sify

CCAOI™
Representing the ecosystem of Internet - Bharat Model

THE RESILIENCE IMPERATIVE:

BUILDING A RESILIENT AND SUSTAINABLE AI BACKBONE FOR INDIA'S DIGITAL ECONOMY

AI
IMPACT
SUMMIT
भारत 2026 INDIA

सर्वजन हिताय | सर्वजन सुखाय
WELFARE FOR ALL | HAPPINESS OF ALL

FEB 2026

TABLE OF CONTENTS

EXECUTIVE SUMMARY

India stands at a defining moment in its technological trajectory. With a digital economy projected to contribute over $1 trillion to the national GDP by 2026, the integration of Artificial Intelligence (AI) has transitioned from an aspirational goal to a systemic necessity. However, the promise of AI to revolutionize healthcare, agriculture, finance, and manufacturing is fundamentally contingent upon the resilience of the underlying infrastructure that supports it.

This report posits that resilience, defined by availability, reliability, fault tolerance, and disaster recovery, is not merely a technical specification but a strategic imperative for national stability. Our analysis identifies significant vulnerabilities in the current landscape. While India has made commendable strides in 5G deployment and digital public infrastructure, acute gaps remain in high-performance compute availability, domestic semiconductor manufacturing, and specialized AI security controls. Current reliance on imported hardware and foreign cloud regions underscores the importance of diversified supply chains to maintain operational resilience during periods of geopolitical volatility. Furthermore, the exponential energy demands of Generative AI threaten to strain national power grids, necessitating an urgent pivot toward sustainable, energy-efficient computing architectures.

To address these challenges, the report proposes a multi-layered resilience framework. For enterprises, we recommend the adoption of hybrid and multi-cloud architectures to mitigate vendor lock-in, alongside the implementation of Zero Trust security models. For the broader ecosystem, we emphasize cloud capabilities that balance elastic scalability with regulatory compliance, leveraging Sovereign Cloud infrastructure where applicable. Ultimately, building a resilient AI ecosystem requires a synchronized effort between government policy, private sector innovation, and robust infrastructure investment to ensure that India’s AI future is not only powerful but also secure, sustainable, and inclusive.

FOREWORD

This strategic report, The Resilience Imperative, is a joint collaborative effort between Sify Technologies and CCAOI. Although commissioned by Sify Technologies, the study has been developed independently with full editorial autonomy.

This study, conducted between November and December 2025, adopts a secondary research methodology. It synthesizes quantitative data from government publications, industry white papers, academic research, and credible media sources available as of January 2026. These findings are complemented by structured stakeholder consultations conducted through pre-events held in the lead-up to the India AI Impact Summit. These sessions brought together policymakers, infrastructure providers, enterprise leaders, and technology experts to validate risk assumptions and refine strategic recommendations.

The primary objective of this collaboration is to provide a harmonized, evidence-based perspective on the critical infrastructure requirements necessary to support India's burgeoning digital economy. By integrating deep operational expertise in data center and network infrastructure with broader policy insights, this report serves as a foundational document for leaders navigating the complex landscape of AI adoption.

sify

CCAOI™
Representing the ecosystem of Internet - Bharat Model

Chapter 1

THE IMPERATIVE FOR RESILIENT AI INFRASTRUCTURE IN INDIA

THE IMPERATIVE FOR RESILIENT AI INFRASTRUCTURE IN INDIA

1.1 Why is Resilient AI Infrastructure Critical?

1.1.1 Defining Resilience in the Context of AI Infrastructure

In an era where AI systems underpin mission-critical operations, infrastructure resilience has evolved from a technical metric to a strategic imperative. In the context of AI, resilience encompasses four interdependent dimensions: Availability (operational continuity), Reliability (consistent performance), Fault Tolerance (graceful degradation), and Disaster Recovery (systematic restoration). Unlike traditional IT, AI workloads are computationally intensive and data-dependent. They act as potential single points of failure that can cascade across the economy. For India, serving a population of 1.4 billion, resilience is an existential requirement.

1.1.2 AI's Expanding Role Across Critical Sectors

The pervasiveness of AI has transformed it into a foundational capability across India's critical sectors:

Healthcare: The Ayushman Bharat Digital Mission relies on digital infrastructure to interconnect over 1.7 lakh health centers. During the pandemic, the Co-WIN platform processed over 2.2 billion vaccine doses, demonstrating that infrastructure uptime is a matter of public health.

Finance: The Unified Payments Interface (UPI) processed over 12 billion transactions in December 2023 alone. With the Reserve Bank of India (RBI) noting a 46.7% decline in fraud due to AI deployment, the financial system’s integrity is now directly linked to AI uptime.

Agriculture & Manufacturing: From the Forecasting Agricultural output using Space, Agro-meteorology and Land-based observations (FASAL) program to Industry 4.0 predictive maintenance, digitized environments now tolerate near-zero latency. This makes infrastructure the bedrock of productivity.

1.1.3 The Cost of Infrastructure Failures

The cost of failure is quantifiable and rising. Industrial businesses in India face unplanned downtime costs of approximately ₹70 lakh per hour. For the broader digital economy, the average cost of a data breach reached an all-time high of ₹19.5 crore in 2024. Beyond finances, the operational cost is severe. Organizations with fragmented observability face 40% more downtime, and breaches involving shadow data take an average of 291 days to contain. Regulatory bodies like the Securities and Exchange Board of India (SEBI) and RBI have begun imposing significant penalties for resilience lapses, reinforcing that operational stability is a non-negotiable compliance expectation.

1.1.4 Current State Assessment: Gaps and Vulnerabilities

Compute Scarcity: Despite the IndiaAI Mission's target to access over 38,000 Graphics Processing Units (GPUs), India faces a structural deficit in high-performance compute clusters, such as NVIDIA H100s, creating a reliance on foreign cloud regions and supply chains.

Cloud Maturity: While the public cloud market is growing, with a projected $10.9 billion in 2024, adoption is skewed. Many legacy enterprises rely on on-premises infrastructure that lacks the elasticity required for bursting AI workloads.

Edge Readiness: India has achieved massive 5G rollout, but a disparity exists between connectivity and compute. Edge data center capacity, currently at 60 to 70 Megawatt (MW), needs to triple by 2027 to support real-time inferencing in Tier-2 and Tier-3 cities.

Security: With over 1.6 million cybersecurity incidents reported by Computer Emergency Response Team (CERT-In) in 2023, the threat landscape is intensifying. Crucially, 80% of organizations lack dedicated AI-specific security controls.

1.2 Resilience by Design: Mitigating Risks through Efficient Architectures

1.2.1 Architectural Patterns for Resilient AI Infrastructure

Translating resilience principles into reality requires adopting specific architectural patterns:

Hybrid and Multi-Cloud: Distributing workloads across providers eliminates vendor lock-in and single points of failure. Hybrid models allow enterprises to keep sensitive data on-premises to meet sovereignty needs while bursting training workloads to the public cloud.

Edge-Cloud Continuum: Distributing intelligence reduces latency and backhaul dependency. Processing inference at the edge can reduce bandwidth consumption by up to 60%, a critical factor for India's diverse connectivity landscape.

Zero-Trust Security: Traditional perimeters fail in distributed AI environments. Adopting a 'never trust, always verify' model has been shown to save Indian organizations an average of ₹9.5 crore in breach costs and reduce containment time by over 150 days.

1.2.2 Sustainability Integration: Energy Efficiency as Resilience Enabler

Sustainability is now a resilience metric. Training a single large language model can consume 1,287 Megawatt- hour (MWh) of electricity, equivalent to 120 households' annual usage. For India, where power availability can be constrained, energy efficiency is vital.

Efficient Compute: Specialized accelerators like GPUs and Tensor Processing Unit (TPUs) offer 10 to 100 times better performance-per-watt than Central Processing Units (CPUs).

Advanced Cooling: Liquid and immersion cooling are essential to lower Power Usage Effectiveness (PUE) ratios.

Carbon-Aware Computing: Intelligent scheduling that shifts workloads to times of high renewable energy generation can reduce the carbon footprint by approximately 35% and reduce stress on the grid during peak hours.

sify

CCAOI™
Representing the ecosystem of Internet - Bharat Model

Chapter 2

KEY CHALLENGES TO BUILDING RESILIENT AND SUSTAINABLE AI INFRASTRUCTURE

KEY CHALLENGES TO BUILDING RESILIENT AND SUSTAINABLE AI INFRASTRUCTURE

2.1 Technical Infrastructure Challenges

2.1.1 Compute and Storage: The Foundation Under Strain

India faces a Compute Deficit. Procurement lead times for high-end GPUs often exceed 4 to 6 months, forcing reliance on foreign infrastructure. While the Semicon India Programme is building domestic capacity, the focus on mature nodes means dependence on imported advanced chips (5 nanometer) will persist. Furthermore, the Digital Personal and Data Protection Act, 2023 (DPDP) data localization requirements create a looming storage gap. India needs to double its data center capacity to approximately 2.5 GW by 2027 to handle sovereign data demands.

2.1.2 Network Reliability and Connectivity Disparities

While urban 5G is robust, the fiber deficit in rural areas remains a bottleneck for agricultural and healthcare AI. Furthermore, quality of service varies. Real-world jitter in Tier-2 cities often exceeds the benchmarks required for mission-critical industrial AI, creating a reliability glass ceiling.

2.1.3 Security Preparedness and Threat Landscape

The attack surface is expanding. Adversaries now use AI to automate ransomware attacks, while data poisoning and model extraction represent new threat vectors. Despite this, fewer than 20% of Indian organizations rigorously test models for adversarial robustness before deployment.

2.1.4 Energy and Sustainability: The Resource Constraint

AI energy demand is outpacing general grid growth. India's data center power consumption is projected to quadruple to 57 Terawatt-hour (TWh) by 2030. Geographic concentration creates localized stress. Hubs like Mumbai face power deficits during peak summer months, increasing the risk of outages. Reliance on fossil-fuel backup generators during grid instability further compromises sustainability goals.

2.1.5 Interoperability: The Integration Challenge

Vendor lock-in is a systemic risk. Data Gravity and prohibitive egress fees, costing upwards of ₹75 lakh to move a petabyte of data, make multi-cloud strategies economically difficult. Unlike the payments sector with UPI, the AI stack lacks a unified standard for compute interoperability, creating engineering overhead and limiting the mobility of startups.

2.2 Operational and Governance Challenges

2.2.1 Cybersecurity Vulnerabilities

The frequency of breaches is rising, with the average cost hitting ₹19.5 crore in 2024. State-sponsored Advanced Persistent Threats (APTs) actively target Indian critical infrastructure and research institutions. The Preparedness Gap is significant. Audits reveal that many facilities lack redundant Security Operations Centers (SOCs), creating single points of failure.

2.2.2 Regulatory Uncertainty

India's regulatory framework is in flux. While the DPDP Act is law, subordinate rules regarding consent and exemptions are pending. Sectoral fragmentation between bodies like the RBI, ICMR, and SEBI creates overlapping compliance mandates. Additionally, the Brussels Effect of the EU AI Act imposes extraterritorial compliance burdens on Indian IT firms serving global markets, increasing the cost of innovation.

2.2.3 Skills Shortages: The Talent Gap

A severe talent crunch threatens infrastructure stability. Demand for AI professionals is expected to reach 1 million by 2027, yet the supply gap for critical roles like AI Architects and Security Specialists ranges between 51% and 73%. This shortage is exacerbated by geographic concentration, as 68% of talent is in Tier-1 cities, and high attrition rates prevent the retention of institutional knowledge.

2.2.4 Best Practices Currently Adopted

Despite challenges, leaders are adapting.

HDFC Bank employs an AI-First strategy with active-active architectures to ensure UPI uptime.

Flipkart utilizes Edge AI to process logistics decisions locally, mitigating connectivity issues.

Industry Frameworks: Adoption of National Association of Software and Service Companies (NASSCOM) Responsible AI guidelines and Data Security Council of India (DSCI) security frameworks is growing, with 60% of surveyed businesses maturing their governance practices.

Chapter 3

STRATEGIC RECOMMENDATIONS FOR BUILDING RESILIENT AI INFRASTRUCTURE

STRATEGIC RECOMMENDATIONS FOR BUILDING RESILIENT AI INFRASTRUCTURE

The construction of resilient AI infrastructure requires coordinated action across stakeholder groups. The following recommendations prioritize a balance between ambitious developmental goals and operational feasibility.

3.1 For Enterprises

Institutionalize Data Infrastructure Readiness: Mandate Data Infrastructure Readiness Assessments prior to scaling. Evaluate data lineage and legacy interoperability to ensure scaled systems are auditable.

Adopt Resilient Hybrid and Multi-Cloud Architectures: Mitigate vendor dependency by distributing workloads. Use containerization (Kubernetes) and service meshes to abstract cloud-specific services. Implement rigorous, regularly tested Disaster Recovery (DR) plans specific to AI systems.

Implement Secure-by-Design and Zero Trust: Embed security from inception via threat modeling and adversarial robustness testing. Transition to Zero Trust architectures with identity-based access and micro-segmentation. Augment SOCs with AI-driven threat detection under human oversight.

Build Comprehensive Observability: Establish visibility across infrastructure, application, and model layers. Institutionalize blameless post-mortems to drive continuous cultural improvement.

Treat Sustainability as Resilience: Adopt energy-efficient hardware, such as accelerators, and efficient workloads like quantization. Implement circular economy principles for hardware lifecycle management.

Establish Robust Governance: Formalize ethics boards and use documentation standards like model cards. Invest systematically in workforce upskilling and cross- functional infrastructure teams.

3.2 For Ecosystem Stakeholders

Develop Open Standards: Industry bodies like NASSCOM and DSCI should create open reference architectures for resilience and security. These should be backed by incentives for adoption by smaller players.

Deepen Academia-Industry Collaboration: Focus research and curriculum design on India-specific challenges, such as low-resource language models and edge deployment in connectivity-constrained settings.

Promote Regulatory Sandboxes: Establish controlled environments that allow for proportionate, experimentation-friendly governance. This allows regulators to gather data on risks without stifling early-stage innovation.

3.3 For Infrastructure Providers

Invest in AI-Ready, Sovereign Infrastructure: Upgrade facilities for high-density GPU workloads using liquid cooling. Offer Sovereign Cloud options that satisfy local data residency requirements while retaining public cloud elasticity.

Provide Deterministic Edge Connectivity: Deploy Software-Defined Wide Area Network (SD-WAN) and fiber backbones deep into Tier-2 and Tier-3 cities to support distributed inference and reduce the digital divide.

Offer Converged Security: Provide Zero Trust by Default services, such as Security Operations Center (SOC)-as-a-Service. Bridge the gap between physical and digital security by integrating biometric surveillance with cyber threat intelligence.

3.4 For Government and Regulators

Incentivize Resilience: Tie Production Linked Incentive (PLI) schemes and subsidies to measurable resilience metrics like DR standards and PUE targets. Create a harmonized National AI Infrastructure Resilience Framework.

Operationalize Compute as a Digital Public Good: Accelerate the National Compute Grid under the IndiaAI Mission. Treat compute as a utility, accessible via open APIs, to democratize access for startups.

Mandate Green Energy Integration: Require new hyperscale facilities to source a minimum percentage of power from renewables, aligning digital growth with Net Zero targets.

Strengthen the Talent Pipeline: Fund Centers of Excellence in AI Engineering and Infrastructure Security, specifically expanding these programs beyond traditional tech hubs.

CONCLUSION

The resilience of Indian AI infrastructure is not a static state but a dynamic capability that emerges from the conscientious and synchronized efforts of policymakers, enterprises, and infrastructure providers.

By aggressively implementing the strategic recommendations outlined in this report, ranging from architectural modernization within enterprises to robust supply-side investments by infrastructure companies, India can secure its position not merely as a consumer of artificial intelligence, but as a global leader in the deployment of robust, secure, and sustainable AI infrastructure.

The successful execution of this vision will determine the nation's ability to harness the transformative potential of AI to drive economic growth and social inclusion while rigorously safeguarding digital sovereignty and stability for future generations. India’s AI future hinges on embedding **resilience-by-design, security, interoperability,** and **sustainability** into the national AI backbone.

Note: This is a condensed version of the full report. For detailed analysis, complete data sources, and comprehensive footnotes, please refer to the complete report "The Resilience Imperative: Building a Resilient and Sustainable AI Backbone for India's Digital Economy.”

About Sify

Sify Technologies Limited is India's trusted sovereign foundation for enterprise AI, built on intelligent networks, data centers, cloud and AI, cyber security, and managed services. Recognized as IndiaAI Mission & MeitY Cloud Partner, Sify empowers organizations to Build, Run, and Govern AI at scale. For over two decades, Sify's resilient digital backbone has powered India's growth story, delivering strategic value to over 10,000 businesses.

About CCAOI

Established in 2009, CCAOI is a trust committed to capacity building, research, and advocacy in Internet and digital policy. CCAOI has evolved into a platform championing the interests of diverse actors across India's Internet ecosystem, representing both connected and unconnected users on issues spanning telecom, Internet, digital policy, and governance.

For Business Enquiry

marketing@sifycorp.com

Know More