments, smart manufacturing and urban intelligence require decisions in milliseconds. Sending every transaction to a distant cloud environment introduces latency that many of these applications simply cannot tolerate. Processing must increasingly move closer to users, enterprises and machines. Telecom operators possess a natural advantage through their extensive network footprint. The question is whether they can convert that advantage into sustainable revenue.

Network slicing offers another opportunity. With 5G Standalone architectures, operators can create dedicated slices optimised for enterprise AI traffic, delivering guaranteed performance, reliability and latency. Such capabilities could transform connectivity from a commodity service into a premium digital platform.

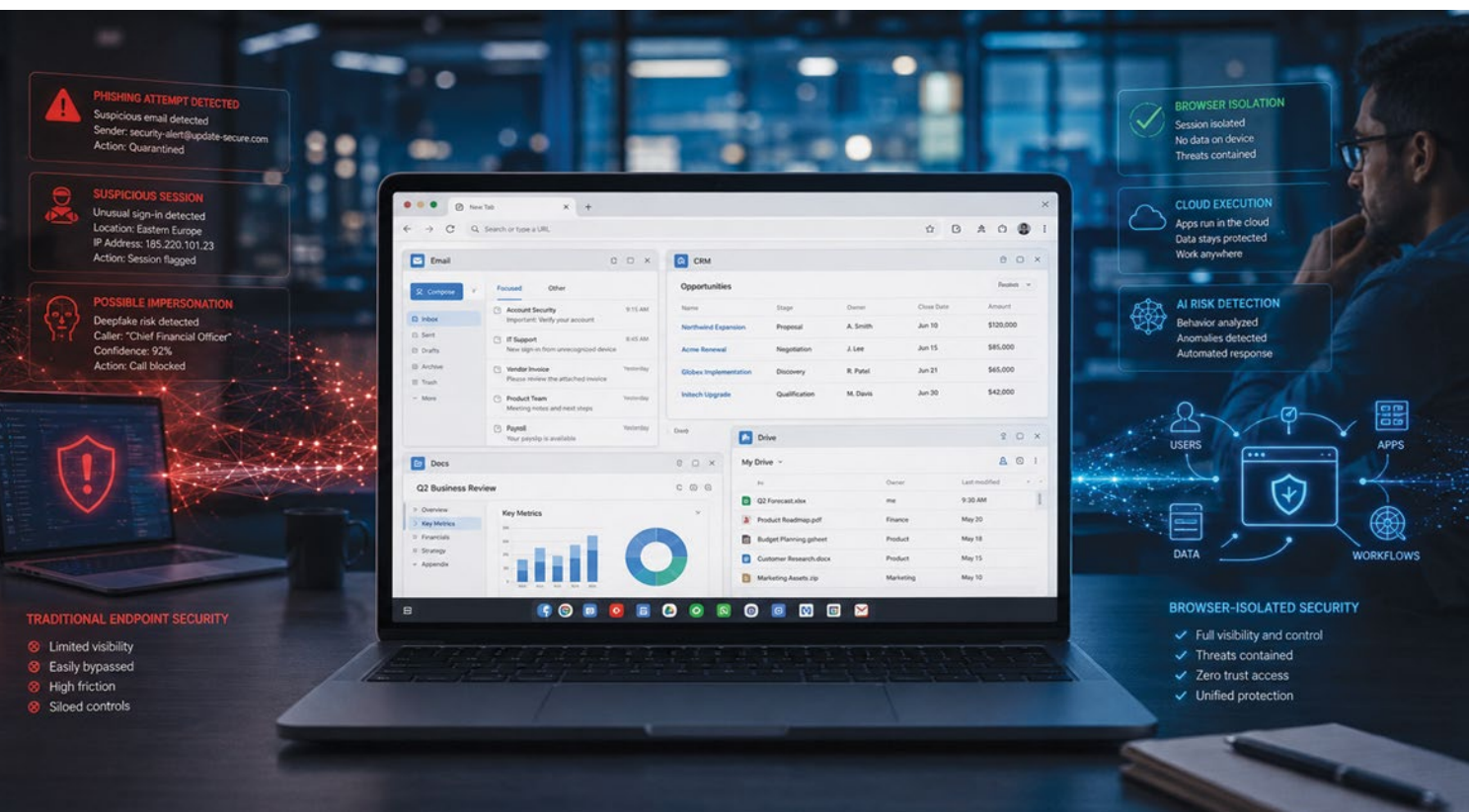
The transition, however, will demand significant investments in optical fibre, edge infrastructure, cooling systems, power resilience and intelligent network orchestration. Standing still is not an option. As India's digital economy moves from roughly 12% of GDP today towards a projected 20% by 2027, value creation is shifting upstream from connectivity to distributed intelligence.

The winners of the next decade will not be those who merely carry data. They will be those who build networks capable of helping compute it.

shubhendup@cybermedia.co.in

Browser-first work exposes endpoint security gaps

As cloud, SaaS, and AI shift enterprise work to the browser, endpoint-led security is leaving dangerous gaps across users, data, applications, and workflows.



BY SHIOUPYN SHEN

Enterprise work no longer happens primarily on the device. It happens inside the browser—across SaaS applications, collaboration platforms, dashboards, developer tools, and increasingly, AI-powered workflows. As organisations accelerate cloud adoption, the browser has effectively become the new workplace.

In India, public cloud adoption is growing at 24.3% annually, according to IDC. Yet beneath this transformation lies a widening security gap. Many organisations still treat the browser as basic infrastructure rather than a critical security control point. That assumption is becoming increasingly costly.

Security teams are finding threats faster, but many attacks still succeed because enterprise architectures give malicious activity too much room to operate.

AI-generated phishing, deepfakes and autonomous agents are exposing the limits of security models built around detection, endpoints and assumed trust.

Employees now spend most of their working hours inside browser-based applications. While the workplace has evolved rapidly, security architecture has not kept pace. Many organisations continue to believe that securing the endpoint is sufficient to secure the business.

That logic made sense when applications and data resided on managed devices. Today, however, work, data, and user interactions are increasingly browser-centric. The result is a structural security gap that organisations can no longer afford to ignore.

DETECTION LIMITS IN MODERN SECURITY

When facing an expanding threat landscape, the natural response is to double down on detection, enabling better threat intelligence, faster incident response, and more advanced monitoring. These capabilities remain essential.

However, detection-based security has a fundamental limitation: it assumes the threat has already entered the environment where it can act. Attackers have repeatedly demonstrated their ability to bypass this model.

In 2025, according to a PIB release, CERT-In handled over 29 lakh cyber incidents in India, with the I4C projecting financial losses from cybercrime exceeding Rs 1.2 lakh crore for the year. These numbers reflect more than slow detection; they highlight a deeper architectural weakness.

Modern browser-based attacks increasingly bypass traditional perimeters. Phishing, credential harvesting, infostealer malware, and malicious browser sessions often exploit trusted workflows already inside the enterprise environment. The core issue is no longer just how quickly we detect threats, but how much opportunity they have to execute in the first place.



IN BRIEF

- Enterprise work has shifted to the browser, making it a primary control point for securing users, applications, data, and AI workflows.
- Endpoint-focused security leaves gaps as phishing, infostealers and malicious browser sessions increasingly exploit trusted workflows.
- AI is accelerating cyber risk through deepfakes, impersonation attacks and autonomous agents operating inside browser environments.
- Detection remains essential, but security architectures must reduce opportunities for threats to execute rather than merely find them faster.
- Browser isolation shifts web execution to the cloud, preventing malicious code and zero-day exploits from reaching enterprise endpoints.
- Gartner expects one in four organisations to adopt secure enterprise browsers by 2028, signalling a major architectural transition.

The next security shift is not only about detecting attacks faster, but also about redesigning environments so that malicious code has fewer places to execute.

AI AMPLIFIES BROWSER SECURITY RISKS

AI is dramatically accelerating both the scale and sophistication of cyberattacks. Highly convincing phishing pages, fake approval portals, and executive impersonations can now be generated in minutes. As a result, threats are evolving faster than traditional knowledge-based detection systems can adapt to.

In India, deepfake-driven business email compromise (BEC) attacks are surging, with fraudsters using AI-generated voice and video to impersonate executives and authorise fraudulent transactions. These attacks are especially dangerous because they occur within trusted browser environments, such as collaboration platforms, finance portals, webmail, and enterprise SaaS applications. Conventional security tools often see nothing wrong.

The next wave will come from AI agents. As organisations increasingly embed autonomous agents into workflows, these systems will retrieve documents, interact with applications, and execute tasks through browser sessions. If those sessions are compromised, attackers will steal data and also influence what the agent sees, processes, and ultimately does. In other words, the attacker can move from stealing from the system to steering it.

ARCHITECTURE AS THE FIRST LINE OF DEFENCE

The most effective defence is not faster detection but designing systems in which entire categories of threats have no place to execute. This principle has long been understood in India's defence and critical infrastructure sectors: the most sensitive assets are air-gapped precisely because some things are too valuable to expose.

Browser isolation and cloud-based execution models follow the same logic. Instead of processing web content directly on the user's device, execution occurs in a controlled cloud environment. The user's device becomes a simple display terminal, receiving only rendered pixels. Any zero-day exploit or malicious code is contained within the isolated cloud

session and discarded instantly—never reaching the endpoint.

This approach is particularly valuable in India's distributed, BYOD-heavy enterprise environment, where organisations often cannot fully control every device.

MEASURING SECURITY BEYOND DETECTION

The industry has traditionally measured security maturity by how quickly threats are detected and contained. While detection remains important, a more meaningful measure is architectural resilience: how effectively systems are designed to minimise opportunities for compromise in the first place.

Gartner predicts that by 2028, one in four organisations will deploy a secure enterprise browser to address gaps in remote access and endpoint security. The forecast reflects a broader shift already underway. Browser security is no longer a niche consideration. It is becoming a foundational element of protecting modern, browser-centric work environments.

Organisations that recognise this transition early will not only strengthen their security posture but also build architectures that are inherently more resilient. Rather than continuously reacting to new threats, they can reduce the pathways through which risk reaches users, devices, and business-critical assets.

The key question enterprises must now ask is whether they are comfortable allowing untrusted web content to execute directly on devices connected to sensitive systems, data, and AI-powered workflows.

Detection will always have a vital role in cybersecurity. However, in a browser-first world, true security maturity should be measured not only by how quickly threats are identified, but by how effectively risk is prevented from ever reaching the endpoint. 🧩

*The author is the Founder and CEO
of CloudMosa.*

feedbackvnd@cybermedia.co.in



India's connectivity risks: Subsea cables and satcom gaps

As geopolitical risks grow, India must strengthen communications resilience by turning satellite connectivity from a policy ambition into a dependable backup layer.



BY TONY VERGHESE & RADHIKA GUPTA

Most of the internet does not travel through space but runs under the sea. More than 95% of international data traffic is carried through submarine fibre-optic cables that support banking, cloud services, markets, and government communications.

This largely invisible infrastructure forms the backbone of the global digital economy and is increasingly exposed in a more contested geopolitical environment. India is deeply tied to cables landing along corridors to Europe, the Middle East, and Southeast Asia, making resilience planning an urgent strategic priority.

VULNERABILITY OF SUBMARINE INFRASTRUCTURE

Submarine cables are exposed in ways that terrestrial networks are not. Accidental damage, typically from ship anchors and fishing activity, remains common. Massive data flows traverse limited routes, and many of them traverse geopolitically sensitive waters.

Recent incidents in the Baltic and Red Seas have exposed the vulnerability of communications infrastructure and prompted renewed scrutiny of resilience planning. As geopolitical tensions intensify and conflicts become increasingly unpredictable,

The greatest weakness in India's digital economy may lie far beyond its shores, where a few undersea routes carry traffic that keeps services moving for all users.



IN BRIEF

- Over 95% of international data traffic relies on submarine cables, making their security central to economic stability and national preparedness.
- Cable disruptions can affect payments, cloud services, markets and government networks, with remote and island regions facing greater risks.
- LEO satellites offer an alternative communications path, but regulatory, licensing and infrastructure hurdles limit readiness today.
- Security safeguards are essential, yet implementation delays can slow the deployment of redundancy designed to protect critical services.
- Satcom cannot replace fibre at the national scale, making clear emergency prioritisation frameworks vital during major disruptions.
- Faster spectrum decisions, gateway approvals and crisis protocols would strengthen India's communications resilience architecture.

chokepoints like the Strait of Hormuz add strategic risk to infrastructure once treated as purely commercial.

For India, a major cable cut would do far more than slow browsing. Overloaded alternate routes could raise latency across financial rails, disrupt payments and exchange operations, and impair emergency communications. Remote regions, island territories, and border areas, already sparsely connected, are especially exposed.

SATCOM: THE PROMISE VS. REALITY

Low-Earth-Orbit (LEO) satellite constellations can provide a geographically independent communications layer that is independent of subsea cable disruptions and can be deployed without laying fibre. In principle, satcom can cushion shocks by providing prioritised links for public safety, financial market utilities, and critical government users.

In practice, however, this redundancy remains largely unrealised because India's satcom ecosystem is still being operationalised.

POLICY DELAYS VS. OPERATIONAL READINESS

The Telecommunications Act, 2023, squarely brings satellite networks within the definition of telecommunication networks and shifts India to an authorisation-based framework. However, several key implementation issues remain unresolved.

The 'authorisation' framework under the Telecommunications Act, 2023, remains under active consideration, particularly on spectrum assignment methods, pricing, and coexistence conditions with terrestrial services.

Under the Unified License–Global Mobile Personal Communication by Satellite (GMPCS) framework, operators must meet stringent security conditions, including routing through Indian gateways and enabling lawful interception and monitoring.

Additional requirements, such as preventing location spoofing, mandating the use of domestic

Satellite networks promise an independent communications layer, yet policy, licensing and operational barriers continue to delay credible readiness at scale today.

navigation systems like NavIC, and ensuring continuous authentication of user terminals, add operational complexity, particularly given the borderless nature of satellite coverage.

Delays in operationalising right-of-way rules across central, state, and local bodies continue to slow gateway deployment and the scaling of supporting fibre backhaul infrastructure.

These conditions are legitimate from a national security and sovereignty perspective. However, they also increase the time, cost, and complexity required to achieve operational readiness.

Satcom in India involves broadly three bodies: the Department of Telecommunications (licensing and spectrum), the Telecom Regulatory Authority of India (recommendations), and the Department of Space/IN-SPACe (space ecosystem). While each institution plays an important role, overlapping responsibilities and sequencing challenges can delay implementation.

WHY SATCOM CANNOT REPLACE FIBRE

Even if fully operational, satcom is not a complete substitute for terrestrial or submarine infrastructure. A major terrestrial outage could generate traffic volumes that current satellite constellations are not designed to absorb at a national scale.

Even with improved LEO latency, aggregate throughput remains limited relative to the demands of hundreds of millions of users. Terminal costs, weather variability, and indigenous gateway requirements further constrain rapid scaling.

Resilience plans should clearly define emergency quality of service: who gets priority, the minimum uptime during congestion, and how nonessential traffic will be throttled.

To date, regulatory discussions have focused primarily on market access and spectrum pricing. By contrast, preparedness standards for large-scale disruptions

arising from geopolitical events or infrastructure failures remain comparatively underdeveloped.

BALANCING SECURITY AND PREPAREDNESS

Security-driven safeguards, domestic gateways, interception readiness, and governance controls are justified. However, if approval processes, compliance integrations, and audit mechanisms are not calibrated to operational timelines, the redundancy they are intended to support may not be available when it is most needed. The policy question is no longer whether satcom matters, but whether India can operationalise it before a crisis forces it to rely on it.

A pragmatic path forward would include: publishing the satellite spectrum assignment framework with clear, time-bound milestones; adopting emergency waivers that pre-authorise limited relaxation of specified license conditions during declared crises, with audit safeguards; pre-clearing mission-critical user segments and quality of service tiers; and standardising gateway and interception compliance through test plans and certification.

These steps would allow operators to scale without prolonged, case-by-case approvals.

Caution in regulating satellite communications is both necessary and understandable. However, it must be accompanied by preparedness. Publishing the spectrum framework, codifying emergency response protocols, and streamlining security compliance mechanisms would help transform satcom from a policy inspiration into a credible layer of operational redundancy for India's critical communications infrastructure.

As India's digital economy continues to expand, resilience cannot be viewed solely as a technical consideration. It is increasingly a matter of economic scrutiny and national preparedness. 🧩

Vergheese (left) and Gupta (right) are partners at JSA Advocates & Solicitors.
feedbackvnd@cybermedia.co.in



Gaming's tax reckoning redraws industry boundaries

The Supreme Court ruling on GST brings long-awaited certainty but forces online gaming firms to confront tax liabilities, regulatory scrutiny and new realities.



BY ANANAY JAIN

The Supreme Court's decision to uphold the 28% GST levy on online gaming is not just another legal call; it is a clear turning point for the industry, one that is set to reshape both its financial dynamics and the regulatory framework in which it operates.

At the core of the ruling is a firm endorsement of the government's position that, once money is put at stake in an online game, it is to be treated as betting or gambling for GST purposes. The long-standing distinction between games of skill and games of chance no longer holds weight in this context. That debate, which the industry relied on for years, has come to an end.

What began as a tax dispute has evolved into a broader industry reset, forcing operators to reassess business models, compliance and growth plans.

The ruling closes years of regulatory ambiguity, replacing legal uncertainty with a framework that could reshape the sector's future direction.

Previously, most gaming platforms argued that GST should apply only to the platform fee, basically, what they earn. But the Court disagreed and stated that tax will be applied to the total amount of the player's wager. If a user places a bet, GST is applied to the entire amount staked rather than just the portion retained by the platform.

Then, there is the larger problem of retrospective applicability. This ruling not only affects future taxes, but companies are now facing past liabilities that could exceed INR 2 lakh crore, especially once interest is included. The Directorate General of GST Intelligence (DGGI) had raised tax demands of about Rs 1.12 lakh crore against 71 online gaming companies. For many, this is not just a compliance issue but a matter of survival.

THE TAX BURDEN NOW FACING GAMING OPERATORS

From a balance sheet perspective, this becomes serious. What were once considered contingent liabilities could now require real payouts. Liquidity will tighten, and investors will re-evaluate. For smaller players, this could lead to tough decisions like restructuring, pivoting, or even exiting the market.

The Supreme Court did not stop at taxation; it also stepped into the question of state regulation. It upheld the laws brought in by Karnataka and Tamil Nadu to curb online games involving monetary stakes, overturning earlier High Court rulings that had struck them down. In effect, this provides state governments with a much stronger footing to regulate, or even restrict, such activities. The Court was quite clear on one point: the moment betting or wagering enters the equation, the debate around skill versus chance ceases to matter.

HOW REGULATION IS RESHAPING GAMING MODELS

If you step back and look at the bigger picture, this ruling is not coming in isolation. It fits into a clear policy shift we have been seeing for a while now. With the Promotion and Regulation of Online Gaming Act, 2025 already imposing limits on real-money gaming formats, the intent is clear: tighter oversight, greater accountability from players in

the ecosystem, and a much stricter stance on models driven by betting or wagering.

However, the transition will not be easy. Many companies have centred their business models around real-money gaming. Shifting to ad-based or subscription-driven models requires time, investment, and changes in user behaviour, none of which happen quickly.

From a strategy lens, this is really a "no time to wait" moment for companies. The first step is getting a clear handle on how big the tax exposure actually is, no guesswork, just numbers on the table. Then they need to get involved in the adjudication process; sitting back is no longer an option. At the same time, leadership will have to make some tough choices if they do need to adjust the current model, move into safer areas, or reduce risk altogether.

There is also the investor angle, which honestly cannot be ignored. A lot of the funding that came into Indian gaming was built around the whole "skill gaming" story. With that line now blurred, investors are likely to pause and reassess. Going forward, capital will likely become more selective, favouring platforms that are fully compliant and do not rely on wagering-based models.

One positive aspect of this ruling is the clarity it provides. For years, the industry operated in a grey area. Now, the rules are more defined. The immediate impact will be hard to absorb. There is no getting away from that, but for the first time in a while, the industry has a more defined ground to stand on as it looks to rebuild.

In reality, this extends well beyond a tax issue. It feels more like a reset. The companies that make it through will be the ones that move quickly, rethink how they operate, and realign themselves with where regulation and the market are clearly headed. 🧩

The author is a Partner and National Media and Entertainment Industry Leader at Grant Thornton Bharat.

feedbackvnd@cybermedia.co.in



Telcos and ISPs: New defensive wall against World Cup scams

The surge in FIFA-themed scams, phishing and malware campaigns is making DNS intelligence and threat sharing critical tools for operators and ISPs.



BY SHUBHENDU PARTH

The FIFA World Cup 2026 is creating another contest beyond the stadiums and across the digital ecosystem. Cybercriminals, fraudsters and hacktivists are exploiting the tournament's global appeal, turning one of the world's most popular sporting events into an opportunity for phishing, credential theft, and online fraud.

Research from FortiGuard Labs paints a picture of a rapidly expanding threat landscape. More than 13,000 FIFA-themed domains were registered between January and May 2026, with approximately 1,100 domains, or nearly 9%, identified as malicious or suspicious.

Researchers also uncovered more than 1,700 suspected FIFA-related impersonation accounts across social media platforms, with nearly 90% concentrated on Facebook and Instagram. The activity was accompanied by credential theft, fake ticketing operations, fraudulent merchandise stores, and phishing campaigns targeting job seekers and football fans.

The findings suggest that the FIFA World Cup 2026 has opened a can of worms for the internet ecosystem, creating fresh challenges for operators, internet service providers (ISPs), hosting companies and security teams tasked with protecting millions

Threat actors are using sporting brands for more than financial fraud, leveraging them for credential theft, malware campaigns and influence operations.

of users engaging with tournament-related content and services.

THE NEW CYBERCRIME LANDSCAPE

The report's findings reveal how major sporting events have evolved beyond physical venues and broadcast networks into sprawling digital ecosystems. Every ticket purchase, hotel booking, merchandise order, streaming subscription and social media interaction creates an opportunity for threat actors seeking to monetise public interest.

What makes the football tournament particularly attractive is scale. Few events generate the same combination of global attention, commercial activity and emotional engagement. Cybercriminals understand that fans are often willing to act quickly when confronted with limited ticket availability, exclusive merchandise offers or last-minute travel opportunities.

Researchers observed a sharp increase in FIFA-themed domain registrations between March and May 2026, suggesting that threat actors were actively building infrastructure to support phishing campaigns, fake ticket sales, credential harvesting and other fraud operations.

FortiGuard Labs identified fake ticketing websites designed to harvest payment information and personal data, fraudulent resale platforms promoted through Telegram channels, fake merchandise stores impersonating legitimate brands and recruitment scams targeting people seeking employment opportunities linked to the tournament.

The report also uncovered malware disguised as betting applications, livestreaming tools and FIFA-themed mobile applications. Researchers observed malicious software capable of credential theft, encrypted communications and persistence mechanisms that could allow attackers to maintain long-term access to compromised systems.

The impact extends well beyond individual fans. Sponsors, broadcasters, hospitality providers, travel operators and event partners all rely heavily on digital

platforms. A compromised account, a successful phishing campaign, or a fraudulent transaction can quickly escalate into operational disruption, financial losses, and reputational damage.

The scale of credential exposure identified in the report is particularly concerning. Researchers observed more than 270,000 credentials associated with FIFA-related web activity through stealer-log telemetry.

The report also identified more than 1,500 FIFA-associated accounts in historical breach datasets and documented the sharing of FIFA-related credentials on underground forums. Such data can fuel credential-stuffing attacks, account takeovers, and targeted phishing campaigns long after the tournament concludes.

DNS INTELLIGENCE: THE CRITICAL DEFENCE

Perhaps the most significant finding for operators and ISPs is not the number of phishing campaigns but the volume of infrastructure supporting them.

The registration of more than 13,000 FIFA-themed domains in just five months demonstrates that threat actors increasingly rely on domain-based infrastructure to support fraud operations. Ticket scams, fake streaming platforms, counterfeit merchandise stores and phishing campaigns all require domains that appear legitimate enough to deceive users.

This places DNS monitoring at the centre of cyber defence.

For many operators, DNS has traditionally been viewed as a foundational internet service. Increasingly, however, it is becoming a valuable source of threat intelligence. Monitoring newly registered domains, identifying typosquatting attempts and correlating suspicious domain activity with threat intelligence feeds can help uncover malicious infrastructure before attacks reach large numbers of users.

The report identified recurring patterns involving FIFA branding, ticketing terminology, betting services, streaming platforms and hospitality-related keywords.

The FIFA World Cup has turned operators from connectivity providers into active defenders against large-scale digital fraud across the wider internet ecosystem.

What Keeps the Service Providers Awake

Threat Category	Infrastructure Impact
Malicious Domain Proliferation	Large volumes of FIFA-themed domains place a burden on DNS monitoring, threat detection, and abuse management systems.
Phishing Infrastructure	Fraudulent websites hosted across multiple providers create challenges for rapid identification, takedown and blocking.
Credential Exposure	Stolen credentials fuel account takeovers, credential stuffing attacks, and the long-term compromise of digital services.
Typosquatting Domains	Attackers register lookalike domains that exploit user trust while evading basic security controls.
Infrastructure Reuse	Criminal groups reuse hosting assets, SSL certificates and IP resources across campaigns, complicating attribution efforts.
Cloud Service Abuse	Legitimate cloud platforms are leveraged to host malicious content and conceal attacker activity within normal traffic.
Malware Distribution Networks	Fake apps, streaming platforms and downloads use distributed infrastructure to spread malware at scale.
Social Media Impersonation	Fake accounts drive traffic to malicious domains and fraudulent services, amplifying the reach of attacks.
Coordinated Fraud Ecosystems	Multiple phishing, ticketing and merchandise scams often operate as interconnected campaigns rather than isolated incidents.
Encrypted Malicious Traffic	SSL-encrypted communications make inspection and detection more difficult for network operators.
Threat Intelligence Gaps	Slow sharing of indicators across providers allows malicious infrastructure to remain active longer.
Hacktivist Influence Operations	World Cup narratives are exploited to spread disinformation, alleged data leaks and reputational attacks.

Source: Based on info from Source: FIFA World Cup 2026: Cyberthreat Landscape Report (2026). FortiGuard Labs; Fortinet.

Such indicators can be used to build detection models that identify potentially malicious infrastructure at an early stage.

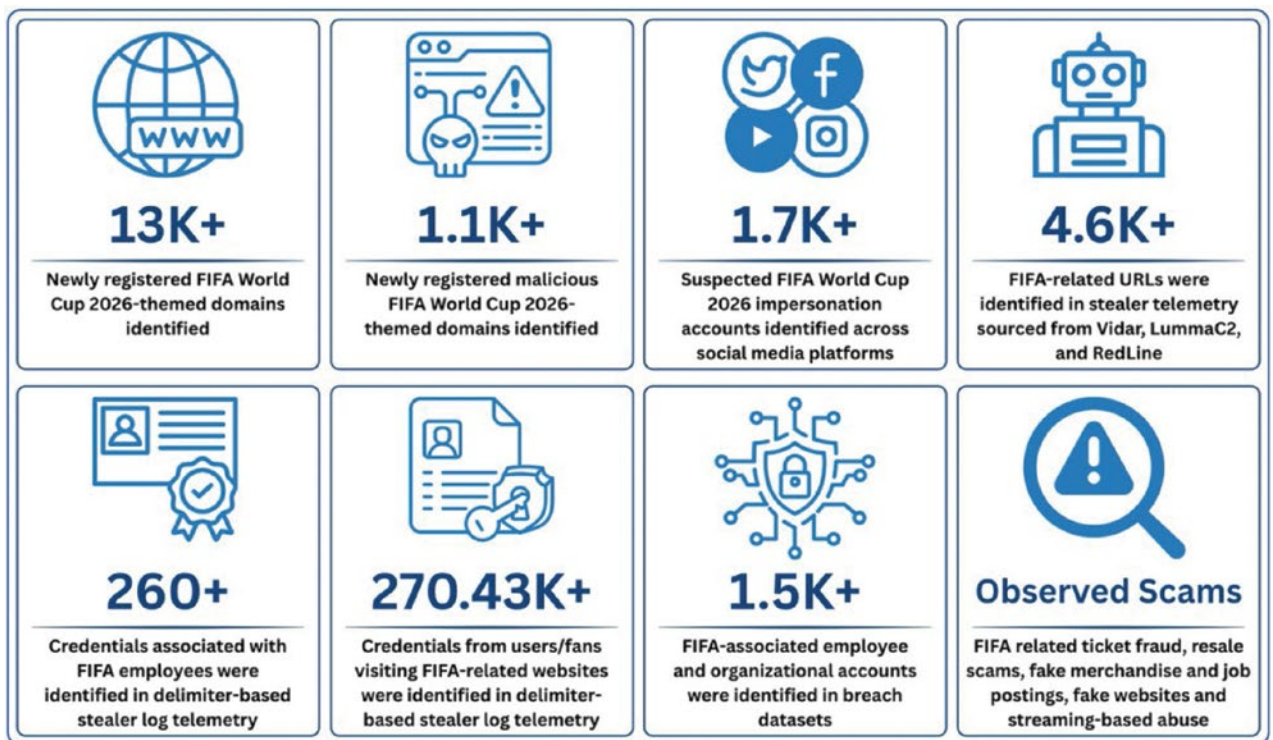
Equally important is passive DNS intelligence. By analysing relationships between domains, IP addresses, SSL certificates and hosting environments, operators can identify broader campaigns rather than responding to individual threats in isolation.

The report’s case studies demonstrated repeated infrastructure reuse, overlapping hosting resources and domain clusters linked to phishing and malware operations.

These patterns highlight the value of intelligence-driven defence rather than reactive blocking.

OPERATORS AND HOSTING PROVIDERS MATTER
The findings also reinforce the growing role of digital infrastructure providers in combating cybercrime. Researchers identified phishing websites and credential-harvesting portals hosted on cloud infrastructure, while several campaigns leveraged legitimate online services to blend malicious activity with normal internet traffic. In some instances, multiple FIFA-themed phishing domains appeared linked through shared tracking identifiers, suggesting coordinated operations rather than isolated scams.

FIFA-Themed Cyberattack Infra



Source: FIFA World Cup 2026: Cyberthreat Landscape Report (2026). FortiGuard Labs; Fortinet.

In several cases, attackers abused legitimate cloud-hosted services and application platforms to conceal malicious communications and credential-harvesting activity. The approach makes malicious traffic harder to distinguish from legitimate activity, creating additional challenges for operators, cloud providers and hosting companies.

For hosting providers, this creates pressure to improve abuse detection, accelerate takedown procedures and collaborate more closely with cybersecurity researchers. The faster malicious infrastructure can be identified and removed, the fewer opportunities attackers have to exploit unsuspecting users.

Threat intelligence sharing is equally important. Indicators such as malicious domains, suspicious IP addresses, phishing infrastructure and credential theft campaigns become significantly more valuable when shared across operators, cloud providers, security vendors and government agencies.

The report also notes that FIFA-related themes are being used beyond traditional cybercrime. Researchers observed hacktivist activity that leveraged World Cup-related narratives to amplify anti-government messaging

and draw attention to alleged data leaks. While not directly targeting tournament infrastructure, such activity illustrates how globally recognised events can be exploited for influence operations and reputational attacks.

The significance of the report lies not simply in the number of malicious domains, impersonation accounts or phishing campaigns identified. They reveal how globally recognised events increasingly function as cybercrime marketplaces where threat actors compete for credentials, financial information and user trust.

For telecom operators, ISPs and hosting providers, safeguarding users now extends beyond connectivity and network availability. It requires visibility into malicious infrastructure, rapid intelligence sharing and coordinated efforts to disrupt fraudulent activity before it reaches victims.

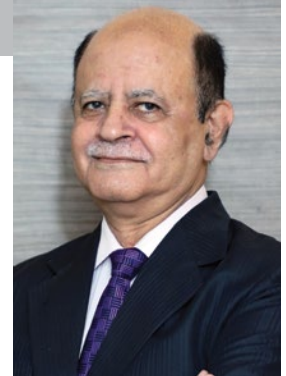
FIFA World Cup 2026 may be football's biggest tournament, but it is also becoming a test of how effectively the internet ecosystem can respond when cybercriminals attempt to exploit global attention at scale. 🧨

shubhendup@cybermedia.co.in

LT. GEN. DR. SP KOCHHAR

TELECOM'S SUSTAINABILITY SHIFT MOVES FROM EDGE TO CORE

As AI and 5G accelerate digital expansion, telecom networks are evolving into cleaner, smarter and more energy-aware systems.



India is currently building one of the largest digital infrastructure ecosystems anywhere in the world. Every month, millions of consumers, enterprises, and public services are becoming increasingly dependent on mobile connectivity, cloud platforms, AI-enabled applications, and real-time digital networks.

Yet, the defining challenge before the telecom industry is no longer only about expanding connectivity. It is about ensuring that India's digital growth story is also sustainable by design.

This transition is already underway. Across the sector, telecom operators are investing in renewable energy-powered towers, energy-efficient 5G infrastructure, AI-led network optimisation, green data centres, and smarter infrastructure-sharing models. Sustainability is no longer being treated as a parallel ESG objective. It is increasingly becoming central to network architecture, operational efficiency and long-term digital resilience.

This shift is important because the future of digital India will not be determined only by how fast networks



Telecom leaders of the next decade will be defined not only by coverage and capacity, but by how intelligently they use networks and conserve energy at scale.



The telecom industry is discovering that sustainability is no longer a peripheral ESG ambition but a defining principle of future-ready network design.

expand, but by how intelligently and responsibly they evolve.

THE TRIPLE EFFICIENCY DIVIDEND

The next phase of telecom evolution can be understood through what may be called the “Triple Efficiency Dividend”, where modern telecom networks simultaneously deliver energy efficiency, infrastructure efficiency and economic efficiency.

#1

ENERGY EFFICIENCY

Telecom operators globally, including in India, are deploying smarter, greener network architectures that consume less power per unit of data transmitted.

Advanced 5G equipment, AI-enabled network optimisation and intelligent sleep modes are significantly improving energy efficiency. Studies and operator disclosures increasingly show that while overall data traffic is growing exponentially, energy consumption is not rising proportionately because networks are becoming far more efficient.

Globally, telecom vendors such as Ericsson and Nokia are integrating AI-driven energy-saving capabilities and intelligent radio systems into network operations. This transition matters because energy remains one of telecom operators’ highest operational costs. Sustainability, therefore, is increasingly aligned not only with environmental priorities but also with long-term operational resilience.

#2

INFRASTRUCTURE EFFICIENCY

India’s telecom sector has long been a global example of infrastructure optimisation through shared telecom infrastructure models. Tower sharing, fibrilization, network virtualisation, and green data centre investments are helping reduce asset duplication while improving network scalability. Shared telecom infrastructure itself is an underrated sustainability success story. By enabling multiple operators to utilise common passive infrastructure, the industry has reduced energy-intensive duplication across the network ecosystem.

India’s growing adoption of cloud-native and software-defined network architectures will further strengthen infrastructure efficiency in the coming years.

#3

ECONOMIC EFFICIENCY

Sustainable telecom infrastructure is also improving economic viability, particularly in rural and remote deployments. Hybrid energy systems combining solar power, batteries and grid connectivity are reducing dependence on diesel generators and lowering operational expenditure. This is especially critical in geographically challenging or power-deficient regions where telecom connectivity plays a vital developmental role.

Increasingly, sustainability investments are becoming business enablers rather than compliance obligations.

INDIA’S GREEN TELECOM TRANSITION

India’s telecom industry has already embedded sustainability into large parts of its operational strategy. Operators are actively investing in renewable energy adoption, energy-efficient network modernisation, battery innovation and green infrastructure deployment.

Bharti Airtel, for example, has solarised over 30,700 telecom tower sites with more than 170 MWp of rooftop solar capacity. Airtel has also indicated that solar and battery deployments are helping save nearly two million litres of diesel every month. Its data centre arm, Nxtra, has also strengthened its renewable energy commitments through partnerships to add over 200 MW of renewable power capacity, reinforcing the role of green data infrastructure in India’s digital future.

Reliance Jio, supported by Reliance Industries’ new broader energy ambitions, is also scaling renewable-powered telecom infrastructure and energy-efficient digital architecture as part of its net-zero vision for 2035.

Vodafone Idea has expanded renewable energy sourcing while investing in captive solar infrastructure to improve operational sustainability. BSNL too is exploring renewable-powered telecom deployments and hybrid energy solutions to strengthen rural connectivity infrastructure.

India's digital infrastructure ambitions may depend not only on network speed and scale, but also on how intelligently systems consume and conserve energy.

Collectively, these initiatives demonstrate that India's telecom industry is proactively aligning digital growth with sustainability goals.

AI AND 5G SUSTAINABILITY PARADOX

One of the defining realities of the digital era is that AI and 5G simultaneously increase energy demand while also becoming the tools that optimise energy consumption.

AI workloads, cloud services, edge computing and immersive digital applications will undoubtedly require higher network capacity and computing power. However, AI is also helping telecom operators build more intelligent, energy-aware networks.

AI-enabled traffic management, predictive maintenance, dynamic spectrum optimisation and automated network management are already improving operational efficiency across telecom systems.

Tomorrow's greenest network may not simply be the one powered by renewable energy, but the one intelligent enough to consume only the energy it truly needs. Globally, telecom companies are already using AI-driven radio optimisation and intelligent sleep modes to reduce network energy consumption during low-traffic periods significantly. Future 6G standards are also increasingly being designed around sustainability-by-design principles, ensuring that efficiency remains central to future digital infrastructure.

TELECOM'S ROLE BEYOND TELECOM

The telecom sector's sustainability contribution extends well beyond reducing its own environmental footprint. Digital connectivity itself is becoming one of the strongest enablers of economy-wide sustainability.

Telecom networks support smart grids, precision agriculture, remote healthcare, intelligent logistics, smart manufacturing and digital governance systems. Every digitally enabled efficiency can potentially reduce resource consumption and carbon intensity elsewhere in the economy.

A digitally connected healthcare consultation reduces travel emissions. Intelligent logistics reduces fuel

consumption. Smart agriculture improves the efficiency of water and fertiliser use. Smart energy systems optimise electricity distribution.

In this sense, telecom networks are not merely a communication infrastructure. They are becoming sustainability infrastructure. A sustainable digital economy cannot exist without sustainable digital infrastructure.

INDIA'S OPPORTUNITY TO LEAD

India is uniquely positioned to become a global leader in sustainable digital infrastructure. Unlike many mature markets that must retrofit decades-old systems, India still has the opportunity to scale large parts of its future telecom infrastructure with sustainability embedded from the outset. The country's strong renewable energy ambitions, expanding digital ecosystem and rapid 5G rollout together create a powerful foundation for green telecom leadership.

Importantly, supportive policy measures are also accelerating momentum. Recent reforms enabling telecom operators to aggregate loads for renewable energy procurement represent an important step toward improving access to clean energy for telecom infrastructure at scale.

The telecom industry remains committed to working collaboratively with policymakers, technology providers and infrastructure partners to advance India's sustainable digital vision.

The next phase of India's digital leadership will not be defined only by the scale of connectivity we build, but by how responsibly and intelligently we build it. Sustainable telecom networks will play a defining role in ensuring that India's digital future is both inclusive and environmentally responsible. 🌱

The author is a decorated military veteran who retired as the Signal Officer-in-Chief, the head of the Indian Army's ICT division. He was also the first CEO of the Telecom Sector Skill Council and is the Director General of the Cellular Operators Association of India (COAI).

feedbackvnd@cybermedia.co.in

[illegible]

**A cultural movement about edited intelligence
in an age of infinite information**

**A constant stream of unobserved update
overwhelms Judgement.**

Editing and curating Information converts it
into insight.

READ LESS. KNOW MORE.

“An Initiative by Association of Indian Magazines”

THE SKINNY NETWORK



Low-power networks are quietly becoming the nervous system running industrial operations, connecting sensors, machines, and AI with unprecedented efficiency.

BY PRATIMA HARIGUNANI

Picture this. PERI GmbH SE, a specialist in formwork and scaffolding systems in Weissenhorn, Bavaria, was facing daily challenges in construction work across 70+ countries, especially in recording the deployment or storage locations of formwork elements more quickly and precisely.

It found its answer in a combination of two IoT tracking systems. The first one for tapping Long-Term Evolution for Machines (LTE-M), NB-IoT, or 2G devices connected to Telekom's IoT Cloud, showing which part is on which construction site. The second one uses Bluetooth Low Energy to show the exact position of the formwork elements on the site.

The company can now gain an up-to-date overview of rented parts, improve stock management, and pinpoint exact delivery times for customers.

Then there is a Northern Irish startup, CreevX, that automates legionella (a bacteria that poses a serious

health risk when water sits unused in pipes for extended periods) compliance (Regulations such as the UK's HSG 274 require building operators to monitor water temperatures) in commercial buildings.

It was a manual process, but this company uses IoT sensors and automated flushing via an IoT device that monitors water temperatures every 15 minutes (which also automatically flushes stagnant water through the pipes, if needed). The connectivity here uses LoRaWAN to communicate with a gateway, which then transmits data to the cloud.

Such use cases point to a specific new need emerging in the industry: simply having IoT for collecting intelligence at the periphery will not suffice unless those smart sensors and things are also lean, thin, and low-power, bandwidth- and connectivity-wise. In short, it is a great time for LPWAN, NB-IoT, and Reduced Capability (RedCap) to serve enterprises with a very different appetite.

Industrial intelligence now needs sensor ecosystems that run for years on minimal power while continuously feeding field data into AI systems at enterprise scale.



“RedCap broadens the 5G ecosystem by balancing performance, cost and power use, making broadband IoT more accessible for low-power industrial devices today.”

RANDEEP SINGH SEKHON

Chief Technology Officer, Bharti Airtel



IN BRIEF

- LPWAN, NB-IoT and LTE-M are enabling large-scale sensor networks with low power consumption and long device lifecycles.
- Predictive maintenance, asset tracking and smart utilities are driving sensor deployments from pilots to core operations.
- RedCap bridges the gap between low-power IoT and full-scale 5G, balancing performance, cost and energy efficiency.
- Industrial sensors, wearables and surveillance devices are emerging as key early use cases for 5G RedCap.
- Hybrid connectivity architectures are becoming essential as enterprises combine high-bandwidth and low-power applications.
- Security, interoperability and IT-OT integration remain major barriers to scaling connected industrial ecosystems.

As Deutsche Telekom shares, overall, the adoption of Low Power Wide Area (LPWA) technologies took off several years ago. “We continue to see high growth in the use of NB-IoT/LTE-M connectivity. The technologies NB-IoT/LTE-M have technically matured (higher performance/feature set) and are a fixed basis of the future 3GPP roadmap,” explained a company spokesperson.

The adoption is only accelerating, points out Bernd Otto Hormann, CEO, MHP India. Sensor ecosystems are becoming the backbone of industrial intelligence by providing continuous visibility across assets, processes, and environments. At the same time, low-power connectivity technologies enable efficient scaling of these deployments.

“At MHP, we see strong momentum in predictive maintenance, energy optimisation, and supply chain visibility. These use-cases are moving from pilots to business-critical applications,” he explained.

Low-power industrial connectivity technologies such as LPWAN, NB-IoT and emerging 5G RedCap solutions are enabling large-scale sensor ecosystems across both industrial environments and autonomous platforms, says Karan Shah, Chief Financial Officer, Jyoti Global Plast.

“These technologies allow organisations to deploy large numbers of connected sensors that can operate for extended periods while monitoring equipment, environmental conditions and operational parameters. In UAV systems, sensors are central to mission capability,” he points out.

Today, modern drones rely on integrated sensor suites that combine electro-optical imaging systems, navigation sensors, environmental sensing modules and telemetry systems to support functions such as surveillance, terrain mapping, obstacle avoidance and situational awareness.

Kunal Bajaj, CEO and Co-Founder, CloudExtel, affirms that direction. “We are clearly seeing a rise in the adoption of advanced sensor ecosystems, driven by use cases like predictive maintenance, smart utilities, and automated logistics. Technologies such as LPWAN and NB-IoT are gaining strong traction because they offer long battery life and the ability to connect large numbers of devices across wide areas, making them ideal for applications like asset tracking, metering, and environmental monitoring.”



“RedCap bridges high-end 5G and low-power IoT by reducing device complexity while retaining lower latency, slicing and positioning advantages for enterprises.”

JOE BARRETT

President, Global Mobile Suppliers Association

Specific verticals, such as smart utilities, benefit greatly from the capabilities of low-power devices. The Smart Gas and Water Metering application segment could account for 25.8% of the LPWAN market revenue in 2025, according to Future Market Insights. Moreover, regulatory requirements are pushing for better resource management and leak detection. This is where real-time data collection facilitated by LPWAN allows utilities to optimise consumption, billing, and maintenance activities.

REDCAP ENTERS THE INDUSTRIAL MAINSTREAM

The most interesting name in this slim basket is RedCap. It is basically 5G shrunk down for the small spoon and the diet of IoT use cases. Something that stands on the bridge between full-blown 5G and low-power IoT set-ups. It is a streamlined form of 5G that addresses cost-sensitive and mid-tier applications such as wearables, industrial sensors, and surveillance devices.

5G NR-Light addresses use cases that fall between the high-speed enhanced mobile broadband (eMBB), the ultra-reliable low-latency communications (uRLLC), and the low-throughput, battery-efficient massive machine-type communications (mMTC) technologies.

It offers comparable latency to existing 4G LTE technologies, which is much lower than that of most LPWA technologies, such as NB-IoT. It can still support applications that require higher data throughput.

5G RedCap, standardised in 3GPP Release 17 with enhancements as eRedCap in Release 18, serves as a strategic mid-tier connectivity solution, enlightens Joe Barrett, who has been President of the Global mobile Suppliers Association (GSA) since 2015, driving its position as the leading global industry association for mobile suppliers.

“It bridges the performance gap between high-end 5G New Radio (NR) capabilities—such as enhanced Mobile Broadband (eMBB) and Ultra-Reliable Low Latency Communications (uRLLC)—and the ultra-low-power,

REDCAP GATHERS PACE

- 30 operators in 21 countries are actively investing in RedCap deployments.
- Commercial launches are underway with operators including T-Mobile (US), China’s major telcos, STC (Kuwait), and Dito (Philippines).
- Vendor support is expanding rapidly, with Huawei, Nokia, Samsung, TCL, and ZTE strengthening RedCap portfolios.
- Six RedCap chipsets and more than 20 devices are already available, with the ecosystem expected to grow further.
- eRedCap, introduced in 3GPP Release 18, promises lower complexity, reduced power consumption, and lower device costs.
- GSA expects RedCap to become the leading mid-tier IoT connectivity option, bridging LTE and full 5G before eRedCap reaches scale.

Source: GSA 5G RedCap Report, April 2025

low-data-rate massive Machine-Type Communications (mMTC) technologies like NB-IoT and LTE-M,” Berrett says.

Earlier, in an exclusive interview with Voice&Data, Randeep Singh Sekhon, Chief Technology Officer for Bharti Airtel, had clearly stated that the introduction of RedCap, or reduced-capability devices, by 3GPP marks a significant milestone in the evolution of the 5G ecosystem.

“This technology is designed to leverage 5G’s wide-scale deployments with fewer functionalities, offering an optimal balance between performance, cost, and power consumption. RedCap broadens the scope of 5G, making it more accessible for IoT and low-power devices, bridging the gap between cost and performance for delivering broadband IoT services,” he stated.



“Low-power connectivity allows large sensor networks to monitor equipment, environments and mission data with better visibility, safety and consistency at scale.”

KARAN SHAH

Chief Financial Officer, Jyoti Global Plast

LPWAN'S GROWTH STORY

- The global LPWAN market is projected to expand from USD 16.9 billion in 2025 to USD 973.1 billion by 2035.
- Smart cities, industrial automation, and remote monitoring are driving demand for long-range, low-power connectivity.
- Smart gas and water metering remain among the fastest-growing LPWAN applications, supported by utility digitisation efforts.
- Advances in network infrastructure, energy-efficient devices, and cloud-based platforms continue to accelerate adoption.
- Asset tracking, predictive maintenance, and distributed IoT deployments are expanding LPWAN use across industries.
- Network hardware currently accounts for 30–35% of deployment costs, while end devices contribute 25–30% and software platforms 15–20%.
- By 2035, hardware and device costs are expected to decline significantly, driven by miniaturisation, efficiency gains, and smarter edge devices.

Source: Future Market Insights

As Barrett explains, by simplifying device architecture, RedCap significantly reduces cost, complexity, and power consumption while preserving essential 5G Standalone (SA) benefits. “These include lower latency than LTE, network slicing, improved positioning, and efficient coexistence with other 5G traffic on the same carrier. RedCap is specifically designed to enable a cost-effective migration for LTE Cat-1 to Cat-4 devices as 4G networks are gradually phased out.”

Additional 5G-native advantages include access to new 5G spectrum bands (easing pressure on 4G

networks), network slicing for guaranteed quality of service, and enhanced power-saving features such as extended DRX. These characteristics position RedCap as an ideal “Goldilocks” technology for mid-tier use cases.

He further highlights that RedCap is emerging as an important addition to this mix, Bajaj also observes. “It effectively bridges the gap between high-performance 5G and low-power IoT by supporting mid-range devices such as cameras, wearables, and industrial sensors in a more cost- and power-efficient way. The advantages are quite compelling, including scalability, energy efficiency, and the flexibility to deploy in hard-to-reach or infrastructure-light environments.”

In Sekhon’s reckoning, RedCap can support video transmission for traffic monitoring and security cameras in smart cities, enhancing urban safety, better patient care in healthcare through wearables and the use of industrial wireless sensors powered by RedCap in manufacturing to monitor machinery conditions such as temperature, pressure, and vibration, improving operational safety and efficiency.

Airtel had conducted successful trials of RedCap devices in collaboration with Ericsson, and Sekhon was quite optimistic as he shared, “We are also exploring using 5G network slicing to create dedicated virtual networks for RedCap devices, ensuring that specific KPIs and SLAs can be met when required. This will enable us to optimise resource allocation for different use cases, ensuring that RedCap integrates smoothly while maintaining the overall network performance,” Singh shared.

Connectivity frameworks such as 5G and RedCap can enhance capabilities by enabling the real-time transmission of imagery, sensor data, and flight telemetry to ground control stations. At the same time, LPWAN and NB-IoT networks can support wider sensor ecosystems, such as infrastructure monitoring, perimeter sensing, or distributed operational networks, with minimal power consumption, according to Shah.



“LPWAN, NB-IoT and RedCap are gaining traction because they connect large device fleets across wide areas with long battery life and deployment flexibility.”

KUNAL BAJAJ

CEO & Co-Founder, CloudExtel

As Marco Contento, VP of Telit Cinterion, explained, the development of 5G RedCap provides a balance between performance and efficiency, which is critical for operations utilising applications such as industrial sensors, smart wearables, and video surveillance. “For devices that do not require ultra-low latency or ultra-high speed, it is also a cost-effective alternative to full 5G New Radio (NR). Because IoT devices often have long life cycles, selecting forward-compatible technologies is essential to protecting long-term investments. RedCap or LPWA options like LTE-M and NB-IoT are preferable.”

Deployment of 5G RedCap requires a 5G Standalone core, Barrett points out. “As of March 2026, the GSA identified 184 operators in 76 countries and territories investing in 5G SA—representing 29% of all operators engaged in any form of 5G activity. For RedCap specifically, GSA reports 42 operators across 27 countries actively investing. The breakdown of investment status shows steady progress.

“In fact, multiple operators have commercially launched services. Several are in the process of deploying or planning. A significant portion remains in trial or evaluation phases,” he adds.

CHALLENGES BENEATH THE CONNECTIVITY BOOM

There is another side to the charm of this lean and lithe category. There are practical challenges that need to be addressed, Bajaj points out. “These include fragmentation across device ecosystems, ensuring reliable indoor coverage, and integrating operational technology data with enterprise IT and analytics platforms securely and seamlessly.”

Yes, the complexity should not be underestimated, echoes Hormann. “Legacy environments, fragmented IT and OT landscapes, and diverse protocols continue to create integration challenges. Cybersecurity and capability building are also critical considerations.”

Shah also reveals that from a manufacturing perspective, the current use of such technologies within organisations like Jyoti Global Plast is more focused on monitoring and verifying precision manufacturing parameters and maintaining process consistency, rather than large-scale industrial sensor networks.

Organisations must address challenges such as secure communications, power constraints for long-endurance UAV missions and integration with existing command and control systems, Shah underlines.

What is becoming clear is that there is no single connectivity approach, reminds Hormann. “High-bandwidth applications such as machine vision coexist with low-power sensor networks. This leads to hybrid architectures that are designed around use cases rather than technology preferences. The focus for organisations should be on ensuring that sensor data is fully integrated into digital platforms, where it can be leveraged through analytics and AI to deliver tangible outcomes.”

While the rise of connected devices is cause for applause, the security concerns it brings are not, Contento had shared, explaining the flip-side of this new wave. “The potential attack surface grows with each new connected device. This requires enterprises to implement strong encryption, authentication protocols and zero-trust network architectures to safeguard their deployments.”

We must actively develop the RedCap ecosystem to realise this vision and address any roadblocks hindering its mass adoption. Some of the key practices that need to be followed for RedCap devices include secure boot, over-the-air updates to address vulnerabilities, and the use of secure hardware components, Sekhon also emphasised.

BUILDING LEANER INDUSTRIAL NETWORKS

As Bajaj captures, in the future, the real opportunity lies in bringing these technologies together into a unified,



“The real value comes when sensor data is integrated with digital platforms, analytics and AI to create scalable, business-critical outcomes across industry.”

BERND OTTO HORMANN
CEO, MHP India

WHY REDCAP MATTERS

RedCap is designed for devices that sit between high-performance 5G and low-power IoT, offering a balance of throughput, latency, power efficiency, and cost.

Key Technical Characteristics

- Supports a maximum 20 MHz channel bandwidth in sub-6 GHz spectrum, reducing device complexity and power consumption.
- Uses simplified radio architecture with fewer antennas and lower baseband processing requirements than standard 5G devices.
- Supports half-duplex FDD operation, helping extend battery life in power-sensitive deployments.
- Can deliver peak downlink speeds of up to 220 Mbps, significantly higher than most LPWA technologies.
- Maintains access to key 5G capabilities such as network slicing, improved positioning, and lower latency.
- Enables a smoother migration path for LTE Cat-1 to Cat-4 devices as operators transition towards 5G Standalone networks.
- The next evolution, eRedCap, is expected to reduce further device cost, complexity, and power requirements for mass-market IoT deployments.

Why It Fills a Critical Gap?

Traditional LPWA technologies prioritise battery life and coverage, while full-scale 5G targets high-performance applications. RedCap occupies the middle ground, making it suitable for devices that need moderate throughput, mobility support, and longer operational life without the cost burden of premium 5G hardware.

service-led architecture that can support diverse industrial needs without adding complexity.

From MHP's standpoint, the key is to approach this transformation with clear priorities, Hormann shares. “Focus on high-impact use cases, drive standardisation across interfaces and data models, and build architectures that can scale over time.

Private 5G plays an important role, but only as part of a broader industrial ecosystem that combines connectivity, edge, cloud, and strong IT-OT integration. Organisations that take this integrated approach will be the ones that unlock real value from automation and AI.”

Hormann reveals how organisations can gain efficiency, flexibility, and transparency as they move closer to autonomous, self-optimising operations. “These technologies form the foundation for resilient and future-ready industrial systems.”

The advantages of these technologies cannot be ignored, especially around greater operational visibility, improved data-driven diagnostics and the ability to scale connected systems across both manufacturing environments and deployed UAV platforms, opines Shah.

We see continuing growth in the number of LPWA networks globally, according to Deutsche Telekom. “The convergence of terrestrial and satellite networks (NB NTN) will increase geographical coverage further. From a customer perspective, the LPWA connectivity product is already at an attractive/competitive price level, particularly in the German market.”

If this is not slow, many IoT use cases will be eager to leverage this new force, especially for enterprises that need data measurement and processing at the edge. XS could be the new X-factor. 🌟

Source: GSA

pratimah@cybermedia.co.in

PCQUEST MAY 2026 EDITION INDIA PLAYS. BUT WHO OWNS THE GAME?

ALSO READ MORE ON

- How AI is reshaping games and the designers who build them
- Why mobile apps must defend themselves in real time
- How AI and biometrics are redefining high-stakes examination infrastructure
- AI debt is the real GenAI trap • Inside India's evolving esports growth engine
- 7 most anticipated games of 2026
- Your gaming laptop choice might already be outdated
- REVIEW: EvoFox Deck 2 | OnePlus Nord Buds 4 Pro | Mini UPS for AirFiber V3.0



Scan QR Code
& Subscribe now...

PCQUEST IS OFFERING
SPECIAL DISCOUNTS
FOR **NEW SUBSCRIBERS**
AND ITS READERS.
AVAIL THE OFFER NOW

Link: <https://bit.ly/3QvNQh8>

FOLLOW PCQUEST FOR THE REGULAR
UPDATES ON TECH AND TRENDS

 @pcquest  @pcquest  @pcquest

Leverage PCQuest platform & network. Write to:
Ajay Dhoundiyal | ajaydh@cybermedia.co.in | +91 99535 40318



For Subscription queries::

 subscriptions@cybermedia.co.in

 9289870545

From rulebooks to reasoning: Telecom's next shift

As 5G, cloud, and edge technologies increase network complexity, operators are adopting AI-driven systems that predict, adapt, and act with minimal oversight.



BY GP. CAPT. CS KRISHNADAS (RETD)

For years, traditional networks have relied on predetermined rules with manual oversight for traffic management, uptime maintenance and failure resolution. This worked well in the past when networks were simpler in design, and the services they provided were fundamentally limited to voice and data.

Today's telecom infrastructure, however, must support a much more complex digital enterprise, driven by 5G, cloud computing, the Internet of Things (IoT), edge technology, and real-time enterprise applications.

Having launched 5G about three years ago, India now has about 400 million 5G subscribers, second only to China, and 4.69 lakh 5G base stations installed across the country. With the expansion of telecom and networking infrastructure across urban areas and developing markets,

business-level telecom and networking operators today also face increased challenges in managing their fibre-based networks, distributed infrastructures, edge environments, and ever-growing service demand.

In addition, the need for continuous connectivity across multiple sectors is becoming critical to achieving business success. Today's networks require high reliability and high speed.

FROM AUTOMATION TO AGENTIC NETWORKING

To succeed in this space, the traditional methods of automating telecom networks will no longer work. As companies around the world deploy across multiple geographic locations and increase interconnection across infrastructure layers, operators require telecom systems capable of providing immediate responsiveness, continuous flexibility, and a high degree of low-touch operations.

Telecom networks can no longer rely solely on fixed scripts, as 5G, cloud, IoT, and edge workloads demand faster decision-making across complex environments.

Thus, the telecom industry is on the path towards what is being referred to as Agentic Networking. Unlike traditional automated platforms, where goal interpretation is performed by programmers configuring scripts for every possible scenario, Agentic AIs will allow the operator to define their objectives, and the AI will determine the best way to achieve them.

This also means that it is no longer necessary for operators to develop a workflow for each possible scenario. Agentic AIs can automate all workflows required to achieve an operator's goals.

This transforms the way telecommunications infrastructure operates by moving away from reactive processes toward proactive, intelligent systems that continually monitor the network for performance disruptions, evaluate their potential impact, and make real-time decisions about how best to proceed.

The result: the network becomes a self-learning, self-adapting ecosystem that continually evaluates itself, learns from its historical behaviours, anticipates future problems, and adjusts contextually in real time.

In healthcare, reliable communication networks are critical to the success of medical procedures such as robotic surgeries and emergency care, as delays of even a few seconds due to network congestion can impair performance. Thankfully, automated networks can now identify when traffic is too high, reroute it to avoid disrupting critical services, and keep essential services operating with no delays.

As telecom infrastructure has become more intelligent, networks are also getting better at handling outages with minimal disruptions. In the event of a fibre breakage that cuts off communication between two endpoints, AI agents will autonomously identify alternative routing options, redistribute workloads, and restore the network to its original stable state.

The AI agents are also able to coordinate activities across the radio access network (RAN), core and cloud layers to perform corrective workflows in near real time,



IN BRIEF

- Telecom networks built for voice and data are struggling to keep pace with the scale, speed and complexity created by 5G, cloud and IoT.
- Agentic networking replaces rigid, pre-programmed workflows with systems that can interpret goals and determine how best to achieve them.
- AI agents can identify faults, reroute traffic and coordinate corrective actions across RAN, core and cloud layers in near real time.
- Intelligent operations can reduce outage detection and resolution times, improve service quality, and lower operational costs.
- As edge computing expands, autonomous coordination across distributed infrastructure will become critical to maintaining performance.
- Human expertise will remain essential for governance, security and accountability as networks assume greater operational autonomy.

frequently before a support ticket has been created. This results in decreased wait times for repairs and allows the customer to operate without any disruption.

INTELLIGENT NETWORKS FOR THE ENTERPRISE ERA

Today, businesses are increasingly relying on systems that process information faster, helping reduce delays

Agentic networking lets operators define the outcome while AI selects the route, triggers workflows and resolves faults before disruption spreads.

and improve response times. At the same time, managing large, interconnected systems manually becomes increasingly difficult as telecom networks continue to expand. Agentic AI can be of help here. It can reduce workload coordination across the edge, cloud, and network layers without a drop in performance.

According to a report by STL Partners, by the end of this decade, edge computing could reach USD 424 billion in global revenue, and companies are already transitioning to decentralised computing for their business processes across areas such as smart factory operations, logistics systems, and urban areas with interconnected networks.

The tech is helpful for telecom providers, too. Today, telecom companies are facing growing network demand and rising customer expectations while trying to keep costs under control. Managing large telecom networks can also become complex and time-consuming. Intelligent network systems help simplify this by detecting problems early, automating routine processes and improving overall network performance.

A report published by Shah Zeb and Shahrukh Khan Lodhi in *Enrichment Journal* shows that AI-driven network operations could reduce outage detection and resolution times by nearly 40–50%. This would help companies reduce maintenance costs by identifying issues early and resolving them faster.

For instance, if a large telecom network experiences a sudden outage, issues such as call drops or slow internet speeds can affect millions of users within an instant. Faster, more intelligent network systems can help operators identify problems early and reduce service disruptions before they worsen.

As businesses become more dependent on digital operations, the need for faster, more reliable networks is increasing. Today, companies expect seamless connectivity that can respond quickly and support real-time operations, whether in manufacturing, retail, logistics, or healthcare.

In this climate, telephone companies are exploring new AI-based techniques to optimise traffic flow and

the potential to deliver differentiated services via 5G network slicing.

BUILDING FUTURE TELECOM INFRASTRUCTURE

The role of telecommunications professionals remains critical as engineers increasingly move into higher-level functions such as strategic planning, governance, security, compliance, infrastructure development and delivery of intelligent network services.

While AI will increasingly automate operational functions across multiple devices at scale, the utility of human judgement will be required to ensure that intelligent systems have appropriate levels of accountability and can be relied on as legitimate service providers to all customers.

The digital ecosystem in India is rapidly expanding as businesses move more services online and consumers rely on connected technologies in their everyday lives. The growing need for faster, more reliable telecom networks continues to expand across multiple sectors, such as smart city infrastructure, connected devices, and cloud-based businesses. Industry estimates suggest India's digital economy will contribute nearly USD 1 trillion to the country's GDP by 2030. If so, it will create sustained demand for intelligent telecom and networking infrastructure.

To meet demand, telecom infrastructure must deliver the speed of next-generation connectivity technologies and the capability to intelligently and adaptively manage a complex telecommunications environment.

The future of telecom and networking requires expanding connectivity footprints and enabling intelligent network environments capable of scalable operations. As the connectivity of digital ecosystems grows, network technologies must increasingly self-optimize, self-heal and respond automatically to support the growth of telecommunications. Agentic Networking is a key step here, essential for creating a new telecom ecosystem that is resilient, responsive, and adaptable. 🧠

*The author is the Chief Executive Officer of
Umiya Buildcon.
feedbackvnd@cybermedia.co.in*



Teaching wireless networks to think for themselves

As 5G Advanced and 6G take shape, AI-native design is becoming essential for wireless systems that learn, adapt, and optimise across network conditions.



BY HOUMAN ZARRINKOUB & MIKE MCLERNON

The wireless industry is experiencing an unprecedented surge in demand, with more than 7.1 billion human mobile users and a growing number of wireless machine-to-machine (M2M) connections.

While the key challenge engineers face when designing wireless systems and networks is their complexity, traditional predefined designs are inadequate or inflexible for handling it. They are also unadaptable when requirements and environments change.

Founded on the principle of learning and adaptability, emerging AI-native technologies promise to address the complexity challenge. The wireless standard organisation, 3GPP, has been vocal about AI's significant role in the forthcoming 5G Advanced and 6G standards. They propose using AI to enhance positioning, beam management, and Channel State Information (CSI) feedback.

The Wireless Broadband Alliance (WBA) also touts AI for its ability to help wireless engineers in indoor positioning and beam management. The industry consensus is clear: engineers must integrate AI-native concepts to stay ahead in the next-gen wireless system race.

WHY AI-NATIVE WIRELESS SYSTEMS MATTER

An AI-native wireless system inherently incorporates AI algorithms into its operational framework. AI-native systems offer three primary benefits for wireless engineers: better coverage, higher capacity, and reliable robustness.

AI-native wireless systems are designed to learn from and adapt to their environment. This approach differs significantly from traditional designs based on more rigid, predefined models, which have scalability limitations and often require costly, time-consuming signal processing resources.

The shift to AI-native wireless design marks a fundamental departure from fixed architectures, enabling networks to learn and adapt in real time at scale now.



IN BRIEF

- AI-native wireless systems can improve coverage, capacity and resilience by learning from changing network conditions.
- Digital twins are helping engineers generate training data and simulate scenarios that are difficult to recreate in real networks.
- Building AI-native networks requires a structured workflow covering data, training, implementation and integration.
- Synthetic and real-world datasets are both critical for training AI models that can perform reliably in production systems.
- Engineers must balance throughput, latency and energy efficiency when optimising AI-enhanced wireless networks.
- AI-native technologies are expected to play a central role in the forthcoming 5G Advanced and 6G wireless standards.

Engineers designing AI-native systems need large, real-world, measured data sets. Most of this data is sourced from physical prototypes or by measuring real-world signals. However, most engineers use digital twins—the representative virtual models that can be simulated—to augment data to train AI-native systems.

Digital twins ensure that AI-native systems have sufficient data to handle adverse situations and efficiently manage system elements.

BUILDING AI INTO WIRELESS NETWORKS

Developing an AI-native wireless system is a complex

process that involves creating a design workflow encompassing data gathering, model training and testing, and integrating the model into the wireless system.

#1

GATHERING AND GENERATING DATA

The first step in creating an AI-native wireless system involves data collection, by either acquiring over-the-air (OTA) signals or synthesising data from a digital twin.

Synthetic data is especially useful, as it facilitates scalability testing, fault tolerance, and anomaly detection, while also aiding in environment modelling and system configuration optimisation.

Maximising model efficiency requires that the training data be representative of the real-world scenarios the system will encounter. Engineers can use the collected data to perform training and validation of AI models, testing and simulation, and optimisation and performance tuning. With the gathered data, the next step is simulation and modelling.

#2

TRAINING AND TESTING MODELS

When training an AI model for a wireless system, it is essential to determine the quantity of system parameters, including bandwidth allocation, latency, signal strength, modulation, and coding.

Using these parameters and the comprehensive dataset obtained in the first step, the engineer selects and optimises machine learning algorithms for key system functions like autoencoders, channel estimation, channel feedback optimisation, and resource allocation.

During training, engineers must consider factors that affect real-time performance, including computational complexity, memory usage, and parallel processing on GPUs or clusters.

After an AI model is trained, the model is tested to ensure reliable performance in real-world systems. At this stage, the model's performance is iteratively adapted to correct for biases, errors, and inefficiencies.

The success of 6G may depend less on radio innovation and more on how deeply AI is embedded into network operations, design workflows and control systems.

Once the adaptation is complete, the AI network should be pruned. Pruning involves converting the model to a fixed point and removing the neural network layers that do not contribute to the system's overall behaviour. At this stage, the model is ready to be implemented in the wireless system.

#3

IMPLEMENTING THE AI MODEL

An AI model is only useful when it is implemented within a real-world system. The first step involves scaling and resource assessment. This involves evaluating the processing power, memory requirements, and data throughput needed for the AI models to operate efficiently.

The second step is to use automatic code generation for deploying pretrained AI models on desktop or embedded targets using low-level code. This step automates the implementation process and reduces manual coding errors.

The final implementation step is the validation process that compares the performance of the implemented system to that of the original AI model. After engineers have identified and addressed discrepancies or performance issues, they are ready to integrate the model.

#4

INTEGRATING THE MODEL

The final step is to integrate the implemented AI models into the overall wireless system. This phase ensures that the newly implemented AI solution works harmoniously with the rest of the legacy system.

Before full-scale integration, engineers must ensure interoperability with existing system components by analysing the end-to-end system performance rather than individual algorithms and subsystems.

OVERCOMING AI INTEGRATION CHALLENGES

Integrating AI into wireless systems presents a variety of hurdles, including balancing conflicting performance metrics and ensuring superior performance relative to legacy systems. The goal is to achieve a balance that supports operational objectives by delivering high-quality overall performance.

In a typical design scenario, optimising one metric often compromises another, making it crucial to find an acceptable balance that meets the system's overall goals. For example, increasing the network's throughput may lead to higher power consumption and latency, necessitating a trade-off to maintain energy efficiency.

Engineers can use modelling and simulation to explore various scenarios and configurations to balance the desired metrics. This predictive approach helps make informed decisions and identify optimal configurations without disrupting the actual system.

DELIVERING BETTER WIRELESS PERFORMANCE

Transitioning from legacy wireless systems to AI-enhanced systems without disruption is challenging, but essential for achieving superior performance. AI models that continuously learn are key to this transition, as they enable the system to adapt to dynamic network conditions. Achieving superior performance requires training models using diverse, representative datasets.

One solution is to simulate the integrated system before full-scale deployment to ensure AI components will interoperate properly with legacy systems. The use of such tools may also facilitate interoperability testing and help in identifying potential compatibility issues and performance bottlenecks.

The wireless industry is at a critical juncture. With the upcoming rollout of 5G Advanced and 6G standards, the next generation of wireless systems will deploy more AI-native technologies. Engineers tasked with designing modern wireless systems have realised that integrating AI is no longer optional; it is essential. By incorporating AI-native design principles, wireless engineers can develop systems and networks that meet today's needs and are equipped to evolve with tomorrow's wireless requirements and advancements. 🧩

Zarrinkoub (left) and McLernon (right) are the Principal Product Manager and Principal Technical Marketing Engineer, respectively, at MathWorks.
feedbackvnd@cybermedia.co.in



When networks turn green, strategy follows suit

As energy costs rise and AI drives power demand, telecom operators are embracing renewables to strengthen resilience, efficiency and future growth.



BY PRATIMA HARIGUNANI

This May, the Ukrainian telecom service provider Kyivstar announced the completion of its acquisition of six solar power plants in the Lviv region, marking renewable energy as a new revenue stream. Interestingly, the expected annual output from its renewable energy portfolio could

be equivalent in volume to around 30% of the company's current annual electricity consumption across its telecom operations.

According to media reports, many cellular phone towers in Africa powered by diesel generators are

Renewable energy is becoming a boardroom priority as telecom operators seek lower costs, greater resilience, and tighter control over future growth paths.



“Sustainability has become integral to how networks and data infrastructure are designed, powered, and managed, with digital demand scaling across India at a rapid pace.”

PANKAJ MALIK

CEO, Invenia-STL Networks

switching to solar power amid the current fuel crisis. Consider the example of Atlas Tower Kenya, which could invest USD 52.5 million to construct 300 new solar-powered telco towers to serve operators such as Safaricom, Airtel, and Telkom Kenya.

Airtel Africa, Vodacom Africa, and MTN are also opening their windows to the sun to increase solar energy use.

Note how BT claims that over the last eight years it has cut global energy consumption by 20%, mainly through rationalising and upgrading buildings and networks, and reducing electricity and gas consumption.

It also achieved a 52% cut in operational carbon emissions and a 30% cut in full value emissions since FY17, and aims to be net zero by the end of March 2031. It pushed towards the supply of renewables in the grid through several long-term Power Purchase Agreements (PPAs), which met 31% of its UK electricity demand in 2025.

There is also Telefonica in this zone, which has announced the use of renewable energy, achieving 100% in its main markets and reducing energy consumption by 12% despite strong growth in data traffic. The company has indicated that it has cut its total emissions by 49% over the last decade, moving closer to its goal of net-zero emissions by 2040.

Meanwhile, in the Netherlands, KPN signed the UN Compact 24/7 Carbon Free Energy (CFE) last year, with the resolve to use only sustainable electricity 24/7 as part of its goal to be Net Zero by 2040. It shared that it has reduced its energy consumption by 43% and has sourced some of its electricity directly from a solar park operated by Eneco.



IN BRIEF

- Renewable energy is moving from a sustainability initiative to a strategic business imperative for telecom and data centre operators.
- Operators are deploying solar, wind and hybrid energy systems to lower costs, reduce emissions and improve energy resilience.
- AI, growing data traffic and expanding digital infrastructure are increasing power needs, accelerating the shift towards renewables.
- Energy efficiency gains in RAN equipment, cooling systems and infrastructure design are making renewable adoption more practical.
- Data centres face mounting pressure to combine sustainability goals with rising electricity demand from AI-intensive workloads.
- Regulatory mandates, investor expectations and market requirements are making green energy adoption a competitive necessity.



“Renewables appear compelling, but AI’s growing dependence on electricity means sustainability ambitions must confront the deeper power challenge at scale today.”

ALESSANDRO GALIMBERTI

VP Analyst, Gartner



TELCOS’ GREEN IMPERATIVES

- Telecom networks rank among the largest industrial consumers of electricity.
- 5G densification and AI workloads are driving higher power requirements.
- Energy accounts for a significant share of telecom operating expenditure.
- Diesel-dependent backup systems face fuel-price and supply-chain volatility.
- Renewable power provides greater long-term cost predictability.
- Energy security is becoming as important as network security.
- Investors and regulators increasingly expect measurable decarbonisation progress.
- Sustainable infrastructure is emerging as a competitive differentiator.
- Renewable integration supports both resilience and business continuity.
- Green energy is shifting from a compliance goal to a strategic necessity.

Since 2011, KPN has also been purchasing certificates to fully offset its annual energy consumption. It aims to move towards a completely fossil-free energy supply and to have its electricity come from sustainable sources at every hour of the day, as stated in its reports and announcements.

The solar park Kabeljauwbeek appears to provide 10% of KPN’s energy needs, with 100% of its energy completely emission-free, with a CFE score of 10%. From January 2027, KPN intends to take a significant portion of energy from the wind farm Ecowende to supply 50% of KPN’s energy needs.

Closer home, we can see Nxtra, the data centre company from the Bharti Airtel group, showing many strides in its Sustainability report 2025. It has contracted 482,800 megawatt-hours (MWh) of renewable energy across nine states and reduced Scope 2 emissions by 9% compared to FY21, despite a 26% increase in electricity use, as the company highlighted.

When we hear about these examples and other telecom majors like Vodafone and Deutsche Telekom tapping AI for energy optimisation, real-time energy monitoring, predictive equipment maintenance, and streamlining operations and emissions, it no longer sounds surprising.

When we read about Orange and T-Mobile moving towards shared RAN infrastructure, it seems like ‘about time’. Telefonica, Swisscom, Tele2, KPN, Turkcell, Telia, Liberty and Telecom Italia have all been joining the green club in their own ways- solar, hybrid and self-generated power on their cell sites. MTN Consulting also reported in 2025 that renewables accounted for 23% of global telco energy consumption in 2024, up from 10% in 2019.

It makes sense for Telcos to dial down on non-renewables. Especially now.



“For CSPs, renewables are now essential to reduce energy costs and emissions at scale, without affecting network KPIs, service quality, or customer experience.”

SHANTHI RAVINDRAN

Principal Analyst – APAC, Appledore Research Group

The industry consumes a lot of energy, and most invisibly so, as it keeps digital connectivity running smoothly and seamlessly across various geographies. Estimates show that telcos spend an average of 4–5% (MTN Consulting) or 10–15% (GSMA Intelligence) of their operating expenses on energy.

In 2024, telcos consumed 340.6 terawatt-hours (TWh) of energy (according to an MTN Consulting report). Just the backhaul parts, air-conditioning, inverters, rectifiers, and repeaters of RAN and base stations make a big slice into the energy consumption of any telco.

Asia's electricity consumption is forecast to grow at an average of 4.4% per year over 2025-2034, according to the latest APAC Data Centre report by BMI, driven by the rapid electrification of transport and industry, expanding data centre demand, and enabling policy measures.

Across Asia (including China), it is expected that wind and solar power will provide the bulk of incremental generation over the next decade, supported by rapid renewables build-out and growing storage systems. “Many South East Asian economies are already actively reducing their LNG dependency, where the US-Iran war will only accelerate this shift away from LNG and towards renewables,” notes Alex Kheder, TMT Analyst, BMI.

The goals of energy efficiency and green network operations, as Shanthi Ravindran, Principal Analyst – APAC, Appledore Research Group explains, are embedded strategic priorities with most Communications Service providers (CSPs), with a goal of increasingly shifting to renewables, reducing carbon emissions over a period and a long-term net zero goal, leading with change in the data centres first.



ROADBLOCKS TO TRANSITION

- Intermittent solar and wind generation requires storage or hybrid systems.
- Grid infrastructure is often inadequate for large-scale renewable deployment.
- High upfront capital investment remains a key barrier.
- Land acquisition can constrain renewable-energy projects.
- Legacy infrastructure slows technology and energy transitions.
- Growing AI demand is increasing pressure on power availability.
- Renewable sourcing remains uneven across markets and regions.
- Policy support and financial incentives vary significantly.
- Reliability expectations leave little room for energy disruptions.
- Sustainability goals must be balanced against commercial realities.



“Renewable integration is now an operational necessity for data centres, but AI workloads make balancing power reliability, cooling, and storage harder at scale.”

PINKESH KOTECCHA
CMD, Ishan Technologies



GREEN LEADERS

- Switzerland leads the GSMA Intelligence Green Network Index with a score of 73.
- Sweden and Spain follow closely, benefiting from strong renewable adoption and energy-efficiency programmes.
- European operators dominate the sustainability rankings.
- High-scoring markets combine renewable energy use with strong network performance.
- Countries with cleaner power grids generally achieve better sustainability outcomes.
- Asia performs strongly on coverage, availability and latency metrics.
- However, Asia's average renewable-energy factor remains just 25%.
- Rapid network expansion is outpacing power-sector decarbonisation in many Asian markets.
- Renewable adoption is emerging as a key differentiator among telecom operators.

She cites Singtel in Singapore, which has an internal carbon pricing, embedding a price on carbon into all significant capex decisions as a financial governance mechanism. “Maxis in Malaysia even sells a Home Solar subscription enabling green energy beyond its own network.”

The green path is not a detour or a merry hike. It is a serious pivot. Here's why.

WHY RENEWABLES ARE BECOMING ESSENTIAL

Telcos and renewables are aligning in ways and strategic reasons that have become significant in the current landscape.

Take Energy management, which, as Ravindran notes, is of paramount importance to them because of their geographically distributed networks, the increasing demands from complex generations of 3GPP technology, variability of energy consumption with load (idle/peak), demands from new technologies like AI, both at cell sites and at large data centres.

John Strand, CEO of Strand Consult, reckons that the green transition is being discussed by many and that green energy will play a central role in many parts of the world. “I come from Denmark, which is considered one of the leading nations in green energy.”

Ravindran points out that most of CSPs' energy consumption occurs in the RAN. “Vendors of base stations have worked diligently on silicon, site solutions, standards and algorithms, shutdowns, sleep modes, at the RF, baseband, site and network levels, to find methods to keep reducing the power consumption (Watts/Gb) enough to make a shift to renewables possible. CSPs and Tower companies adopt solar hybrid deployments for off-grid towers, with intelligent cooling (sensors and ambient air/liquid cooling) to reduce consumption.”



“Green energy will play a central role worldwide, but telecom operators need stronger national grids to transport clean power to where it is really needed today.”

JOHN STRAND
CEO, Strand Consult

Telcos can find revenue colours on this green path too. Consider how KPN and Google sometimes receive more sustainable power from their solar and wind parks than they can use, and at other times receive too little. They have entered into exchange pacts to help each other to run on sustainable sources for more hours of the day. KPN, Google and Eneco have started a pilot project to exchange surpluses of sustainable electricity.

“The telecom and data centre sectors in India are now adopting more energy-efficient and sustainable infrastructure models. As digital demand scales, sustainability has become integral to how networks and data infrastructure are designed, powered and managed,” points out Pankaj Malik, Chief Executive Officer of Invenia-STL Networks.

He further shares that across the ecosystem, there is growing adoption of renewable energy integration, intelligent power management, advanced cooling technologies and more efficient infrastructure architectures.

The telecom industry and Indian data centre sector are steadily leaning towards renewable energy, largely driven by rising energy consumption, sustainability commitments, and the growing demand for AI-ready digital infrastructure, echoes Pinkesh Kotecha, Chairman and Managing Director, Ishan Technologies.

According to a recent JLL report, India’s data centre capacity is expected to surpass 1.8 GW by 2026, with sustainability and renewable energy integration emerging as key priorities for operators. “As data centres continue to become among the largest power-consuming assets within the digital ecosystem, renewable integration is no longer just an environmental consideration but also an operational necessity.”

Underscoring how renewables have shifted from a compliance burden to a market-access requirement,

Kheder cites Singapore’s DC-CFA2, which mandates at least 50% green energy sourcing, and Mainland China, which requires 80% renewable sourcing for new data centres from 2026, backed by subsidies that cut energy costs by up to 50%.

“Equinix’s PUE below 1.4 in 2024, alongside a 10% reduction in Scope 1 and 2 emissions, illustrates how sustainability performance now actively reduces pipeline resistance,” he points out.

Malik spots how, from large-scale data centres to distributed telecom infrastructure, the focus today is on building environments that deliver high operational resilience and energy efficiency at scale. “The next phase of digital infrastructure growth will depend on assets that are scalable, resilient and optimised for long-term sustainability.”

“We are witnessing a strong shift towards energy-efficient infrastructure, intelligent cloud ecosystems, and optimised computing environments. Our Tier 3 Mumbai Data Centre has been designed with energy-efficient architecture to support high-performance workloads while reducing operational inefficiencies.” Kotecha illustrates.

THE CHALLENGES BEHIND THE TRANSITION

Strand notes the bumps in this green road. “What we can see is that the biggest challenge today is the quality of the national grids, the networks that are used to transport green energy around the country. In countries such as Denmark, the Netherlands, Germany and the United States, they have major challenges when it comes to transporting the electricity to where it is needed.”

As to India, Strand opines, “To put it very simply, India is also facing major challenges in this area. The challenges with mobile infrastructure have been solved. Today, India has access to better 5G infrastructure than it has in Europe, where, unlike India, Chinese infrastructure

The race to greener networks is increasingly driven by economics, as operators balance energy security, AI demand, rising traffic and profit pressures at scale.

is used. Subsea cables are being considered, and I am sure India will find a solution in that area as well. When it comes to energy, I think India is facing significantly greater challenges than you admit. I cannot imagine how much money will be invested in new energy infrastructure in India in the next 10 years.”

Malik avers that while challenges remain around renewable energy availability, grid readiness and upfront investments, the long-term direction is clear. “The industry is moving toward greener, more intelligent infrastructure with a sharper focus on efficiency, reliability and lifecycle performance.”

Kotecha identified issues such as intermittency, new burdens, and greater capacity pressures. “Renewable infrastructure requires substantial upfront investment, especially for large-scale data centres operating 24/7. Intermittency in solar and wind energy can create reliability concerns without adequate storage or hybrid power systems.”

He further shares that data centres also require extensive cooling and water resources, which can increase pressure on local infrastructure if not managed responsibly. “As AI workloads grow, balancing sustainability with rising power demand will remain one of the industry’s biggest challenges.”

WHERE THE GREEN OPPORTUNITY EXPANDS

As captured by GSMA Intelligence’s GNI report 2026, Countries with high renewable penetration and strong efficiency metrics tend to perform well across the board, and their advantage is widening as others struggle with basic electricity availability, grid dependency, and regulatory delays.

The biggest upside of renewable adoption in telecom and data centres, as Kotecha affirms, is long-term operational sustainability. “It also strengthens resilience as enterprises increasingly prioritise green and compliant digital infrastructure.”

Tellingly, the move towards renewables is still not pervasive and deep. Imagine the state when the top 10

by renewable adoption are all in Europe: Turkcell, Tele2, Telia, DT, KPN, Swisscom, A1 Telekom Austria, Telefonica, Telecom Italia, Liberty Global.

The study also identified some laggards, such as telcos, where electricity accounts for about 90% of total energy use, with relatively high shares of diesel and other direct energy sources, and renewables accounting for less than 10%. Examples include Charter Communications, Comcast, Etisalat, Grupo Televisa, Lumen Technologies, Millicom, MTN Group, Ooredoo, PLDT, Rostelecom, STC, Turk Telekom, Veon, and Zain.

The geopolitical wind towards renewables – while apparently a big nudge – is exactly not that strong or well-sprawled. Alessandro Galimberti, VP Analyst, Gartner, reminds us how the cloud was once also a sustainability step, promising enterprises the vision of saving environmental burden by moving to a shared infrastructure. “It was a big tick box.

Similarly, the current scenario may look like a good reason to lean towards renewables, but would it be easy? AI is a dominant force in many technology investments, and it depends on electricity for so much of its capacity.” He points out an inherent dependency that cannot be ruled out that easily.

Ravindran opines that as we continue to consume more spectrum and deliver higher data rates, energy costs remain a significant share of CSPs’ operating costs. “A shift to renewable energy is a must to reduce costs and, from an environmental perspective, without affecting KPIs and services.”

The renewable push can definitely go deeper and greener. Telcos could find better pastures ahead by achieving higher operational efficiency, energy independence, affordable energy, and new revenue opportunities by joining the renewables league. If someone were thinking of changing the stove, the timing could not be better. The front-burner is waiting. 🍳

pratimah@cybermedia.co.in

AI + IoT + Cloud = Preventive healthcare by 2030

As connected devices, analytics and digital platforms mature, care delivery is shifting from treatment-led models to continuous health management.



BY SURJEET THAKUR

The healthcare system is changing rapidly, driven by advances in artificial intelligence (AI), the Internet of Things (IoT), and cloud computing. A Statista report indicates that 40.6 billion IoT devices will be connected by 2030, with a growing share coming from

healthcare applications such as remote monitoring, smart diagnostics, and connected medical devices.

Today, healthcare is becoming proactive rather than reactive, providing patients with data-driven, holistic,

The convergence of connected devices, intelligence and scalable platforms is creating a healthcare model built on foresight, prevention and wider access today.

A wearable can now do more than track activity. Combined with analytics, it can anticipate health risks and trigger timely interventions for patients.

and preventive medical care rather than waiting to treat them until they develop an illness or condition.

improve patient outcomes, and reduce long-term treatment costs.

BUILDING CONTINUOUS PATIENT CARE MODELS

IoT is at the heart of the ongoing transformation of healthcare, enabling the continuous, real-time capture of patient health data. Wearable devices such as activity trackers, biosensors, heart-rate monitors, and other connected medical devices are no longer used solely for fitness purposes. They are increasingly being deployed as clinical tools to monitor vital parameters such as heart rate, blood pressure, oxygen saturation, blood glucose levels, and respiratory patterns beyond traditional healthcare settings.

By enabling continuous monitoring, IoT allows healthcare providers to move beyond episodic consultations and adopt a more proactive, data-driven approach to patient care through ongoing remote supervision.

This has accelerated the adoption of Remote Patient Monitoring (RPM), enabling physicians to track patients' health in real time, identify potential issues earlier, intervene when necessary, and improve clinical outcomes. RPM also helps reduce hospital readmissions while easing the burden on healthcare systems.

TURNING HEALTH DATA INTO INSIGHT

AI is turning the vast volumes of data generated by the Internet of Things (IoT) into actionable health insights. Rather than replacing clinicians, AI is augmenting their capabilities by converting real-time and historical patient data into actionable insights that support better decision-making. By analysing large datasets, machine learning algorithms can identify patterns, detect anomalies, and predict potential health risks before they become critical.

This predictive capability lies at the core of preventive healthcare. AI can help physicians identify early warning signs of chronic conditions such as diabetes, cardiovascular disease, and respiratory disorders long before symptoms become clinically evident. Early intervention can slow disease progression,

AI is also enhancing diagnostic accuracy. Trained on extensive radiology, pathology, and clinical datasets, AI models can help clinicians detect abnormalities in medical images and other diagnostic data with greater speed and precision. This enables faster, more informed clinical decisions, supporting improved patient care while reducing the likelihood of diagnostic errors.

SCALING HEALTHCARE THROUGH CLOUD

Cloud computing is a critical enabler of both AI and IoT in healthcare, providing the infrastructure needed to connect, manage, and scale the entire digital health ecosystem. By offering a secure environment for storing, processing, and sharing vast volumes of healthcare data in real time, cloud platforms enable healthcare stakeholders to access the information they need, when they need it.

As healthcare organisations increasingly integrate data from multiple sources and deploy AI applications at scale, cloud infrastructure becomes indispensable. It supports a unified view of patient information, enabling seamless data exchange, real-time analytics, and faster clinical decision-making. This enhanced visibility improves care coordination and contributes to better patient outcomes.

Cloud computing also provides the scalability required to manage the growing volume of healthcare data without compromising performance, reliability, or security. Equally important, it supports interoperability—the ability of diverse healthcare systems and applications to communicate and exchange information effectively—which is fundamental to connected healthcare delivery.

In India, initiatives such as the Ayushman Bharat Digital Mission are strengthening the country's digital health infrastructure by promoting standardised health records, interoperability, and seamless access to healthcare services. Together, cloud, AI, and IoT are laying the foundation for a more connected, efficient, and patient-centric healthcare ecosystem.

The next leap in healthcare may come from prediction rather than treatment, with algorithms identifying risks before symptoms become visible to doctors now.

FROM MONITORING TO EARLY ACTION

The true transformation in healthcare is emerging from the convergence of IoT, AI, and cloud computing. IoT devices continuously collect patient health data, cloud platforms securely store and manage this information, and AI analyses the combined datasets to identify patterns, predict risks, and recommend appropriate interventions. Together, these technologies create a continuous feedback loop that makes healthcare more intelligent, responsive, and patient-centric.

This integrated approach enables healthcare providers to move beyond reacting to illness and towards anticipating it. By identifying risk factors early and triggering timely interventions, connected healthcare systems can help prevent complications before they escalate into serious medical conditions.

A practical example is the use of wearable devices that continuously monitor vital signs such as heart rate, blood glucose levels, blood pressure, or oxygen saturation. The data is transmitted to cloud-based platforms, where AI algorithms analyse trends and detect anomalies. If a potential health risk is identified, alerts can be sent instantly to both the patient and healthcare provider, enabling prompt action.

For instance, combining Continuous Glucose Monitoring (CGM) systems with AI can help predict fluctuations in blood sugar levels before they reach dangerous thresholds, allowing patients to take preventive measures. Similarly, AI-enabled cardiac monitoring systems can detect abnormal heart rhythms or out-of-range heart rates in real time and immediately notify healthcare professionals, improving the chances of early intervention and better clinical outcomes.

PERSONALISED, PREVENTIVE, ACCESSIBLE CARE

The convergence of AI, IoT, and cloud computing is accelerating the shift towards personalised healthcare. Increasingly, treatment plans are being tailored to an individual's unique medical history, lifestyle, risk profile, and, where available, genetic information. AI-driven systems can continuously refine recommendations by analysing new health data generated throughout a

patient's care journey, enabling more precise and adaptive treatment strategies.

In countries such as India, this model presents a significant opportunity to improve healthcare access and outcomes. Persistent challenges related to healthcare infrastructure, specialist availability, and geographic barriers—particularly in rural and underserved regions—can be addressed through connected digital health technologies. By enabling remote monitoring, virtual consultations, and predictive care, AI, IoT, and cloud platforms can extend quality healthcare beyond traditional hospital settings.

Such capabilities can help reduce pressure on overcrowded urban healthcare facilities while ensuring that patients in remote areas receive timely medical attention. As digital health ecosystems mature, healthcare delivery is likely to become more accessible, equitable, and patient-centric.

By 2030, healthcare is expected to evolve from a system centred on episodic hospital visits to one built around continuous, connected care. Individuals will increasingly benefit from an always-on health ecosystem powered by real-time data collection, predictive analytics, and intelligent decision support.

Advances in AI, IoT, and cloud computing will not only enhance the efficiency of healthcare delivery but also fundamentally reshape how care is provided. Rather than focusing primarily on treating illness after it occurs, healthcare systems will be better equipped to anticipate risks, detect diseases earlier, personalise interventions, and support preventive care at scale.

The future of healthcare lies in this transition from reactive treatment to proactive health management. As these technologies continue to converge, they have the potential to improve clinical outcomes, expand access to care, reduce healthcare costs, and create a more resilient and patient-focused healthcare ecosystem. 🌟

*The author is the Founder & CEO,
TrioTree Technologies.
feedbackvnd@cybermedia.co.in*



“AI sprawl is becoming the biggest enterprise risk now”

Enterprise AI is entering a new phase. What began as isolated experiments with chatbots and copilots is rapidly evolving into large-scale deployments of AI agents across customer service, operations, software development, compliance and business processes. As organisations race to embed AI into everyday workflows, they are discovering that scaling intelligence is not simply a technology challenge. It is increasingly becoming a governance challenge.

Multiple teams are now building agents across different frameworks, cloud platforms and model providers, often at a pace that outstrips enterprise oversight mechanisms. The resulting complexity is giving rise to what many industry observers describe as “AI sprawl”, a fragmented environment where visibility, accountability and control become difficult to maintain.

Prasanna Arikala, CTO and Head of Products at Kore.ai, believes this challenge will define the next phase of enterprise AI adoption. In this interaction with **Shubhendu Parth**, he explains why governance must evolve alongside innovation, how enterprises can establish control across heterogeneous AI environments, and why a central operational layer is becoming essential for managing increasingly complex agent ecosystems. Excerpts:

As enterprises deploy multiple AI agents across platforms and clouds, how significant is the challenge of AI sprawl, and what risks does it introduce?

I think AI sprawl is already one of the biggest enterprise

AI challenges, and it is happening much faster than most organisations anticipated.

In almost every enterprise we engage with, multiple teams are experimenting simultaneously. One team may be building on a particular framework, another may be using a different cloud provider, while a third may be optimising for a specific model vendor. All of them are under pressure to move quickly because the technology landscape itself continues to evolve. Models improve rapidly, frameworks change frequently, and new optimisation techniques emerge almost continuously.

The natural response is to keep building, but speed without coordination creates fragmentation. The problem is not merely the number of AI agents being deployed. The larger concern is that many of these agents are being built without a clear understanding of how they behave under failure conditions, what data they access, which tools they invoke, or the policies that govern their actions. That is where AI sprawl becomes dangerous, as organisations accumulate operational and governance risks that remain largely invisible until an incident occurs.

As fragmentation increases, enterprises begin to see inconsistent customer experiences, duplicated development efforts, rising infrastructure costs, and quality issues that are difficult to diagnose. In regulated industries, the risks become even more significant because organisations must demonstrate accountability, auditability and compliance.

“Multiple AI agents across clouds and frameworks create hidden compliance, cost, and quality risks unless firms establish a single control layer early across teams.”



PRASANNA ARIKALA
CTO & Head – Products, Kore.ai

“Enterprises do not need a prettier inventory. They need an operating system to govern agents, policies, owners and runtime actions safely at enterprise scale.”

When nobody has a complete picture of what AI systems are running and how they are behaving, risk accumulates quickly. That is why I view AI sprawl as one of the defining challenges of enterprise AI adoption. Without a central operating layer, such as an Agent Management Platform (AMP), speed eventually leads to fragmentation, which ultimately becomes a business risk.

How can organisations achieve centralised visibility and control over AI agents operating across different frameworks and environments?

Organisations gain control not by forcing every team onto a single framework. That is usually unrealistic and often counterproductive. The right approach is to create a central operating layer that sits above the framework and cloud choices.

In practice, centralised visibility has to be multidimensional. It is not enough to know that an agent exists. Organisations need to understand how it is performing, where quality is breaking down, which models and tools it is calling, which data it is touching, which policies apply to it, who owns it, what environment it is running in, and what it is costing the business.

That is the role we see for AMP. It becomes the common control plane across heterogeneous agent systems. It normalises telemetry and traces from different frameworks, captures evaluation results, maps policies to runtime behaviour and gives enterprises a single place to understand the health of their AI estate. When that visibility is missing, every team sees only its own slice of the problem. When that visibility exists, leaders can finally answer critical questions such as which agents are safe to scale, which are drifting, which are failing silently, and where the biggest business risks actually reside.

Centralised control also has to go beyond dashboards. It requires policy inheritance, role-based access, deployment lineage, auditability and the ability to intervene when something goes wrong. In other words, enterprises do not need a prettier inventory. They need an operating system

for enterprise agents. That is how visibility turns into control, and control turns into confidence.

What capabilities are required to monitor, govern and enforce policy across multi-agent systems in real time?

In multi-agent systems, real-time governance cannot be based solely on human review, nor on vague pattern matching. The volume, speed and complexity are too high. In practice, AI has to help monitor AI. However, that only works if the monitoring is carefully engineered. A single generic model watching everything will generate too many false positives, too many false negatives and ultimately not enough trust. What enterprises need instead is a layered governance architecture.

At the first layer, there must be deterministic controls such as identity checks, tool allow-lists, data boundary rules, rate limits, policy routing and hard stops for known violations. On top of that, organisations need specialised evaluators capable of assessing quality, safety, hallucination risk, prompt injection attempts, privacy exposure and policy compliance within the appropriate business context. Those evaluators require clean context windows, tuned instructions and optimised parameters.

In many cases, different models are needed for different governance functions because the model that excels at security review may not be the one best suited for conversational quality assessment.

Beyond observation, enterprises need the ability to act in real time. Systems must be capable of warning, redacting, re-asking, quarantining, escalating to a human reviewer or stopping execution altogether when required. The platform must also provide access to a deep library of prebuilt policy templates aligned with security standards, privacy obligations and emerging regional AI regulations.

Most enterprises do not possess that catalogue internally today. Ultimately, the requirement extends beyond monitoring. It is about runtime observation, decision-making, enforcement and auditability at enterprise scale.

“AI must monitor AI through specialised evaluators, deterministic controls and automated interventions before failures spread across workflows at speed today.”

Can platforms like yours act as a central command layer to detect and contain unintended AI behaviour?

Yes, platforms such as AMP can absolutely act as a central command layer, but it is important to frame that role correctly. A platform can identify patterns of unintended behaviour far earlier than fragmented teams operating independently. It can correlate traces across multiple agents, detect quality or safety drift, monitor abnormal tool usage, identify policy violations and surface risky behaviour before it develops into a broader operational incident.

More importantly, it can help contain that behaviour. Organisations can throttle an agent, turn off a tool, switch to a safer model path, invoke stricter guardrails, route sessions to a human operator or temporarily remove an agent from circulation while the issue is investigated. This becomes particularly important in multi-agent environments because failures rarely remain isolated.

A single weak agent can pass incorrect context to another, while a permissive tool policy in one workflow can expose it across several others. A command layer enables enterprises to see and respond to those chain effects in real time.

At the same time, I do not believe the platform alone is the answer. Enterprises must still establish the right controls, define ownership, train the right teams and develop the internal discipline needed to interpret signals and act upon them.

AMP can accelerate that journey, provide a strong starting point through compliance and policy templates, and help organisations scale good governance practices. What it cannot do is substitute for organisational learning. In many ways, that may be the more important challenge. Technology can accelerate governance, but enterprises still need to build the muscle to govern well.

How should enterprises balance rapid AI adoption with the need for governance, control and accountability at scale?

I do not think enterprises should approach this as a trade-off between speed and governance. At scale,

governance is what makes speed sustainable. One of the biggest mistakes organisations make is treating governance as a second phase that can be addressed after experimentation succeeds. In reality, postponing governance creates rework, introduces additional risk and ultimately slows execution because organisations are forced to retrofit controls into an environment that has already become fragmented.

The organisations that will move fastest over the next few years are those that build governance directly into their operating model from the outset. That starts with adopting a platform approach before the AI estate becomes too complex to manage. It also requires clearly defining accountability.

Enterprises need to determine who owns agent quality, who owns policy, who approves deployments, who responds when behaviour drifts and who has the authority to intervene when necessary. Without those ownership structures, governance quickly becomes everyone's responsibility and nobody's responsibility at the same time.

Continuous education is equally important. This is not a one-time training exercise, because models, attack patterns, and regulations evolve, and internal teams must keep pace. The mindset shift is critical. Enterprises should not ask how much governance they can afford without slowing down innovation. They should ask what operating discipline will allow them to scale adoption safely, consistently and repeatedly. In practice, that means release gates, runtime monitoring, evaluation loops, auditability and clear escalation paths.

Governance should not be viewed as a tax on innovation. It is the system that prevents innovation from collapsing under its own success. My view is simple: start now, put a control layer such as AMP in place early, and treat governance as a foundational requirement rather than an afterthought. In enterprise AI, waiting is often the riskiest choice. 🧠

shubhendup@cybermedia.co.in

The death of the network perimeter is rewriting security

As work moves beyond enterprise networks, security is shifting from location-based trust to continuous identity, device and contextual access verification.



BY SHUBHENDU PARTH

The enterprise network was once the centre of cybersecurity. Applications resided within corporate data centres, employees worked from managed offices, and security teams could draw a clear line between trusted and untrusted environments. Hybrid work has dismantled that model.

Today, employees connect from homes, airports, client sites, branch offices, and co-working spaces. Applications increasingly reside in multiple clouds, while business data flows across SaaS platforms, mobile devices, and third-party ecosystems. The traditional network perimeter has become porous, forcing organisations to rethink how they secure access, validate trust, and manage risk.

The result is a fundamental architectural shift. Security is moving away from location-based controls towards models built around identity, context, device posture, and continuous verification. At the same time, enterprises

must confront a growing range of challenges, from AI-powered attacks and shadow IT to fragmented security architectures and human error.

Industry experts believe the future of enterprise security will depend not on defending fixed boundaries, but on securing users, applications, and data wherever they reside.

NETWORK PERIMETER IS NO LONGER THE BOUNDARY

The first challenge facing enterprises is recognising that hybrid work represents more than a workplace policy change. It has altered the very assumptions on which traditional security architectures were built.

Murtuza Kachwala, Managing Director, Protiviti Member Firm for India, believes many organisations have yet to fully appreciate this reality. As he notes,



The collapse of traditional boundaries is accelerating SASE and ZTNA adoption, enabling secure, identity-aware access without exposing enterprise infrastructure.

HARISH KUMAR GS

Head of Sales – India & South Asia, Check Point Software Technologies

“The biggest mistake organisations make is assuming that hybrid work is just an extension of their existing IT environment. However, it is not, and it fundamentally dissolves the traditional network perimeter.”

According to Kachwala, many enterprises continue to rely on perimeter-based thinking even as users increasingly operate beyond corporate networks. The result is inconsistent identity enforcement, uneven endpoint protection, and declining visibility outside office environments.

Harish Kumar GS, Head of Sales, India and South Asia at Check Point Software Technologies, sees the same transformation from a security architecture perspective. He argues that hybrid work has accelerated “a structural shift from perimeter-led security to a distributed, identity-first security architecture.”

Vivek Srivastava, Country Manager, India and SAARC at Fortinet, similarly observes that hybrid work is removing the constraints of the traditional network perimeter and forcing security to follow users, devices, and applications wherever they operate.

Together, these trends signal the end of an era in which network location served as the primary determinant of trust.

IDENTITY EMERGES AS THE NEW TRUST LAYER

As the traditional perimeter recedes, identity has emerged as the primary control mechanism for securing enterprise access.

Kumar believes this shift lies at the heart of modern cyber defence. According to him, hybrid work has accelerated a structural shift from perimeter-led security to a distributed, identity-first security architecture.

“As users operate across unmanaged networks and devices, endpoints have become the primary entry point for attacks, while identity has emerged as the central



IN BRIEF

- Hybrid work has weakened traditional perimeter-based security models built around trusted enterprise networks.
- Identity is replacing network location as the primary mechanism for validating trust and controlling enterprise access.
- AI-driven phishing, deepfakes and MFA fatigue attacks are making identity compromise easier and harder to detect.
- Shadow IT, unmanaged devices and unsecured home networks are expanding invisible attack surfaces for enterprises.
- Zero Trust adoption remains uneven as organisations struggle with legacy systems and fragmented identity environments.
- Enterprises are shifting from fragmented tools to integrated security and networking platforms built around SASE models.

control layer. This is pushing enterprises towards Zero Trust models where access is continuously validated based on user, device, and behavioural context rather than assumed trust,” he explains.

Identity is no longer merely an authentication mechanism. It has become the foundation for determining



Public Wi-Fi, personal devices, and shadow IT are now routine enterprise risks, creating invisible attack paths through unmanaged tools and unsecured data flows.

MURTUZA KACHWALA

Managing Director, Protiviti Member Firm for India



REBUILDING NETWORK TRUST

- Audit identity flows across cloud, SaaS, and remote-access environments.
- Replace location-based trust with continuous user and device verification.
- Integrate endpoint, network and cloud telemetry into unified visibility platforms.
- Map shadow IT usage across unmanaged applications and collaboration tools.
- Prioritise SASE and Zero Trust around business workflows, not products alone.
- Enforce device posture validation before granting application access.
- Reduce fragmented security stacks through orchestration and policy integration.
- Expand employee awareness beyond phishing drills to behaviour-based security.
- Monitor AI-driven threats, including deepfakes, credential abuse and MFA fatigue.
- Treat hybrid work security as a network architecture issue, not only a cyber issue.

who gains access, under what circumstances, and with what level of privilege.

Srivastava notes that organisations increasingly rely on multifactor authentication, single sign-on, and contextual risk signals to validate users based on “who they are and not where they connect from.”

Kachwala echoes this view, arguing that identity has effectively become the new control plane for distributed enterprises. In hybrid environments, access decisions must be dynamic and risk-aware, taking into account user behaviour, device status, and business context rather than simply network location.

The shift represents one of the most significant changes in enterprise security since the emergence of corporate networking itself.

ENDPOINTS BECOME THE NEW ENTERPRISE EDGE

The disappearance of fixed boundaries has also elevated the strategic importance of endpoints.

Laptops, smartphones, tablets, and remote workstations now function as extensions of the enterprise network. Each endpoint serves simultaneously as a productivity tool, an access gateway, and a potential attack vector.

Kumar notes that endpoints have become the primary entry point for modern attacks, increasing demand for advanced endpoint detection, response, and visibility capabilities. However, he argues that traditional endpoint security alone is insufficient because attacks increasingly move across identities, cloud services, networks, and applications.

Srivastava believes enterprises must continuously assess device posture, operating system health, patch status, and security configurations before granting access. Endpoint trust cannot be assumed simply because a device belongs to an employee.



Credential compromise, including MFA fatigue and session hijacking, is increasingly used to bypass perimeter controls and gain access to cloud and SaaS applications.

VIVEK SRIVASTAVA

Country Manager, India & SAARC, Fortinet

Kachwala highlights another challenge: consistency. Organisations often maintain strong controls within office environments, while remote users operate under entirely different security conditions. This creates fragmented security postures that attackers can exploit.

As a result, endpoints are increasingly becoming part of broader security architectures that integrate identity, access control, risk assessment, and behavioural analytics.

AI IS ENABLING AGGRESSIVE IDENTITY ATTACKS

The rise of hybrid work has coincided with another major shift: the growing use of artificial intelligence by attackers. Rather than targeting infrastructure directly, cybercriminals increasingly focus on compromising user identities through phishing, credential theft, social engineering, and account hijacking.

According to Kumar, organisations are witnessing “a pronounced rise in identity-led attacks” as attackers shift their attention from networks to users. He points to credential phishing, session hijacking, MFA fatigue attacks, deepfake-driven social engineering, and adaptive malware as examples of an evolving threat landscape.

Srivastava notes that AI-enabled cybercrime has fundamentally altered the scale and sophistication of attacks. According to research cited by Fortinet, 72% of organisations in India reported encountering AI-powered cyber threats during the previous year. These include AI-assisted credential attacks, automated reconnaissance, AI-generated phishing campaigns, and deepfake-enabled business email compromise schemes.

Kachwala argues that technology alone cannot explain this trend. Many successful attacks exploit human behaviour rather than technical vulnerabilities. As employees move between devices, applications, and

networks throughout the day, attackers increasingly target decision-making processes rather than infrastructure weaknesses.

The convergence of AI and identity-based attacks is forcing organisations to rethink both security technologies and user awareness strategies.

SHADOW IT IS EXPANDING THE INVISIBLE NETWORK

One of the least visible consequences of hybrid work is the growth of shadow IT. Employees routinely use unauthorised applications, personal devices, consumer collaboration tools, and unsecured networks to perform legitimate business activities.

While these practices often improve productivity, they can also create significant security blind spots.

Kachwala believes organisations underestimate these everyday risks. Public Wi-Fi, credential reuse, unmanaged devices, unsecured home networks, and shadow applications collectively expand the enterprise attack surface. As he puts it, “The biggest risks are the most routine.”

Similarly, Kumar points to unmanaged devices and inconsistent security practices as major contributors to enterprise exposure. In distributed environments, organisations often have limited visibility into the networks and devices employees use to access corporate resources.

Srivastava observes that employees increasingly operate outside traditional office environments, making it more difficult to enforce consistent controls across all users and devices.

For many organisations, the invisible network created by shadow IT may ultimately prove more difficult to secure than the official one.

Enterprise security is shifting from defending fixed office networks to continuously validating users, devices and application behaviour across distributed workforces.

ZERO TRUST NEEDS MORE THAN TECHNOLOGY

Few concepts have gained greater prominence in enterprise security than Zero Trust. Yet implementing the model remains far more difficult than discussing it.

Kachwala believes many organisations misunderstand the scale of transformation required. “Awareness of zero trust is high, but execution maturity is low,” he observes. Many enterprises approach Zero Trust as a collection of security tools rather than a comprehensive redesign of access, trust, and governance. Legacy infrastructure, fragmented identity systems, and resistance to tighter controls frequently undermine implementation efforts.

For Kumar, Zero Trust is fundamentally about continuous verification. He describes it as a “never trust, always verify” model in which access decisions are constantly validated using identity, device posture, behavioural context, and risk indicators.

Srivastava views Secure Access Service Edge (SASE) as a critical enabler of this approach. By converging networking and security into a cloud-delivered architecture, organisations can apply consistent policies, deliver application-level access, and maintain continuous risk validation regardless of user location. The most successful organisations increasingly view Zero Trust not as a security product but as an operating model for a distributed enterprise.

SECURITY PLATFORMS ARE REPLACING SECURITY SILOS

The evolution of enterprise networks is also changing how organisations invest in security technologies. According to Kumar, a growing shift away from fragmented point solutions towards integrated security platforms that combine endpoint, identity, network, and cloud intelligence. Enterprises increasingly favour prevention-first architectures that can correlate information across multiple security domains.

Srivastava points to Gartner forecasts suggesting that by 2028, 70% of new SD-WAN purchases will be part of single-vendor SASE offerings, up from 20% in 2024. The market is increasingly rewarding convergence rather than specialisation.

Kachwala warns that tool proliferation without integration often creates additional risk. “Companies invest in multiple security solutions, but without orchestration, they create blind spots rather than resilience.”

The future appears to belong to architectures that combine visibility, orchestration, automation, and policy enforcement within unified platforms rather than isolated security products.

IT IS TIME FOR SECURITY TO TRAVEL WITH THE USER

Ultimately, the defining characteristic of modern cybersecurity may be its ability to operate independently of location.

Whether employees connect from headquarters, home offices, branch locations, customer premises, or public networks, security controls must remain consistent while adapting dynamically to changing risks. Kumar captures this evolution succinctly when he says that security travels with the user, not the network.

Srivastava argues that organisations increasingly require “consistent protection, real-time risk validation, and a seamless user experience—regardless of where employees work or how they connect.”

Kachwala believes success ultimately depends on balancing security with flexibility. Organisations must embed security into workflows and business processes rather than imposing controls that users inevitably bypass. As he notes, “The organisations that get this right are not the ones with the most controls, but the ones with the most intelligent and adaptive ones.”

The death of the network perimeter is therefore not merely a cybersecurity story. It is a story about how enterprise networks, applications, users, and trust relationships are being re-engineered for a world where work happens everywhere. Organisations that embrace identity-led access, integrated visibility, adaptive controls, and continuous verification will be better positioned to secure that future. 🌟

shubhendup@cybermedia.co.in

25th TELECOM
LEADERSHIP
FORUM
EMPOWERING LEADERS IN TELECOMMUNICATIONS

33rd
ICT
BUSINESS
AWARDS

CyberMedia Leadership & Awards Night 2026

FROM CONNECTIVITY TO INTELLIGENCE:
HOW TELECOM AND IT TOGETHER BUILD DIGITAL INDIA



ONE EVENING



TWO INDUSTRY
POWERHOUSES



INFINITE LEADERSHIP
CONNECTIONS

**CELEBRATING EXCELLENCE IN TECHNOLOGY,
TELECOM & DIGITAL INFRASTRUCTURE**

A uniquely curated gathering where India's foremost technology and telecom leaders come together to celebrate achievement, exchange ideas, and shape the future of the industry.

Date: 3 July 2026, New Delhi

Attendance by Invitation Only. For delegate or partnership inquiries, visit: <https://tlfindia.in>
or contact the below

For Sponsorship Opportunities:

Rajnish Jamur

General Manager Business Solutions

✉ rajnishj@cybermedia.co.in

☎ +91 98188 93544

For Marketing & Alliances:

Ajay Dhoundiyal

Sr. Manager Business Solutions & Sales

✉ ajaydh@cybermedia.co.in

☎ 91 9953540318

For Delegate Registrations:

Ankit Parashar

General Manager Events

✉ ankitp@cybermedia.co.in

☎ +91 98733 73763

The 5G building code is being written in DAS

Neutral-host DAS is shifting from telecom add-on to core building infrastructure as developers prepare properties to meet demands for indoor 5G.



BY PANKAJ TAMBE

Building connectivity was long approached in much the same way as parking: something to be figured out after the building was completed. Add a few signal amplifiers, deploy a Wi-Fi network, and the job was considered done. That approach is now changing.

As 5G rollouts continue and device density within buildings rises exponentially, one reality is becoming

increasingly clear: future-ready connectivity cannot be achieved solely through retrofitting.

The wireless infrastructure required to deliver seamless indoor coverage in large-scale buildings, particularly neutral-host Distributed Antenna Systems (DAS), must be incorporated from the outset of construction. This is not a passing trend. It is rapidly becoming a necessity.

As 5G signals struggle to penetrate modern building materials, developers increasingly view indoor wireless infrastructure as a design requirement at the earliest stages.

Installing neutral-host DAS during construction reduces retrofit costs, preserves valuable building space, and simplifies future technology upgrades.

INDOOR 5G COVERAGE BECOMES CRITICAL

There are two main aspects of the science behind 5G technology, depending on whether it uses mid-band or mmWave. These higher frequencies transmit more information, though they cannot easily penetrate barriers such as walls, glass windows, reinforced concrete, or surfaces coated with increasingly popular low-emissivity (low-E) glass. An energy-efficient building is, by definition, one that blocks wireless signal transmission.

Beyond these technical limitations, expectations around indoor connectivity have changed dramatically. Whether in offices, residential complexes, shopping malls, or healthcare facilities, fast and reliable wireless connectivity is now considered as essential as running water and climate control.

Failure to provide adequate indoor wireless coverage can have serious consequences. These range from reduced productivity and disruption of IoT sensors and building automation systems to failures in healthcare monitoring applications and, in some cases, risks to public safety when first responders are unable to communicate effectively within a building.

HOW NEUTRAL-HOST DAS IMPROVES COVERAGE

A Distributed Antenna System improves indoor cellular coverage by distributing mobile signals throughout a building via multiple small antennas connected to a central signal source. The neutral host concept is a step beyond the DAS, enabling multiple mobile operators to use a single passive infrastructure concurrently. This delivers two significant advantages.

One, it eliminates the problem of carrier fragmentation. If a building relies on a single mobile operator's infrastructure, users on other networks may experience poor or no coverage. A neutral-host DAS ensures consistent connectivity for all occupants and visitors, regardless of their network and service provider.

Two, it offers greater cost and space efficiency. Building separate infrastructure for individual operators is neither practical nor scalable. A shared

DAS can be installed during construction and subsequently upgraded as network technologies evolve from 4G LTE to 5G NR, without requiring disruptive structural modifications such as tearing down walls.

WHY DAS MUST START AT CONSTRUCTION

This is where the industry's approach to connectivity must fundamentally change.

Deploying a DAS in an existing or newly completed building is often costly, complex, and disruptive. Challenges typically include the absence of planned conduit pathways, limited riser space, and the need to create dedicated head-end facilities. The result is frequently a suboptimal solution that is difficult to maintain and more expensive to operate over its lifecycle.

By contrast, incorporating DAS during the construction phase transforms the economics of deployment. Conduits, cable trays, equipment rooms, and power provisioning can be integrated into the building's core design, much like fire suppression systems, HVAC infrastructure, and electrical risers. As a result, installation costs are significantly lower than those associated with post-construction retrofits.

Forward-looking developers and architects have already recognised this shift. Many now specify in-building wireless infrastructure during the design or tendering stage. In several international markets, reliable indoor wireless coverage, particularly for emergency services communications, has evolved from a recommended practice into a regulatory requirement.

CONNECTIVITY BECOMES A BUILDING ASSET

Beyond its operational benefits, connectivity infrastructure is increasingly emerging as a measurable asset that influences property valuations, rental premiums, and investment attractiveness. Building certification programmes are placing greater emphasis on digital infrastructure readiness, with FTTx backbones and in-building wireless systems becoming important contributors to overall connectivity scores.

Connectivity is becoming a measurable real estate asset, influencing leasing decisions, property valuations, and certification frameworks globally.



DAS BY DESIGN

As neutral-host DAS moves into the construction blueprint, developers must begin treating wireless infrastructure like any other core building system. Key considerations must include:

- Plan DAS during the design phase, not after occupancy certificates are issued.
- Reserve riser space, conduit pathways and cable trays for future wireless expansion.
- Allocate dedicated equipment and head-end rooms within the building design.
- Ensure adequate power and backup power provisioning for telecom equipment.
- Design infrastructure to support multiple mobile operators through a neutral-host model.
- Integrate DAS planning with fibre backbones, managed Wi-Fi and smart-building systems.
- Factor indoor coverage requirements into sustainability and digital-building certification goals.
- Consider emergency services communications requirements that may become regulatory mandates.
- Future-proof deployments for technology evolution from 4G LTE and 5G to next-generation wireless standards.
- Treat connectivity as a long-term asset that influences tenant satisfaction, occupancy rates and property value.

This shift is creating a competitive advantage for commercial real estate developers. Enterprise tenants, particularly in technology, financial services, and healthcare, are conducting connectivity assessments before committing to leases. Buildings that lack carrier-grade wireless infrastructure risk losing tenants and potential revenue.

As a result, developers are increasingly seeking infrastructure partners that understand both the built environment and the requirements of modern communications networks. Industry experience in delivering in-building mobility and managed Wi-Fi solutions reinforces the view that digital connectivity should be treated as a core building utility, designed, deployed, and maintained to carrier-grade standards.

WHY NEUTRAL-HOST DAS IS ESSENTIAL

The transition from optional amenity to essential infrastructure may not occur uniformly across markets, but the direction of travel is unmistakable. In some jurisdictions, building regulations are beginning to incorporate minimum wireless connectivity requirements. Investors and private equity firms are paying closer attention to digital infrastructure when assessing property value, while anchor tenants are increasingly making connectivity a prerequisite for leasing decisions.

For developers, the implication is clear: neutral-host DAS should be planned as an integral part of a building's 5G strategy from the outset, not introduced as a retrofit after construction is complete. Early adoption enables buildings to meet evolving connectivity expectations while avoiding the cost and complexity of future upgrades.

As digital infrastructure becomes as fundamental as power, water, and climate control, buildings that prioritise carrier-grade indoor connectivity will be better positioned to attract tenants, command premium valuations, and remain relevant in an increasingly connected world. 🌐

*The author is Vice President and Business Head of Mobility at iBUS Networks.
feedbackvnd@cybermedia.co.in*



Campus networks face a test beyond bandwidth limits

As device density surges across campuses, AI-led broadband is becoming the foundation for resilient, secure and future-ready digital learning ecosystems.



BY NAVNEET SHARMA

India's campuses have never been more connected—or more constrained. Classrooms, hostels, and laboratories are now packed with laptops, smartphones, and a growing layer of IoT devices, all competing for the same finite wireless infrastructure.

In a country with around 950 million internet users in 2025, according to IAMA's Internet in India Report 2025, young people are among the heaviest data consumers, bringing constant, high-frequency usage patterns into lecture halls and common spaces.

The result is an often-overlooked bottleneck in Indian higher education: networks designed for the pre-smartphone era struggling to serve a digital-native generation.

On a typical large campus, tens of thousands of concurrent devices now operate on legacy infrastructure that was never architected for this scale, density, or diversity of applications. When that infrastructure fails to keep pace, it is no longer a minor inconvenience. It directly affects teaching quality, research productivity, and the overall student experience.

LEGACY NETWORKS UNDER CAMPUS STRAIN

Most campuses still experience the familiar symptoms of overloaded infrastructure: patchy coverage, dead zones in hostels and lecture halls, dropped video calls, and random disconnections even when users appear to be online. The real challenge is density. Consider a 300-seat lecture hall where every student simultaneously connects at 10:00

When campus networks fail to keep pace with demand, the impact extends beyond inconvenience, affecting teaching quality, research output and student experience.

a.m., competing for the same wireless spectrum during peak demand.

For students, this is more than an inconvenience. When a webinar buffers, a placement interview drops, or a seminar fails to stream, connectivity becomes an academic and career issue.

The problem is not a lack of equipment; it is a lack of orchestration. High-density, high-performance campus broadband is therefore not a theoretical aspiration but an achievable goal when networks are designed for concurrency, coverage, and continuity rather than simply raw access.

Adding more routers often increases interference and operational complexity. What campuses need instead is a smarter network architecture that can support dense usage patterns without creating new bottlenecks.

SMARTER CONNECTIVITY FOR LEARNING

Adding routers indiscriminately may appear to solve a coverage problem, but it often increases interference, congestion, and management complexity. What campuses need instead is intelligent connectivity that can analyse traffic patterns in real time and prioritise critical applications.

This is where AI-enabled access points change the equation. Rather than simply balancing traffic mechanically, they can distinguish between different use cases and allocate network resources accordingly. A student downloading a game in a hostel does not have the same connectivity requirements as a professor conducting a PhD viva, streaming a lecture, or accessing the learning management system during peak academic hours.

Unlike a game download, a PhD viva or live lecture is highly latency-sensitive, where even a brief delay can

A CAMPUS CIO CHECKLIST

Before investing in additional bandwidth or access points, campus technology leaders should evaluate whether their network is prepared for the realities of modern digital education.

- ☐ Can the network support thousands of concurrent devices during peak academic hours?
- ☐ Are lecture halls, hostels, libraries and laboratories covered without dead zones?
- ☐ Can critical academic applications receive priority over recreational traffic?
- ☐ Is AI-based traffic management being used to optimise network performance?
- ☐ Is there multi-ISP redundancy to minimise service disruption?
- ☐ Is SIM-based backup available in the event of primary link failures?
- ☐ Are guest, student, faculty and administrative networks properly segmented?
- ☐ Are EDR, antivirus and web filtering embedded into the network layer?
- ☐ Can suspicious devices or malicious traffic be identified and isolated quickly?
- ☐ Does the institution have visibility into network health through real-time dashboards?
- ☐ Are VPNs, remote access and cloud-based learning platforms adequately secured?
- ☐ Is the network architecture scalable enough to accommodate future growth in users, devices and IoT deployments?

The objective is no longer simply providing internet access. It is building a secure, resilient and intelligent digital foundation that supports learning, research and institutional growth.

AI-enabled access points change the equation by recognising diverse usage patterns and dynamically allocating network resources to optimise performance today.

disrupt the experience. Intelligent traffic prioritisation is therefore not a luxury but an academic necessity.

When combined with managed CPE, multi-ISP support, and SIM-based backup, campuses can build a more resilient network foundation that minimises outages and maintains service continuity during traffic spikes or link failures. The result is smoother hybrid learning, fewer disruptions, and more reliable access to digital libraries, research platforms, and cloud-based academic tools.

SECURING THE CAMPUS NETWORK FABRIC

As network usage scales, so does risk. Laboratories, administrative systems, and student devices increasingly share the same digital environment, and a single infected endpoint can disrupt examinations, result processing, or ERP operations.

Network-level endpoint detection and response (EDR) and antivirus capabilities embedded within the connectivity layer can help identify and contain malware before it spreads across the campus fabric, reducing the risk of ransomware incidents affecting critical academic systems.

Segmentation is equally important. Separating guest and student Wi-Fi from administrative and research networks limits the lateral movement of threats, helping to protect examination infrastructure, ERP platforms, and sensitive institutional records from compromised personal devices.

Web filtering at the network layer can block malicious websites, phishing attempts, and non-academic bandwidth drains, strengthening security while improving service quality for legitimate academic activities.

With India's evolving data protection framework, safeguarding student data from exposure through unsecured access points is no longer optional. It has become a matter of institutional compliance and data sovereignty.

Static IP capabilities further support stable VPN connectivity, hosted learning platforms, inter-campus collaboration, and secure remote access for faculty. This enables more consistent identity management, access control, and network monitoring across distributed environments.

In an ecosystem where students routinely access mobile applications, cloud services, and public websites, embedding security and control into the network fabric is critical not only for threat mitigation but also for institutional resilience, integrity, and data sovereignty.

BUILDING FUTURE-READY DIGITAL CAMPUSES

Connectivity is no longer a utility; it is a foundational layer of digital equity that shapes a student's ability to learn, collaborate, and compete. Today's networks sit at the intersection of massive national digital adoption and the expectations of a generation that experiences education, collaboration, and assessment through connected devices.

Enterprise-grade broadband, combined with AI-powered connectivity, managed CPE with multi-ISP and SIM backup, secure guest access, URL filtering, and embedded EDR and antivirus capabilities, provides campuses with an end-to-end ecosystem designed for continuity, security, and control.

Real-time performance dashboards and self-service portals offer visibility into network health and policy enforcement, enabling IT teams and administrators to manage connectivity as strategically as any other critical institutional asset.

The era of "good enough" Wi-Fi is over. Institutions that continue to rely on ageing infrastructure risk falling behind peers that can attract stronger faculty, deliver seamless hybrid learning experiences, and demonstrate greater digital readiness to prospective students.

Campuses that invest in AI-powered network foundations are not simply upgrading connectivity. They are strengthening academic resilience, improving the student experience, and preparing for the next phase of digital education.

The question is no longer whether to upgrade campus networks, but whether institutions can afford the cost of delay. 🌟

*The author is the COO of ACT.
feedbackvnd@cybermedia.co.in*



TO STAY AHEAD OF THE CURVE IN TELECOM READ VOICE&DATA

**Celebrating
Dataquest
40 years:
Avail Special
discount
on V&D.**

**Digital
subscription
also available on
Magzter, Zinio,
Readwhere,
& Readly**



Book Digital Subscription Now!

Yes! I want to subscribe to Voice&Data



Scan QR Code
& Subscribe now...

Subscribe to Digital Edition @ ₹735/-

Period	Issues	Print Subscription Rate		Digital Subscription Rate
		New	Renewal	
☐ 1 year	12	₹1,140/-	₹1,050/-	₹735/-
☐ 2 years	24	₹2,190/-	₹2,020/-	₹1,470/-
☐ 3 years	36	₹3,285/-	₹3,020/-	₹2,205/-

or **Subscribe online:** subscriptions.cybermedia.co.in/voicendata

Please tick your subscription choice above, fill the form below in CAPITAL LETTERS and mail it to us at subscriptions@cybermedia.co.in

☐ I want to avail premium service of receiving your copy by courier. Tick which ever is applicable.

☐ ₹ 600/- 1 year ☐ ₹ 1200/- 2 years ☐ ₹1800/- 3 years

Name [•]: Mr/ Ms _____ Date of Birth:

Organisation: _____ Designation: _____

Delivery Address: _____

City: _____ State: _____ Postal Code:

Mob [•]: Tel: Email [•]: _____

GST No. [•]: PAN No. [•]:

☐ I am paying ₹ by DD/Cheque No.: Dated:

Payable at (specify bank and city) _____

OR

☐ Please Remit for ₹ Through RTGS/NEFT to our A/C details given below:

Bank Name: ICICI Bank Limited, A/c no. 017705000132, Branch & IFS Code: Gurgaon, ICIC0000177

[•] Essential fields

Signature _____ Date: Subscription No. (for renewal) _____

Order form can be mailed with payment (cheque/DD) to:

Cyber Media (India) Ltd, Cyber House, B-35, Sector-32, Gurgaon-122003

Contact: Alok Saxena, Tel: 0124-4237517 (Extn-347), 91+9953150474, Email: aloksa@cybermedia.co.in

For Subscription queries:

9289870545

Terms & Conditions: _____

• This offer is valid for a limited period. • Rates and offer valid only in India. • NEFT/UTR No., Email & Mobile number mandatory. • Please allow 4-6 weeks for delivery of your first copy of the magazine by post. • Send crossed Cheques in favour of Cyber Media (India) Ltd. • Please write your name and address on the reverse side of the cheque or DD. All outstation cheques should be payable at par. • Cyber Media (India) Ltd. will not be responsible for postal delays, transit losses or mutilation of subscription form. • Cyber Media (India) Ltd. reserves the right to terminate or extend this offer or any part thereof. The decision to accept or reject any or all forms received is at the absolute discretion of the publishing company without assigning any reason. • Please include pin code for prompt delivery of your copy. • In case payment is through credit card, date of birth must be mentioned. • All disputes shall be subjected to Delhi jurisdiction only.

Data quality: The bedrock of AI observability

As enterprises embrace AI-driven operations, trusted data is emerging as the foundation for visibility, resilience and reliable outcomes.



BY GAURAV MOHAN

Data is the fuel that drives businesses in today's rapidly evolving digital world, powered by artificial intelligence (AI). But AI systems are only as good as the data they are fed. If the fuel is low-quality, the organisation's decisions reinforce the "garbage in, garbage out" principle, compelling Chief Data Officers to prioritise data quality to navigate the complexity of the modern enterprise efficiently.

It is also quite apparent that AI needs data and not the other way around. Data has always existed for millennia, sometimes good, sometimes bad, sometimes factual, and sometimes opinion-based. History is full of

decisions made from bad data that did not always end well. AI creates insights from data, both good and bad, and amplifies them with algorithmic certainty, whether true or not.

The digital transformation of organisations has created complex environments due to growing cloud infrastructure, hybrid and mobile workforces, distributed applications, encrypted web traffic, tool sprawl, zero-trust architectures, cloud-native microservices, edge computing, and more.

These environments have fractured visibility across infrastructure layers. Observability platforms powered

by AI can help assemble the fragmented pieces for better visibility, but they cannot eliminate the complexity in the environment. If the data inputs for observability are incomplete or distorted, the AI model's outputs will become flawed at best or operationally meaningless at worst.

AI systems cannot see what the data cannot capture, confirming their limitations. They depend heavily on the quality of data they process. If the data is biased or unclear, the AI recommendations will be flawed. Over time, this will introduce compounding errors, leading to missed anomalies, increased false positives, operational uncertainties, and further complexity.

WHY PACKET-LEVEL VISIBILITY MATTERS?

At the centre of trustworthy AI observability lies high-fidelity telemetry, especially packet-level data. Packet-level data captures the actual network conversations between endpoints, applications, workloads, users, and services.

Packet-level insights reveal real-time behaviour necessary for evaluating AI workloads, which are critical indicators of network and service behaviour, more importantly, where dynamic AI models and complex IT infrastructure meet.

Packets capture entire transaction details, what and when it was sent, and how systems responded across the entire stack. With the AI observability market projected to grow at a CAGR of 14.59% from 2025 to 2030, there is an increasing need for packet-level and high-fidelity data, which is critical for reliable AI outcomes.

In the absence of high-quality data, on which AI observability effectiveness depends, organisations may only end up diagnosing failures after suffering painful financial, reputational, and regulatory damage.

HIDDEN COSTS OF POOR OBSERVABILITY DATA

Decisions based on poor observability data are inaccurate, fuelling strategic initiatives that are bound to fail, disrupting operations and impacting customer satisfaction and business outcomes. Ineffective observability data eats up teams' time, forcing them to spend time troubleshooting data issues, leading to increased operating costs and downtime, reduced efficiency, and productivity loss.

Slow or inaccurate decision-making caused by low-quality observability data results in missed innovation

opportunities, potential loss to the competition, and revenue losses and reputational damage. Poor observability data increases the risk of non-compliance, inviting fines, penalties, and legal issues.

Regardless of the observability platform you use, ensuring you can obtain an accurate, trustworthy, comprehensive data foundation for your observability stack is critically important, and this becomes even more significant as AI-driven automation continues to raise the risks and potential rewards.

DATA OBSERVABILITY FOR MODERN ENTERPRISES

As Indian organisations transition to AI-driven environments and adopt hybrid and multi-cloud architectures, prioritising high-quality data for observability becomes critical.

This enables enterprises to overcome data silos and legacy system complexity by delivering a unified, real-time view of data—breaking down silos and ensuring end-to-end transparency across the entire data lifecycle.

Robust data observability practices improve operational efficiency, establish proactive anomaly detection, and ensure real-time incident resolution before they impact business outcomes. To reap the benefits of effective data modernisation, organisations should understand that data observability is critical.

It is neither controversial nor debated that the future of data observability will be shaped by automation and real-time intelligence. Artificial intelligence and machine learning will power continuous monitoring and more precise anomaly detection, strengthening data quality, resilience, and trust.

By adopting these capabilities, organisations can achieve greater operational efficiency, scalable growth, and dependable decision-making, laying a strong foundation for a truly data-driven enterprise, but only if the data is of the highest quality and unimpeachable in terms of accuracy and certainty. Otherwise, the wrong kind of decisions get made that are simply not based on the truth. 🧠

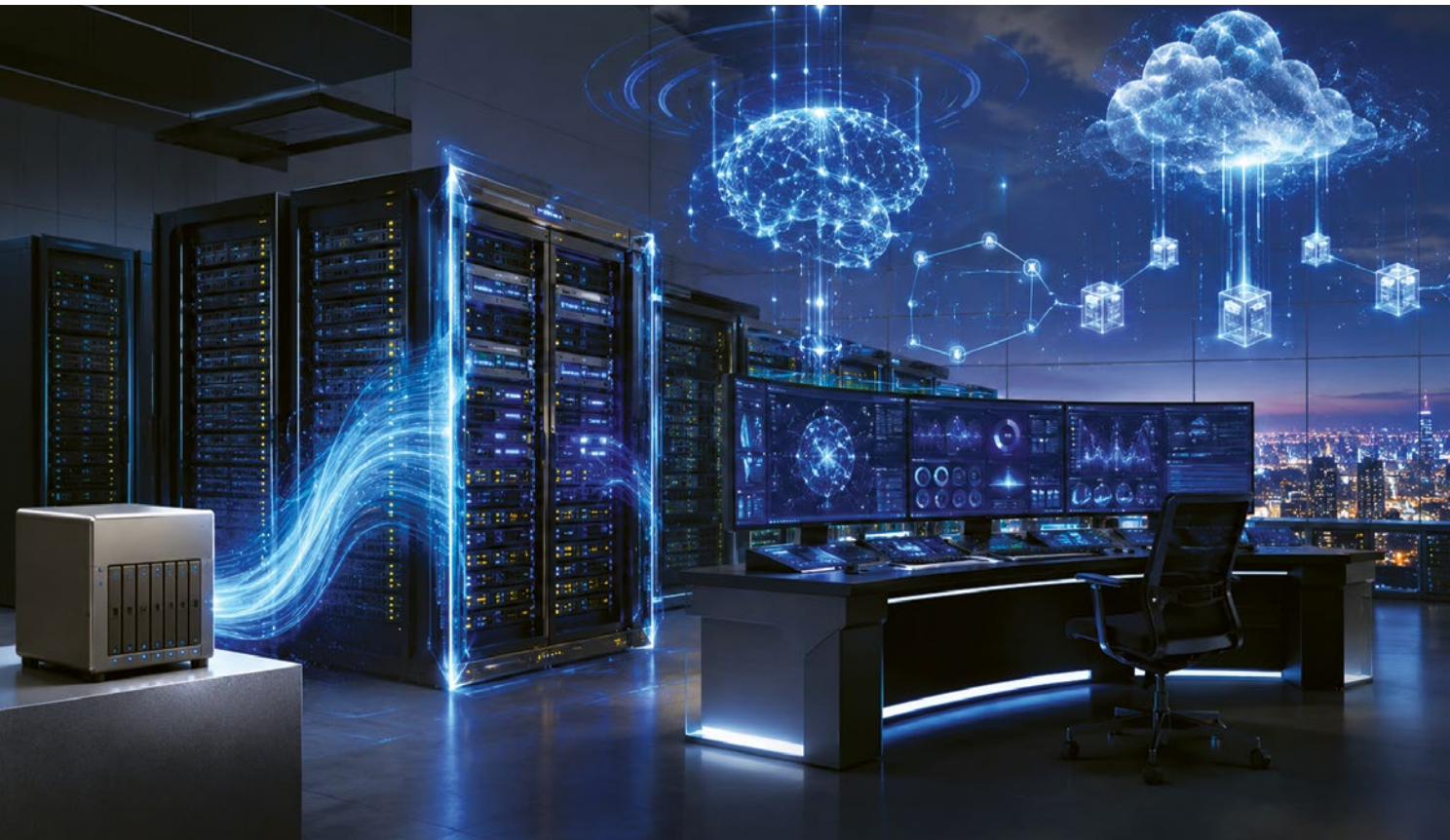
The author is the Vice President of Sales for APAC, India, and the Middle East of Netscout.

feedbackvnd@cybermedia.co.in



From storage box to data control tower for enterprises

As AI and hybrid cloud reshape IT priorities, enterprise data infrastructure is becoming the foundation of Synology's growth strategy across environments.



BY SHUBHENDU PARTH

As enterprises grapple with the demands of artificial intelligence, hybrid cloud and cybersecurity, the boundaries between storage, data protection and infrastructure management are beginning to blur.

A series of recent announcements from Synology suggests the company is positioning itself to capitalise on that convergence. The unveiling of the next-generation DiskStation Manager (DSM) and ActiveProtect Manager 2.0 at Computex 2026 Taipei, along with the launch of

Infrastructure value is shifting towards the data layer, where governance, observability and policy enforcement increasingly shape enterprise decisions today.



“Data ownership is becoming a strategic priority as organisations seek trusted platforms that keep governance, privacy and control close to the data.”

PHILIP WONG

Chairman & CEO, Synology

the PAS7700 enterprise storage platform, and earlier enhancements to its ActiveProtect portfolio, point to a strategy that extends beyond network-attached storage into the broader enterprise data infrastructure stack.

The shift reflects a larger trend unfolding across data centres. As organisations distribute workloads across private infrastructure, public clouds and SaaS platforms, managing data has become a strategic challenge rather than a storage problem. AI initiatives, meanwhile, are forcing enterprises to reassess where data resides, how it is governed and how it can be protected without sacrificing performance or compliance.

Against this backdrop, infrastructure vendors are increasingly competing to become the control layer that sits between applications, data and operations. Synology’s recent roadmap suggests it wants to play a larger role in that space.

The company’s messaging increasingly centres on data ownership and governance. Philip Wong, Chairman and CEO of Synology, recently stated that “data is at the heart of everything we build, and trust is the foundation”, underscoring the company’s ambition to provide organisations with greater control over data across enterprise infrastructure and personal cloud environments.

The emphasis aligns closely with growing enterprise concerns around data sovereignty, security and compliance in AI-driven environments.

BUILDING A PLATFORM FOR HYBRID CLOUD AND AI

The centrepiece of that strategy is the evolution of DSM from a storage operating system into what Synology describes as an intelligent data platform.

The significance lies less in the addition of AI assistants and more in the company’s attempt to

transform storage infrastructure into a platform for governed AI operations. Under the proposed architecture, enterprise data, system logs and operational metrics can be transformed into a private knowledge base accessible to AI agents operating within controlled environments.

The approach addresses a growing concern among enterprises experimenting with generative AI. While public cloud AI services offer scale and convenience, many organisations remain cautious about exposing sensitive corporate information to external platforms. Data sovereignty, compliance requirements and governance obligations are increasingly driving interest in private AI deployments.

Synology’s emphasis on local inference through GPU-enabled systems and dedicated AI appliances reflects this shift. Rather than positioning AI as a standalone capability, the company is embedding it within the data layer itself.

The roadmap also acknowledges a challenge that has received less attention than AI model development: operational complexity. As AI deployments move beyond pilot projects, organisations will require infrastructure capable of managing data, compute resources and governance policies across multiple locations and environments.

Features such as Cluster Manager, containerised workloads and fleet-wide deployment tools indicate a focus on infrastructure orchestration at scale. Expanded role-based access controls, observability features and audit capabilities similarly point to a future in which AI adoption becomes as much a governance challenge as a technology one.

The strategy is reinforced by Synology’s recent launch of PAS7700, the company’s first active-active all-flash NVMe storage platform. Featuring dual controllers, high-



“Cyber resilience increasingly depends on identifying threats before recovery begins, making protection platforms part of security itself.”

BIE-I LIU

Executive Vice President, Synology Data Protection Group

speed networking and support for both file and block workloads, the platform moves Synology further into enterprise data centre territory.

While positioned as storage systems, platforms of this class increasingly serve as the foundation for virtualised environments, private clouds, analytics workloads, and AI infrastructure. As enterprises seek greater control over data-intensive applications, storage performance, availability and scalability become critical infrastructure considerations rather than standalone procurement decisions.

DATA PROTECTION BECOMES INFRASTRUCTURE RESILIENCE

If DSM reflects Synology's ambitions around data management and AI, ActiveProtect Manager 2.0 illustrates how the company views the future of cyber resilience.

The latest release expands protection across Amazon EC2, Microsoft Azure, Nutanix AHV, Proxmox VE and Google Workspace, while introducing support for cloud-to-cloud recovery and cross-platform workload restoration. These capabilities reflect the realities of modern enterprise environments, where applications and data are increasingly spread across multiple clouds and on-premises infrastructure.

The challenge for IT teams is no longer simply backing up data. It ensures consistent protection, governance, and recoverability regardless of where workloads reside.

This is an area where Synology has been steadily building its platform. Earlier ActiveProtect updates expanded centralised management capabilities to support hundreds of thousands of workloads through a single management plane, signalling an ambition to address infrastructure-wide resilience rather than relying solely on traditional backup requirements.

The latest addition of AI-powered threat detection takes that evolution further. Using machine learning to analyse backup histories, the system is designed to identify anomalies such as unusual change patterns, mass deletions and potential ransomware activity before compromised data is restored into production environments.

Synology sees this as part of a broader shift in cyber resilience. As Bie-i Liu, Executive Vice President of the Synology Data Protection Group, observed, “ActiveProtect Manager 2.0 extends protection across major cloud, hypervisor and SaaS environments while introducing AI-driven threat detection designed to move data protection from reactive recovery towards proactive defence.”

Features such as automated quarantine, malware scanning and clean-point recovery illustrate a broader shift occurring across the industry. Data protection platforms are increasingly expected to function as active security controls rather than passive recovery repositories.

Viewed collectively, Synology's announcements point to a wider transformation in enterprise infrastructure. Storage systems are evolving into intelligent platforms that manage, govern and protect data across increasingly distributed environments. At the same time, backup platforms are becoming integral components of cyber defence and operational resilience strategies.

Whether enterprises ultimately embrace large-scale private AI deployments remains uncertain. What is becoming clearer, however, is that the value of infrastructure is moving closer to the data itself. As organisations seek greater control over information spread across data centres, clouds and AI environments, vendors capable of unifying storage, governance and resilience may find themselves competing for a larger share of the enterprise infrastructure stack. 🧠

shubhendup@cybermedia.co.in

DATAQUEST JUNE 2026 EDITION: AI ROI FACES ITS HARDEST TEST

ALSO READ MORE ON

- AWS and the Enterprise Realignment – Why India's Tech Wave Demands Multi-Model AI
- Claude Mythos and the Cyber Resilience Question Banks Can No Longer Avoid
 - Salesforce's New Identity – CRM Legacy Meets Digital Labour
 - Why Metadata Is Becoming the Trust Layer for Enterprise AI
- The story of the reincarnated CIO - rowing the Boat of Theseus - Ross Tisnovsky
 - Agentic is in. Humans are not out. And RPA stays - Balaji Sundararajan
 - AI's next enterprise test: moving from pilot hype to production discipline - Praveen Sridhar



Scan QR Code
& Subscribe now...

DATAQUEST 40+ YEARS CELEBRATIONS:
GET 40% EXCLUSIVE DISCOUNT ON
DATAQUEST PRINT SUBSCRIPTION
AND DATAQUEST DIGITAL
SUBSCRIPTION AT FLAT 420/- ONLY.
AVAIL THE OFFER NOW

<https://shorturl.at/vn6tN>

**FOLLOW DATAQUEST FOR REGULAR
AND LATEST UPDATES ON THE
BUSINESS OF ICT ECOSYSTEM.**



Dataquest



dataquestindia

Leverage Dataquest platform & network

Ajay Dhoundiyal | ajaydh@cybermedia.co.in | +91 99535 40318

#ImpactingICTfor4Decades

For Subscription queries:



subscriptions@cybermedia.co.in



9289870545



Brain chips, AI, and virtual worlds to reshape work by 2050

As artificial intelligence, neural interfaces and immersive platforms converge, the workforce may soon operate through connected ecosystems that transcend offices.



BY VOICE&DATA BUREAU

Neural implants and immersive digital environments could transform the workplace by 2050, enabling employees to interact with technology, colleagues and information through increasingly integrated digital ecosystems, according to a study by International Workplace Group (IWG).

The report, IWG's Work Reimagined: The Office of 2050, found that neurotechnology is the workplace innovation employees and HR leaders are most likely to expect over the next 25 years as advances in artificial intelligence (AI), computing and connectivity converge.

Neural implants are emerging as the most anticipated workplace innovation, signalling a future where human and machine interaction deepens.

The workplace of 2050 could combine immersive digital environments with responsive infrastructure tailored to employee needs and wellbeing.

The findings come as India emerges as one of the world's fastest adopters of AI. According to the study, India ranks highest globally on the AI Advantage score at 53 points, compared with a global average of 34, with 86% of employees and 90% of employers reporting productivity gains from AI. Prime Minister Narendra Modi has also outlined a vision for India to become one of the world's top three AI powers by 2047.

The research points to a future in which work is conducted through connected digital networks rather than within the confines of a single office. Around 70% of HR leaders and 75% of employees expect work to take place across multiple locations, while 64% of employees and 78% of HR leaders believe hybrid working will become the standard model by 2050.

The study also found that 66% of employees and 63% of HR leaders expect return-to-office mandates to disappear as organisations place greater emphasis on flexibility and employee autonomy.

NEURAL IMPLANTS MOVE CLOSER TO WORKPLACE USE

More than seven in 10 employees (72%) and 68% of HR leaders believe workplace technology will be unrecognisable by 2050. Neural implants, which connect the human brain directly to external devices, emerged as the most anticipated workplace technology in the study. The technology is already under development by companies including Neuralink and Synchron.

Respondents expect intelligent systems to automate complex workflows, personalise workplace experiences and accelerate decision-making. More than 70% of employees and HR leaders believe AI and automation will reshape most office-based roles over the coming decades.

AI is also expected to play an increasingly important role in workplace coordination. Around 64% of employees and 69% of HR leaders believe AI systems will determine the optimal location and

timing for collaboration, helping organisations manage increasingly distributed workforces.

The pace of business is also expected to increase. Nearly three-quarters of employees (74%) and 70% of HR leaders believe the speed of work will accelerate significantly as AI-enhanced learning and automation reduce time spent on routine activities and improve access to knowledge.

CONNECTED DIGITAL ECOSYSTEMS RESHAPE WORK

The report envisages future workplaces built on cloud, AI and immersive communications technologies. Nearly 70% of employees and HR leaders expect virtual and augmented reality meeting environments to replace many traditional workplace interactions, creating integrated workspaces that connect remote and office-based teams in real time.

Employees also expect workplaces to become increasingly responsive through cloud-connected infrastructure. Future work environments could include interactive digital surfaces, adaptive lighting aligned to individual body clocks, and systems capable of detecting fatigue and recommending recovery periods.

While technology is expected to transform how work is performed, respondents also anticipate greater emphasis on employee wellbeing. Family-friendly facilities, flexible multi-purpose workspaces and nature-inspired office designs featuring indoor gardens and natural light were identified as preferred workplace concepts for the coming decades.

The shift towards connected workplaces is already visible in India. According to Knight Frank data cited in the report, flexible workspace penetration increased from 5% of commercial office stock in 2017 to 21% in 2025. Also, large enterprises now account for 72% of seat absorption. 🌱

feedbackvnd@cybermedia.co.in

O2 trials network technology for hearing loss

The network-based call enhancement technology could improve accessibility and reduce listening effort for users.

O2 has completed a proof-of-concept trial of network-based technology designed to improve mobile phone calls for people with hearing loss, working with cloud-native network software provider Mavenir.

The trial tested a system that adapts call audio in real time based on an individual's hearing profile. Participants completed a short, automated hearing assessment that measured their perception of different sound frequencies. The resulting profile was securely linked to their mobile number, allowing the network to adjust speech delivery during calls to improve clarity.

Unlike accessibility features built into devices or third-party applications, the technology operates within O2's network. This enables users to continue making and receiving calls with their existing phones and numbers without changing their behaviour or installing additional software.

According to the trial results, nearly 90% of participants reported improved call clarity. Users said conversations were easier to follow, with fewer misunderstandings and reduced listening effort.

The trial also indicated that the technology could provide a more natural calling experience for people who struggle with conventional voice calls. One participant with profound hearing loss reported hearing calls clearly without hearing aids and needing fewer repetitions during conversations.

Virgin Media O2 said the trial explored how intelligence within the mobile core network can be used to address communication challenges faced by people with hearing loss. The company plans to further investigate the potential of network-based accessibility services following the positive results from the proof-of-concept. The project demonstrates how mobile core networks can support service innovation and deliver new capabilities for customers through software-based enhancements.



Even our coffee machine is built for 'zero latency'. It delivers coffee as soon as you start thinking about it!

Find more smiles at NormanAndOzi.com



Our cloud-native architecture is highly scalable. Just like your friend here, it easily handles massive data volumes!

Find more smiles at NormanAndOzi.com

YOUR CUSTOMERS ARE EVOLVING. LET YOUR BRAND LEAD WHERE IT MATTERS MOST. CYBERMEDIA'S INTEGRATED GO-TO-MARKET ENGINE PROVIDES INFLUENCE, VISIBILITY, AND HIGH-INTENT LEADS ACROSS INDIA'S MOST TRUSTED TECH MEDIA PLATFORMS.

LEAD THE CONVERSATION USING CYBERMEDIA'S 360° GTM STRATEGY. UNMATCHED REACH ACROSS OUR FLAGSHIP BRANDS



DATAQUEST
Enterprise &
Tech Leadership



PCQUEST
CIOs, Tech
Influencers & SMBs



VOICE&DATA
Telco & Digital
Infra Leaders



DQCHANNELS
ICT Partners &
Channel Decision Makers

OUR BESPOKE B2B MARKETING PROGRAMMES BUILD, ENGAGE AND SCALE COMMUNITIES

Account-Based CXO Connects & C-Level Roundtables | Content-Led Thought Leadership Campaigns | Audience Segmentation Across IT & Business Decision Makers | Print, Digital, Event, Podcast & Research Integration | Measurable ROI & Lead-Nurturing Programmes

High-Impact Verticals We Specialise In: Cloud & Multi-Cloud Solutions | Cybersecurity & Risk Management | Data, AI & Advanced Analytics | Enterprise IT Infrastructure & SaaS | Telecom, 5G & Network | SMBs & Mid-Market Technology Buyers | Transformation | Sustainability & Green IT | Channel Ecosystem: VARs, MSPs, Distributors, SIs | SMBs & Mid-Market Technology Buyers

DELIVER INFLUENCE AND OUTCOMES WITH CYBERMEDIA

42+ Years of Tech Publishing Legacy | Deep CXO Access & Vertical Intelligence | Custom Campaigns with Content + Conversion Focus | Trusted by Top Global & Indian IT Brands

LET'S BUILD SMART, VERTICAL-LED CAMPAIGNS THAT TURN YOUR BRAND MESSAGE INTO MEASURABLE BUSINESS IMPACT.

www.dqindia.com | www.pcquest.com | www.voice&data.com | www.dqchannels.com

Partnerships & Advertising Enquiries

Ajay Dhoundiyal – Marketing Alliances & Business Solutions : ✉ ajaydh@cybermedia.co.in, ☎ +91-9953540318



Apeejay Institute of Mass Communication

Dwarka, New Delhi | Estd. in 2003 | AICTE Approved



Empowering Future Media Leaders with Expertise, Innovation, and Excellence!

ADMISSIONS

OPEN 2026



PROGRAMMES OFFERED

FULL TIME 2 YEARS PROGRAM

- Management in Mass Communication

(CAT/MAT/XAT/GMAT/CMAT/ATMA Score Acceptable)

FULL-TIME 1 YEAR POST GRADUATE PROGRAMS*

- Television & Radio Journalism/Production
- Advertising & Marketing Communication
- Digital Media & Online Journalism
- Corporate Communication/ PR & Event Management
- Business & Financial Journalism



*Institute offers lateral entry option into 2nd year MA at Apeejay Stya University (UGC recognised) in accordance with UGC's choice based credit system.

PLACEMENTS IN TOP MEDIA HOUSES



and many more

Excellent Placement Record across various media & entertainment platforms in over 100 reputed companies.

For more information, please contact us:

Apeejay Institute of Mass Communication

Institutional Area, Sector - 8, Dwarka, New Delhi - 110077

Admission Helpline: +91-9910-222-777 | Email: aimc.del@apj.edu



Follow us on: [f](#) [in](#) [t](#)