B-DIA
Bharath Digital Infrastructure Association

KNOWLEDGE PARTNERS

rishihood university

I·D·F

CONSOCIA ADVISORY

DATA SWARAJ FOR SECURE DIGITAL INDIA

NATIONAL IMPERATIVE FOR DIGITAL AUTONOMY

A NATIONAL EMERGENCY

Authored By: Soham Ghosh, Consultant-Research and Insights, BDIA

DATA SWARAJ for SECURE DIGITAL INDIA

Contents

Executive Summary

India's ascent as an emerging global superpower is underscored by significant milestones. The nation achieved political independence in **1947**, followed by a transformative economic liberalization in **1991**, dismantling the constraints of the License Raj. Over the subsequent three decades, India has witnessed remarkable progress, becoming the **fastest-growing major economy**, the **fifth-largest globally**, boasting the **third-largest start-up ecosystem**, the **fourth most valuable capital market**, the **third-largest aviation market**, and holding the rank of the **fourth most powerful military worldwide**

Beyond these achievements, India stands as a **world leader in real-time payments (RTP)**, a phenomenal milestone achieved and now being replicated globally through its innovative UPI technology. In **2023**, India accounted for an astounding **49% of all global RTP transactions**, surpassing the combined volume of the top ten other real-time payment markets.

As the world transitions into the "data economy," India stands at a critical juncture in pursuing **digital sovereignty**. Data, often called the ***"new oil,"*** has become the **foundation of global power dynamics**. Just as India secured independence in 1947 and championed economic self-reliance in 1991, it must now assert **data autonomy** by investing in sovereign cloud infrastructure. This is not merely a technological evolution but a **strategic necessity—**essential for **protecting national security, ensuring economic self-sufficiency, and safeguarding citizen privacy in an era dominated by global tech giants like AWS, Microsoft, and Google.**

As of April 2024, 95.15% of villages have access to the internet in India with 3G/4G mobile connectivity. Total internet subscribers have witnessed an extraordinary **400% growth in just ten years**, surging from 251.59 million in March 2014 to **954.4 million by March 2024**, nearing a billion users.**!!** India's remarkable **digital transformation, fuelled by this vast user base and the ambition of a $1 trillion digital economy by 2030, faces an existential threat: foreign control over its cloud and data infrastructure.**

Alarmingly 90% of India's cloud market dominated by U.S. hyperscalers (AWS, Azure, Google Cloud), exposing sensitive data to extraterritorial laws like the **U.S. CLOUD Act and surveillance under FISA Section 702, alongside the Patriot Act.** These laws directly conflict with India's local data privacy laws, subjecting various sensitive data to foreign control. This paper will **explore the alarming threats posed by legal complexities of these extraterritorial laws, which compel these tech giants to disclose any data they handle in their home country government, irrespective of data ownership concerns.**

India's cloud service market is experiencing robust growth, currently valued at **$12.75 billion in 2025**, (a significant increase from **$4.23 billion in 2020** with CAGR of 24.5%), and projected to reach **$36.70 billion by 2030** at a CAGR of 23.54%. However, the combined market share of major global providers (AWS, Azure, Google, and others like IBM/Oracle) constitutes approximately **90% of the Indian cloud market—**virtually the entire market is served by global cloud companies. The "big three" (AWS, Azure, Google) alone account for roughly 65% of this dominance.

This dominance translates to an estimated **annual revenue loss of $10.5 billion USD** flowing out of India to pay for the cloud services of global hyperscalers—an amount equivalent to the current Union Health Budget. This outflow not only exacerbates current account deficits from a macroeconomic perspective but also deprives highly capable Indian start-ups of the opportunity to serve their nation in the cloud services space. If this dominance by foreign tech cartels is allowed to persist amidst the exponential growth of the digital economy, the revenue loss to global cloud service providers could reach a staggering **$30 billion USD by 2030—**equivalent to 2.5 times the current education budget and 3 times the current health budget of the country.

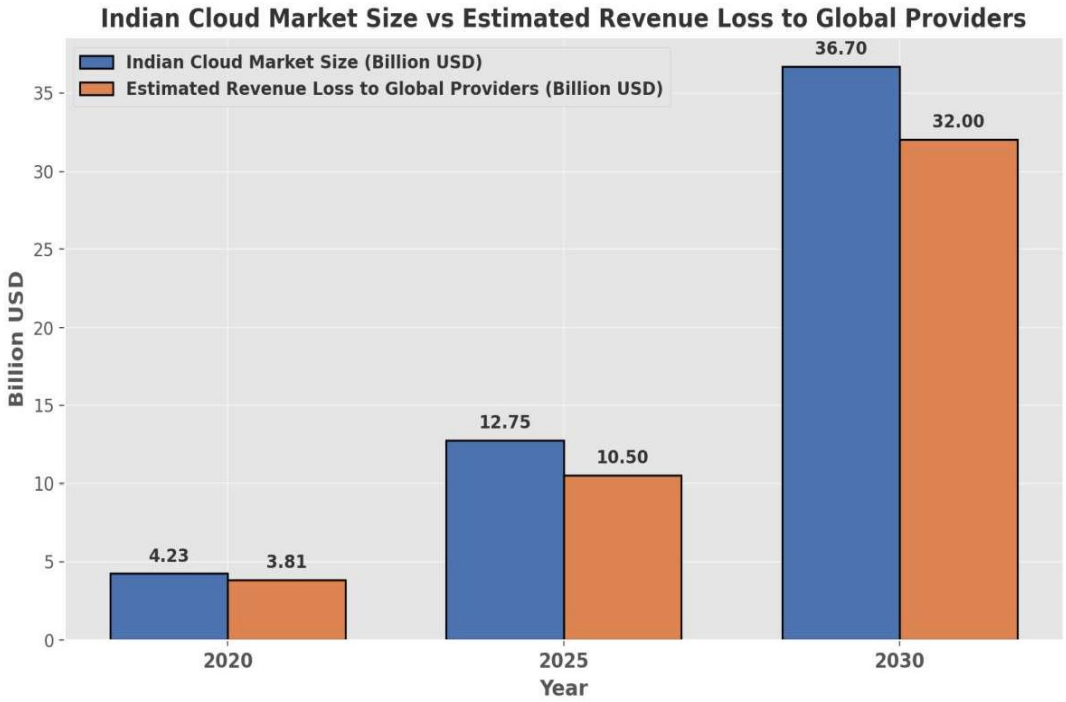


Figure 1

Allowing the **dominance of foreign tech giants risks a modern-day "digital colonialism" in India**, echoing the East India Company era, which began with trade and culminated in colonial rule. These Big Tech entities are essentially repurposing Indian data and selling it back as AI, a scenario that increasingly resembles "East India Company Part 2" in the digital age. The scrutiny faced by AI solutions like OpenAI and Grok3 AI, not only from the Government of India and Indian businesses but also from numerous nations and enterprises worldwide, underscores this growing concern.

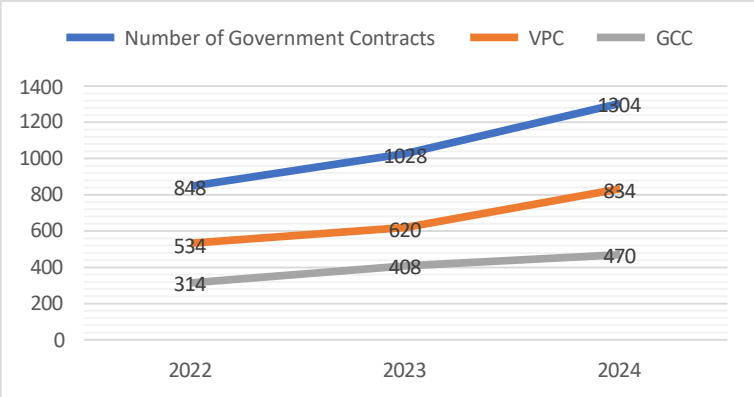
Furthermore, the Five Eyes alliance, an intelligence network linking the United States, the United Kingdom, Canada, Australia, and New Zealand, has evolved into a comprehensive surveillance system. Originating in World War II, it now collects and analyzes vast amounts of electronic data, from signals intelligence to communications metadata, ostensibly to enhance national security. However, such extensive surveillance, even when aimed at security threats, can encroach upon personal privacy and civil liberties, particularly when the data of citizens from non-member countries is inadvertently captured.

In India, the Public Sector Banks' Association (PSBA), comprising twelve public sector banks including SBI, PNB, and Bank of Baroda, has chosen AWS to facilitate cloud adoption for its members, who handle highly sensitive financial data. Similarly, critical national infrastructure like the National Health Authority (NHA) and the Government e-Marketplace (GeM) rely on AWS to scale their digital operations, further exposing sensitive citizen and transactional data to foreign cloud infrastructure. Hospitals like AIIMS[1] And private chains still rely on foreign cloud service providers, exposing critical health data.

Our **analysis of government contracts** over the last three years (2022–2024) reveals the following:

[1] https://405d.hhs.gov/post/detail/ac4a5b61-2335-4768-b83b-40763bd6fef6

Table 1:Source: nexdigm Research



The **data unequivocally demonstrates a robust adoption of Cloud Services, with a growing preference for the Virtual Private Cloud (VPC) model**. This significant shift raises critical concerns regarding data sovereignty, as increasingly sensitive government data is being managed beyond the secure perimeter of government-controlled infrastructure.

India's dependence on foreign cloud infrastructure represents a modern form of digital colonization. To safeguard its digital economy, India must prioritize sovereign cloud infrastructure, just as it did with its strategic advancements in space (ISRO) and nuclear technology. The path to becoming a global cloud superpower begins with **Data Swaraj**. The time to act is now, before escalating geopolitical tensions further compromise our digital autonomy.

This white paper examines why establishing sovereign cloud infrastructure is not just important, but a national imperative. It presents a three-phase roadmap to securing India's digital sovereignty through legislative reforms, domestic capacity building, and strategic international partnerships. By synthesizing legal, economic, and geopolitical insights, the paper positions sovereign cloud infrastructure as a defining strategic priority for India's digital future.

This is a call to action for policymakers, industry leaders, and citizens to protect the nation's digital future and achieve Data Swaraj, where we guarantee global connectivity while also maintaining full local strategic control of our data. Now is the time for India to take the lead in shaping the Global Data Governance Architecture, which involves managing data governance among state, non-state actors, and individuals, as well as overseeing data flows across borders.

Problem Statement: India's dependence on foreign hyperscalers for cloud services undermines its digital sovereignty, exposing sensitive data to extraterritorial legal regimes and resulting in significant economic leakage.

- **Exposure to Foreign Jurisdiction:** Reliance on U.S.-based cloud providers subjects critical government, financial, and healthcare data to extraterritorial laws such as the CLOUD Act and FISA Section 702, which can mandate data disclosure to foreign authorities. (*Fisher-Streinz* [2] *(2022) commented that international investment law is being amended to impose new*

[2] Fisher, A., & Streinz, T. (2021). Confronting data inequality. Colum. J. Transnat'l L., 60, 829

frameworks such as 'data-as-a-resource', which will seek to more strongly protect data ownership rights, and bring to a near standstill efforts to redistribute data.

- **National Security Risks:** Unauthorized surveillance and data exploitation jeopardize the integrity of sensitive information, eroding public trust and national security.
- **Economic Drain and Innovation Stifling:** With an estimated **$10.5 billion drained annually to foreign providers,** India loses revenue while domestic cloud innovation and job creation remain constrained.
- **Barrier to Indigenous Cloud Growth:** The dominance of global tech giants restricts the development of a competitive, homegrown cloud ecosystem, reinforcing a cycle of digital colonialism.

Hypothesis: Establishing a sovereign, open, and interoperable cloud ecosystem—with local data residency, Indian-controlled encryption, Indian IP Address, and incentives for domestic start-ups—will reduce dependency on foreign providers, secure sensitive data, and position India as a global leader in cloud services.

- **Enhanced Data Sovereignty:** Mandating local data storage and Indian management of encryption keys will ensure that sensitive data not just remains within Indian jurisdiction, free from extraterritorial legal challenges, but more importantly,also ensure "Data Attainability"
- **Improved National Security:** A robust, locally governed cloud infrastructure will protect against unauthorized surveillance and data breaches, thereby strengthening national security.
- **Economic and Innovation Boost:** Reducing reliance on foreign clouds will capture lost revenue and stimulate the growth of indigenous cloud services, creating a vibrant start-up ecosystem that drives cost-effective innovation.
- **Global Competitiveness and Export Potential:** An open, federated cloud ecosystem based on an Indian cloud stack can serve not only domestic needs but also be exported to developing countries, positioning India as a competitive, cost-effective global cloud leader.
- **Resilient and Interoperable Digital Infrastructure:** Leveraging standardized, open protocols will lower migration costs, enhance system flexibility, and future-proof India's digital infrastructure against evolving technological and geopolitical challenges.
- **Data as a Public Good:** The need for data-sharing policies and incentives for reducing transaction costs in data markets, i.e., instead of curating data from scratch, markets can allow one to procure data sets that could be repurposed for a given objective.

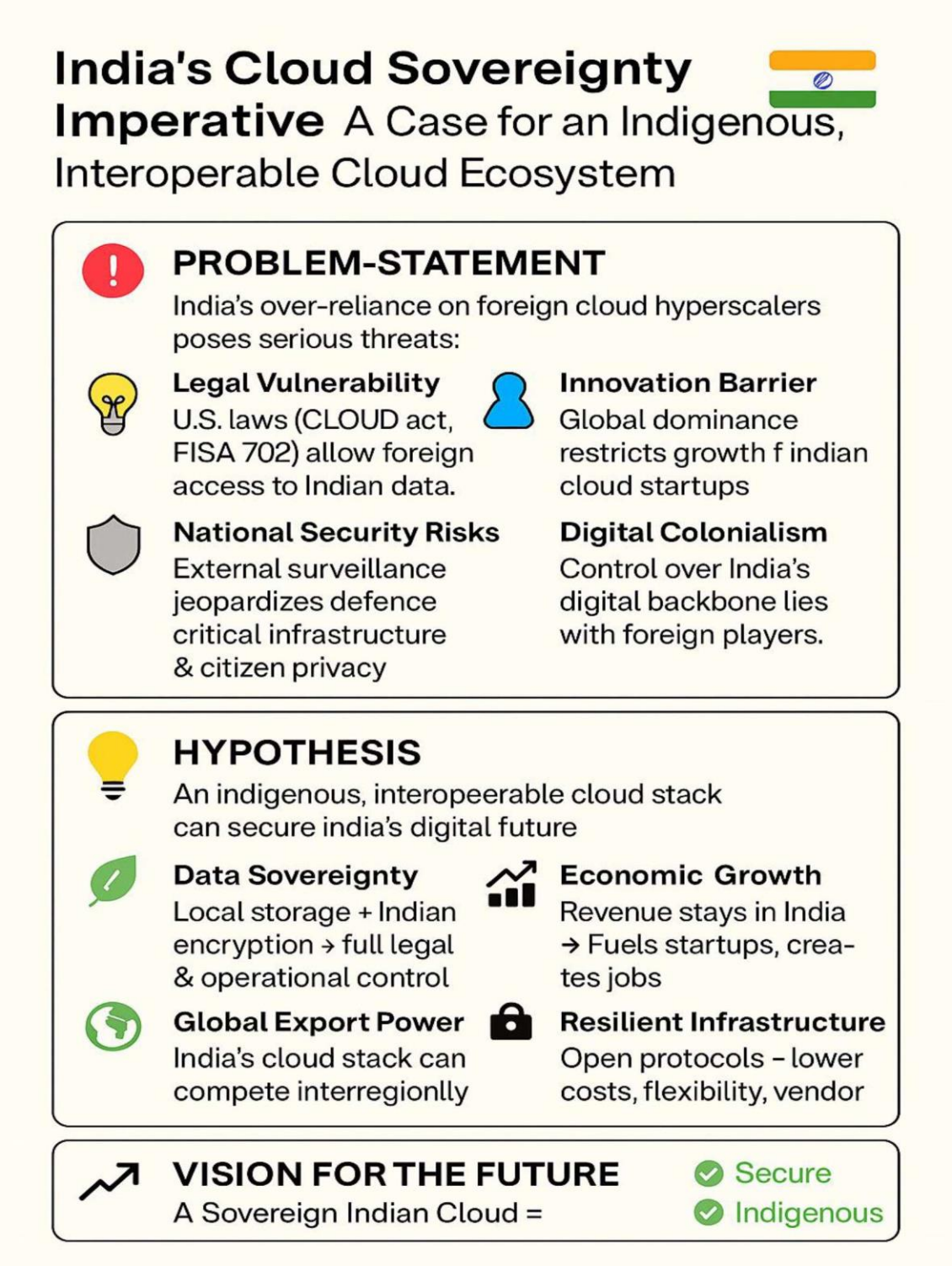

India's Cloud Sovereignty Imperative A Case for an Indigenous, Interoperable Cloud Ecosystem
PROBLEM-STATEMENT
India's over-reliance on foreign cloud hyperscalers poses serious threats:
Legal Vulnerability
U.S. laws (CLOUD act, FISA 702) allow foreign access to Indian data.
Innovation Barrier
Global dominance restricts growth f indian cloud startups
National Security Risks
External surveillance jeopardizes defence critical infrastructure & citizen privacy
Digital Colonialism
Control over India's digital backbone lies with foreign players.
HYPOTHESIS
An indigenous, interopeerable cloud stack can secure india's digital future
Data Sovereignty
Local storage + Indian encryption → full legal & operational control
Economic Growth
Revenue stays in India → Fuels startups, crea-tes jobs
Global Export Power
India's cloud stack can compete interregionlly
Resilient Infrastructure
Open protocols – lower costs, flexibility, vendor
VISION FOR THE FUTURE
A Sovereign Indian Cloud =
Secure
Indigenous

Figure 2

DATA SWARAJ for SECURE DIGITAL INDIA

Introduction

Historical Context: From Colonialism to Data Colonization

India's Sovereignty Journey: From Political Freedom to Digital Self-Determination:

1. **1947**: **Political Independence:** India broke free from colonial rule, gaining control over its political destiny.
2. **1991**: **Economic Liberalization:** While opening up the economy catalyzed growth, it also deepened India's dependence on foreign technology and digital infrastructure.
3. **1998**: **Digital Trade Constraints:** At the WTO Geneva Ministerial, India became a signatory to the global moratorium on customs duties for electronic transmissions—marking a pivotal moment in the onset of data colonisation, as it restricted India's ability to regulate and tax cross-border digital trade.
4. **2025**: **The Age of Digital Colonialism:** Data, now widely recognized as the "new oil," is predominantly stored, processed, and monetized by foreign cloud providers. This concentration of power represents a modern form of di gital colonialism, where control over India's digital economy lies outside its borders.
    - **Case in Point:** Just as the East India Company monopolized India's trade 200 years ago, today's Big Tech firms dominate the country's digital infrastructure—shaping data flows, monetization models, and digital governance. This unchecked dominance echoes the extractive practices of the colonial era, now in a digital avatar.

India's Digital Transformation and the Rise of Digital Public Infrastructure (DPI)

Over the past two decades, India has emerged as a global leader in developing **Digital Public Infrastructure (DPI)**—a transformative framework of open, interoperable systems that has democratized access to governance, financial services, and essential citizen-centric programs for its 1.4 billion people. This remarkable journey, powered by innovation, public-private collaboration, and forward-thinking policy, can be traced through a series of landmark milestones:

1. Foundational Pillars (2000–2010)

- **Aadhaar (2009)**: Launched as the world's largest biometric identification program, Aadhaar assigned a unique 12-digit ID to over 1.3 billion Indians. It played a transformative role in eliminating ghost beneficiaries and enabling direct, targeted delivery of welfare services at scale.
- **National e-Governance Plan (NeGP, 2006):** A landmark initiative to digitize governance, NeGP established critical service delivery infrastructure such as Common Service Centers (CSCs), ensuring access to essential government services in rural and underserved areas.

2. Financial Inclusion Revolution (2010–2016)

- **Jan Dhan Yojana (2014)**: Enabled over 500 million unbanked citizens to open bank accounts, forming the foundation of the **JAM Trinity** (Jan Dhan–Aadhaar–Mobile) for inclusive financial access.
- **Unified Payments Interface (UPI, 2016)**: Transformed India's digital payments ecosystem with real-time, low-cost, peer-to-peer transactions. By 2023, UPI was processing over **10 billion transactions monthly**, outpacing credit card usage and becoming a global benchmark.
- **Direct Benefit Transfer (DBT)**: Utilized Aadhaar to directly deliver subsidies and welfare payments to beneficiaries, eliminating intermediaries and saving the exchequer **₹2.2 lakh crore (approx. $27 billion)** by reducing leakages and fraud.

3. Scalable Platforms (2015–2021): Laying the Digital Rails for Bharat

- **Goods and Services Tax Network (GSTN)**: Seamlessly unified India's previously fragmented tax regime, onboarding over **14 million taxpayers** onto a single digital platform and enabling real-time compliance and transparency.
- **DigiLocker (2015) & Government e-Marketplace (GeM, 2016):** Together, these platforms digitized over **5 billion documents**, including educational certificates, licenses, and procurement records—significantly reducing bureaucratic friction and enabling paperless governance.
- **Parivahan Sewa**: A flagship initiative of the **Ministry of Road Transport and Highways (MoRTH)**, it modernized vehicle registration, driver licensing, and transport-related services, bringing uniformity and efficiency across state-level systems.
- **Open Network for Digital Commerce (ONDC, 2021)**: Aimed to **democratize e-commerce**, ONDC empowered small retailers and MSMEs by breaking the monopoly of large platforms and fostering an open, interoperable digital marketplace.

4. Global Recognition and Impact

- **Financial Inclusion**: India's Digital Public Infrastructure (DPI) has significantly reduced the unbanked population, from **47% in 2011** to **just 20% in 2023**, enabling millions to access formal financial systems.
- **Ease of Living**: Today, over **80% of Indians** access essential public services such as ration distribution, pensions, and healthcare through digital platforms, enhancing transparency, efficiency, and citizen empowerment.
- **Global Leadership**: India's pioneering **India Stack** (Aadhaar, UPI, DBT) has emerged as a global model for digital governance, inspiring adoption and replication in countries like **the Philippines, Morocco, and Indonesia**.

5. Challenges and the Road Ahead

- **Bridging the Digital Divide:** Nearly 40% of rural India still lacks internet access, underscoring the urgent need for nationwide digital infrastructure expansion to ensure inclusive access to digital public goods and services.
- **Data Privacy, Protection & Attainability**: With the implementation of the **Digital Personal Data Protection Act (2023)**, India must now strike a delicate balance between enabling innovation and ensuring robust data safeguards. Additionally, ensuring **data attainability**—i.e., sovereign and timely access to data stored on cloud platforms—must become a strategic priority.
- **Cybersecurity Imperatives**: As cyber threats targeting critical infrastructure grow in scale and sophistication, India must bolster its cybersecurity posture through advanced threat detection, incident response capabilities, and international collaboration on cyber norms.
- **Open-Source Policy and Vendor Neutrality**: There is a pressing need to reform government cloud and data centre RFPs by:
    - Mandating the **disclosure of source code**, especially in cases involving public deployment.
    - Avoiding biased terminologies like "Native Services" that promote proprietary platforms over open technologies.

  Such measures will not only foster **vendor-neutral procurement** but also promote **indigenous Cloud Service Providers (CSPs)** and create an enabling environment for **third-party software OEMs**, reducing dependency on closed, foreign technologies.
- **Inspections & Audits***:* Many foreign Cloud Service Providers (CSPs) and OEMs seek to limit physical audits and deny source code access—even for backdoor checks and cybersecurity audits—citing business sensitivities. However, for developing nations, the ability to **mandate audits and inspections** is critical. Restricting this policy space risks weakening oversight over foreign technologies and undermining national efforts to:
    - Detect cybersecurity vulnerabilities.

- Ensure algorithmic transparency and accountability.
- Protect citizens from biased or exploitative decision-making systems.

6. Advancements in Data Infrastructure and Emerging Technologies (2021-2025)

Between 2021 and 2025, India has witnessed rapid expansion of its data infrastructure, fueled by accelerated digital adoption, the nationwide rollout of 5G, and major investments in data center capacity. This transformative period also marked the mainstream integration of emerging technologies such as **artificial intelligence (AI)**, **quantum computing**, and **blockchain** across key sectors of the economy.

Expansion of Data Centres: India's data center industry is experiencing rapid growth. Valued at approximately **USD 5.7 billion in 2024**, the market is projected to more than double, reaching **USD 12 billion by 2030**, with a **CAGR of around 13%** between 2025 and 2030. This expansion is driven by rising internet penetration, increasing demand for cloud computing, government-led digitalization efforts, and growing data localization requirements from service providers. Notably, global tech giants are making substantial investments in India's data infrastructure. **Microsoft**, for example, has announced a **$3 billion investment** to expand its **Azure cloud** and **AI capabilities** in India over the next two years, underscoring the country's strategic importance as a global digital hub.

Integration of Emerging Technologies: The Indian government has been proactive in promoting the adoption of emerging technologies to drive inclusive growth. The **National Strategy for Artificial Intelligence**, launched by **NITI Aayog**, aims to harness AI across critical sectors such as healthcare, agriculture, and education. India's AI market is expected to reach **$8 billion by 2025**, growing at a **CAGR of over 40%** between 2020 and 2025[3]. In the realm of **quantum computing**, the **U.S.–India Initiative on Critical and Emerging Technology (iCET)**, established in 2022, has paved the way for bilateral collaboration in cutting-edge domains including **quantum technologies** and **semiconductors**, reinforcing India's commitment to building future-ready digital capabilities.

Key Takeaways

*India's Digital Public Infrastructure (DPI) journey—driven by frugal innovation and a commitment to inclusivity—has transformed governance and enabled broad-based economic participation. By 2030, this infrastructure is set to anchor a **$1 trillion digital economy**, empowering citizens at scale and positioning India as a global leader and exporter of DPI models. However, sustaining this momentum will require **closing access gaps** and ensuring **ethical, transparent, and accountable tech governance**.*

Market Snapshot Cloud Service Providers

India's cloud computing market has witnessed rapid expansion in recent years, driven by digital transformation across sectors. However, the market remains heavily dominated by global cloud service providers, with **Amazon Web Services (AWS)**, **Microsoft Azure**, and **Google Cloud Platform (GCP)** leading in market share. Below, we outline the most recent available data (circa 2023) on these providers' market share in India, including their combined share, other notable players, and differences in adoption between the private sector and government. We also break down the cloud market by service categories – Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

[3] https://www.linkedin.com/pulse/artificial-intelligence-india-2025-loganayaki-b-lqdkc#:~:text=Machine%20learning%20and%20internet%20information%E2%80%A6&text=The%20Artificial%20Intelligence%20(AI)%20market,40%25%20from%202020%20to%202025.

Market Share of Key Global Cloud Providers in India

AWS, Azure, and Google Cloud: AWS is the clear market leader in India's cloud services market. Microsoft Azure holds the second position, and Google Cloud is third. According to industry analysis by Course5i,[4] As of late 2022, AWS accounted for about 32.6% of India's cloud services market, Azure about 20.8%, and Google Cloud around 11.4%[5]. This means AWS alone holds roughly one-third of the Indian market, with Azure at roughly one-fifth and Google just over one-tenth.

Other Global Players: The remaining ~35% of the market is split among other global providers and smaller players[6]. These include companies like **IBM Cloud, Oracle Cloud, Salesforce**, and others. No single one of these "others" has more than a single-digit percentage share individually in India. Globally, for example, providers like Oracle and IBM each hover in the low single digits of market share.[7], and a similar pattern is seen in India. In fact, by the first half of 2024, the **top five cloud providers together accounted for just over 60%** of the Indian market.[8].

Combined Market Share: If we consider the combined share of the major global providers (AWS, Azure, Google, and others like IBM/Oracle), it amounts to essentially **90 %+ of the Indian cloud market** – in other words, virtually the entire market is served by global cloud companies. **The "big three" (AWS, Azure, Google) alone make up roughly 65% of the market.[9]**.

This dominance underscores that **global cloud giants drive India's cloud adoption**, with relatively little market left for any purely local cloud providers.

Table 1 below summarizes the estimated market share of key providers in India:

Cloud Provider	India Market Share (approx. 2023)
Amazon Web Services (AWS)	~32–33% livemint.com
Microsoft Azure	~21% livemint.com
Google Cloud Platform (GCP)	~11% livemint.com
Other global providers (IBM, Oracle, Salesforce, etc.)	~25% (combined) livemint.com
Total (All Global Providers)	90%

Cloud Service Market Dynamics in India

India's cloud service market is on a robust growth path, with a current valuation of **$12.75 billion in 2025**, a significant increase from **$4.23 billion in 2020** (CAGR of 24.5%), and a projected value of **$36.70 billion by 2030** at a CAGR of 23.54%.

[4] https://www.ciotechoutlook.com/news/microsoft-india-revenue-soars-39-to-rs-19229-crore--nid-11451-cid-70.html#:~:text=Microsoft%20Azure%20has%20a%2020.8,to%20business%20intelligence%20platform%20Course5i

[5] https://www.livemint.com/companies/news/microsoft-india-revenue-rises-39-in-fy23-on-services-boost-11697744242328.html

[6] https://www.livemint.com/companies/news/microsoft-india-revenue-rises-39-in-fy23-on-services-boost-11697744242328.html

[7] https://www.crn.com/news/cloud/2025/aws-microsoft-google-fight-for-90b-q4-2024-cloud-market-share#:~:text=Share%20www.year%20over%20year%20compared

[8] https://www.computerweekly.com/news/366617722/Indian-public-cloud-market-set-to-hit-over-25bn-by-2028#:~:text=In%20the%20first%20half%20of,followed%20by%20IaaS%20and%20PaaS

[9] https://www.livemint.com/companies/news/microsoft-india-revenue-rises-39-in-fy23-on-services-boost-11697744242328.html

India faces two acute challenges:

- *Despite generating 20% of global data consistently for the last 5 years, it hovers around only a 2-3% range of global data storage capacity, which is a serious problem in a data-based economy in this digital world.*[10]
- *Even in the stored data, we lack strategic control of the data and face data sovereignty issues, which we discuss in this paper*.

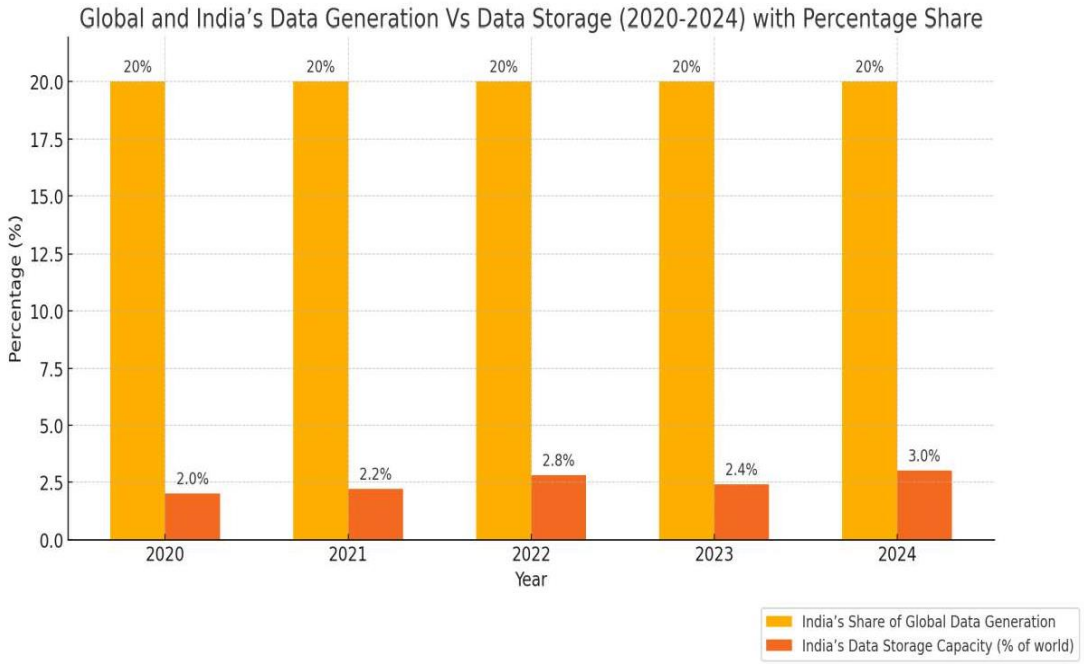


Figure 3

Cloud adoption by the Government Sector (the Nation's Critical Data)

Cloud adoption in the government sector—including central and state governments, public sector undertakings, and affiliated agencies—has been steadily increasing, though it continues to account for a relatively smaller portion of the overall market compared to the private sector.

While precise figures remain scarce, industry experts observe a growing adoption of cloud technologies by the Indian government, driven by various e-governance and digital public infrastructure initiatives. To support this shift, the government launched the "GI Cloud (MeghRaj)" initiative, aimed at promoting cloud adoption across departments[11]. Major cloud service providers have since been empanelled to deliver services for government workloads. AWS was the first global cloud provider to be empanelled by the Ministry of Electronics and Information Technology (MeitY) in 2017. By 2023, both AWS and Microsoft Azure had established multiple India regions approved for government use.[12].

[10] https://www.firstpost.com/tech/india-generates-20-per-cent-of-the-worlds-data-but-only-has-2-per-cent-of-data-centres-intels-santhosh-viswanathan-13771439.html

[11] https://aws.amazon.com/blogs/publicsector/accelerating-indias-digital-future-meity-empanels-aws-asia-pacific-hyderabad-region-government-

[12] https://aws.amazon.com/blogs/publicsector/accelerating-indias-digital-future-meity-empanels-aws-asia-pacific-hyderabad-region-government-workloads/#:~:text=Amazon%20Web%20Services%20%28AWS%29%20India,Standardization%20Testing%20and%20Quality

Government projects in healthcare, education, agriculture, and citizen services are increasingly leveraging these public clouds. Major cloud providers are actively courting public sector clients – for example, Google Cloud partnered with India's central "Bhashini" language data initiative in 2023[13] Microsoft and AWS have announced large investments in Indian data centers, partly to serve government and regulated sectors.[14]

India's cloud market encompasses all major service models—Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS)—with adoption spread across these categories. Among them, SaaS commands the largest share, accounting for an estimated 45–50% of total cloud spending. According to IDC, in the first half of 2024, the revenue ranking by category in India was: SaaS (highest), followed by IaaS, and then PaaS.

In 2018, the Government of Maharashtra issued a ***Cloud Computing Policy - Empanelment of Cloud Service Providers and Guidelines for Government organizations.***[15] This policy mandated that all government departments transition from traditional data centers to cloud infrastructure services. However, it also provided flexibility, allowing departments to select cloud services best suited to their specific needs. ***While making this choice, departments were instructed to carefully consider the nature and sensitivity of the data involved—particularly with respect to data privacy, confidentiality, matters of State and National security, and obligations under the Right to Information Act. This policy framework offers a replicable model for adoption by government organizations across the country***.

India's Digital Economy: Growth vs. Vulnerability

Exponential Data Generation

- As of March 2024, the average monthly data consumption per user in India reached 20.27 gigabytes (GB), a substantial increase from 0.27 GB in 2014-15, reflecting a compound annual growth rate of 54%.
- With an internet subscriber base of approximately 954.4 million users, comprising 556.05 million urban and 398.35 million rural users, this equates to a total monthly data consumption of about 19.34 exabytes (EB), or 232.08 EB annually.
- India's data consumption and generation are growing at an exponential rate, with the country consuming around 20% of the world's data.

Gaps in Data Storage & Cloud Infrastructure

- When it comes to **data storage and cloud services infrastructure**, India faces a significant shortfall that is not aligned with its current and future requirements.
- According to current data, India's data centre capacity represents only around 2-3% of the global data centre capacity, when we consume 20% of global data, indicating a significant under-penetration in the market despite the rapid growth in India's digital landscape.
- India's data generation, growing exponentially, is driven by 1.3 billion Aadhaar IDs, 10 billion+ UPI transactions/month, and digitization in healthcare (Ayushman Bharat), finance (Jan Dhan), and governance (e-governance initiatives, Smart Cities).

---

[13] https://www.livemint.com/companies/news/microsoft-india-revenue-rises-39-in-fy23-on-services-boost-11697744242328.html

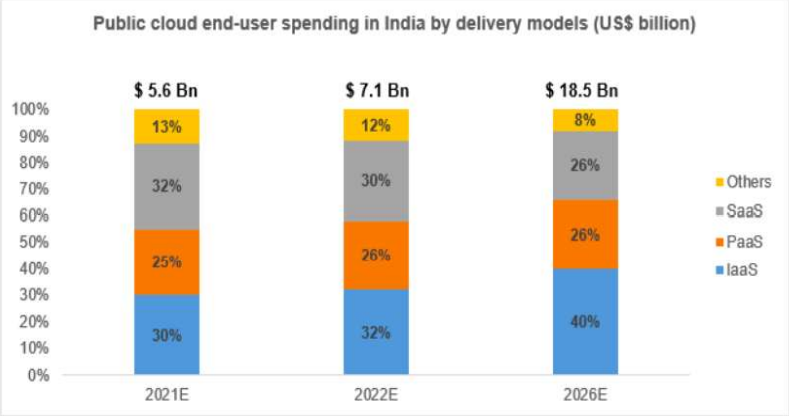
[14] https://www.business-standard.com/technology/tech-news/ai-in-india-gets-a-boost-as-microsoft-amazon-invest-billions-in-data-infra-124061800328_1.html

[15] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://exciseappeal.mahaonline.gov.in/Site/Downloads/CauseList/Test-30_08_2019%2011_14_37.pdf

- Industries such as e-commerce, BFSI, EdTech, healthtech, and entertainment along with many others are heavily reliant on large-scale data storage and computing power.

Projections

- According to recent data from IDC, the Indian Public Cloud Services market is expected to reach $24.2 billion by 2028, growing at a CAGR of 23.8%, with the revenue in 2023 standing at $8.3 billion. This indicates a significant growth trajectory for cloud services revenue in India
- Data center capacity demand to hit 1,200 MW by 2025; current supply is 144 MW (12%).



Note: E-Estimated; Infrastructure as a Service (IaaS); Platform as a Service (PaaS); Software as a Service (SaaS); Other segments like Business Process Services (BPaaS), Desktop as a service (DaaS), Disaster Recovery as a Service (DRaaS) and Cloud Management & Security Services.

Source: Oliver Wyman, NASSCOM

Figure 4

Foreign Dominance: Risks and Realities

- **Market Control**: AWS, Azure, and Google Cloud control ***most of India's cloud market***, operating under U.S. laws:
  - **CLOUD Act**: Grants U.S. authorities access to data stored globally, undermining any local regulation. It allows unilateral data seizures, threatening India's $1 trillion digital economy.
  - **FISA Section 702**: Allows warrantless surveillance of non-U.S. citizens, including retrieving all data held by US companies operating globally.
  - **Patriot Act:** Grants foreign governments access to data stored globally

This directly conflicts with local laws and puts India in a strategically disadvantageous position.

- **Virtual Private Clouds (VPCs)** refer to dedicated, isolated sections within public cloud infrastructures that allow organizations to configure and manage their own private networks, complete with customized security settings and network controls.
- These services are offered by hyperscalers and global technology giants and are widely adopted by Indian enterprises, including government entities. However, VPCs are not truly sovereign. ***Critical elements such as encryption keys, administrative controls, root IP addresses, and backup systems often remain under foreign jurisdiction***. This raise concerns around data surveillance and potential legal conflicts. Moreover, the underlying software source code is typically withheld—citing copyright and intellectual property laws—preventing independent audits. This lack of transparency limits the ability to detect backdoors or vulnerabilities, thereby posing a significant risk to national security.

- The Public Sector Banks' Alliance (PSBA), a consortium of 12 public sector banks including SBI, PNB, and Bank of Baroda, has partnered with AWS to streamline cloud adoption across its member institutions. Through this collaboration, member banks can access AWS's Community Cloud Services without undergoing separate procurement processes. AWS services will be delivered via two managed service providers —Orient Technologies and Hitachi Systems—who will support integration and limited cloud operations management for the banks.
- **The National Health Authority (NHA) and the Government e-Marketplace (GeM) rely on AWS** to scale their digital operations, inadvertently exposing sensitive national data to a foreign tech giant governed by U.S. laws**.**
- **Technical Vulnerabilities**: Recent research has uncovered critical flaws in AWS services — such as **"Shadow Resource" vulnerabilities in S3 buckets—**that could permit unauthorized access to stored data. Although these issues have since been patched, they highlight the ongoing risks posed by cloud misconfigurations and compromised credentials, which can potentially expose sensitive data to unauthorized entities, including foreign actors.
- **Economic Drain**: **$8 billion/year** flows from India to foreign providers, stifling domestic innovation.
- **Alternate Route:** In the Data Centre as a Service (DCaaS) model, local companies—such as Reliance—provide the physical foundation by offering land, developing core infrastructure (including power, cooling, and security systems), and constructing the data centre facility. Global technology firms then deploy and operate the advanced computing and networking equipment, manage the overall operations, and deliver cloud or hosting services atop this foundational infrastructure**.**

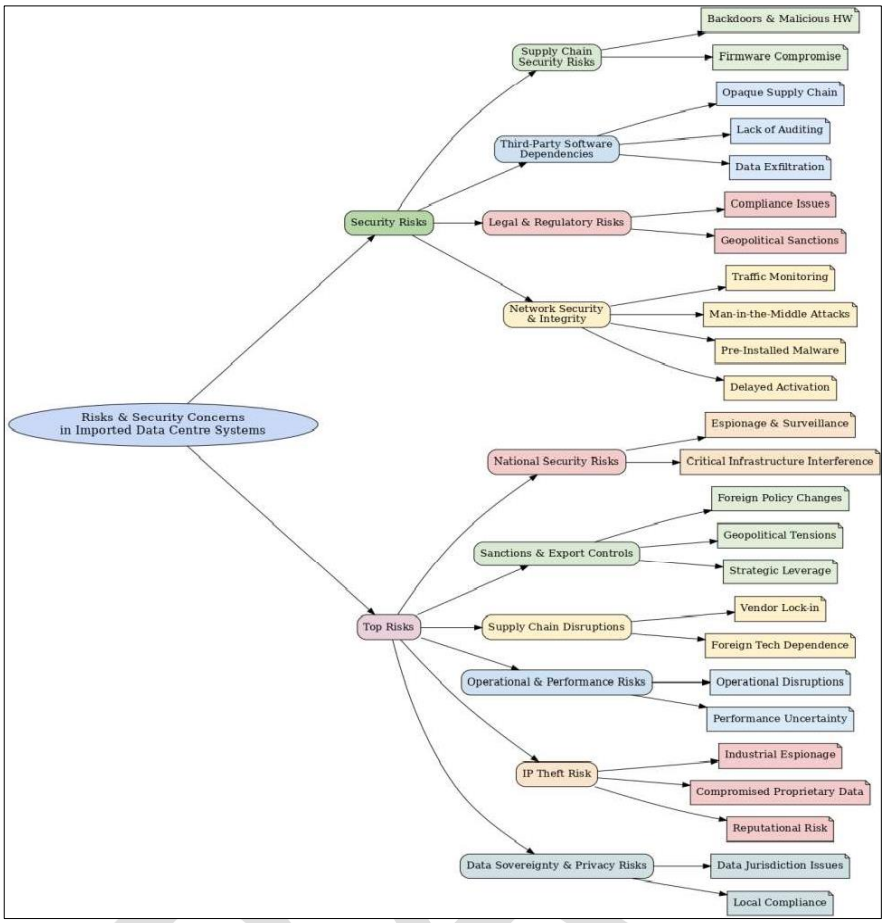


Figure 5

What is VPC?

Imagine you've built a secret, custom-designed room inside a grand, high-tech castle. This room is completely yours—you decide its layout, who can enter, and what level of security protects your valuables. You even choose where the windows and doors go.

But here's the catch: the castle itself belongs to a powerful landlord—the cloud provider—who owns the entire building. While you don't own the whole castle, your room (the VPC) is private, secure, and isolated from everyone else's. You get the freedom to build your own little kingdom within someone else's infrastructure, with complete control over your space.

Your Secret Room (The Virtual Private Cloud- VPC and Public Cloud)

- **Your Space:**
  Think of your Virtual Private Cloud (VPC) as a secret room inside a vast castle. It's your private, secure space—where you store your most valuable possessions, like sensitive data or critical applications. Just as you'd trust a locked room to guard your treasures, the VPC offers a layer of isolation within the broader cloud environment.

The Castle's Hidden Controls (Risks)

1. **The Landlord's Keys**
   Even with your own lock, the landlord —the cloud provider—holds a master key. This means they can access your room if necessary. In cloud terms, this represents the provider retaining encryption keys or administrative privileges.
2. **Castle Laws and Kingdom Rules**
   The castle exists within a larger kingdom, and the landlord must obey its laws. If the kingdom demands an inspection, the landlord might have no choice but to comply. Similarly, cloud providers may be required to hand over your data if compelled by foreign governments, even if it's encrypted.
3. **Hidden Vaults – Secret Backups**
   The landlord keeps backup copies of each room's contents in hidden vaults scattered throughout the castle. While intended for safety, these backups can become a liability—especially if stored in jurisdictions with different or weaker data protection laws.
4. **Limited Control in Emergencies**
   You may feel in charge of your secret room, but in critical situations —legal disputes, breaches, or outages—the landlord ultimately decides who gets access and when. This lack of final authority creates a layer of uncertainty.
5. **The Castle's Address Mystery**
   Even if your room is physically located in India, its postal address (IP address) might belong to another country. This geographic mismatch can complicate data sovereignty and jurisdictional claims.

Key Takeaway: A VPC or public cloud may feel like your own private space, but it's still part of a larger, externally managed system. This means that under certain legal, technical, or operational pressures, your "secret room" can be opened—exposing your critical data to outside forces.

Case Study – Jurisdictional Conflict (2024):

- A U.S. financial firm in India shared customer transaction data with U.S. agencies, violating RBI's data localization rules under DPDPA 2023.
- Bengaluru's Developers Face Rs 150 Crore Loss After Data Vanishes from AWS[16]

Sovereignty Risks in Foreign-Controlled Cloud Infrastructure

- **Jurisdictional Overreach: The Microsoft Ireland Precedent (2018)**
  In 2018, the U.S. government compelled Microsoft to hand over user data stored in Dublin, Ireland, despite the data being protected by EU's General Data Protection Regulation (GDPR). This raised concerns over cross-border data access, underscoring the risks of sovereignty violations when foreign entities control critical cloud infrastructure.
- **Encryption Key Control: The Issue of Master Keys with Hyperscalers**
  Foreign cloud providers, such as Microsoft, maintain control over encryption keys —even for data stored within Indian ter ritories. For example, Tata Power's grid data hosted in Azure's India regions remains accessible to Microsoft, highlighting the risk of unauthorized access to sensitive data controlled by foreign entities.
- **Geopolitical Coercion: The Impact of Trade Wars**
  Geopolitical tensions, such as the U.S.-China trade war, have led to disruptions in cloud services. For instance, AWS (Amazon Web Services) suspended services for Chinese firms,

[16] https://www.deccanherald.com/india/karnataka/bengaluru/cloud-over-amazon-web-services-after-builder-claims-rs-150-cr-data-loss-tech-firm-faces-fir-3408628

which impacted Indian SMEs dependent on Alibaba Cloud, demonstrating the vulnerability of Indian businesses to global political conflicts.

- **Infrastructure Deficits: Capacity Gaps and Vendor Lock-In**
  India faces a significant data center capacity deficit, with only 12% of the required capacity for 2030 currently in place. Additionally, Indian firms face substantial vendor lock-in costs. Migrating data from AWS or Azure to domestic cloud providers is four times more expensive, making it a challenging prospect for companies to reduce reliance on foreign cloud providers.

Challenges of Foreign-Controlled Cloud Infrastructure

Jurisdictional Conflicts

- **CLOUD Act Overreach**: U.S. authorities have the power to compel American cloud providers to disclose data stored in India, even when it conflicts with Indian privacy laws, such as the *Digital Personal Data Protection Act (DPDPA) 2023. While the DPDPA safeguards data protection within India, it does not address data processed outside India, or the issues of data accessibility and interoperability*. For instance, in 2024, a U.S.-based financial firm operating in India was required to share customer transaction data with U.S. agencies, which clashed with the Reserve Bank of India's (RBI) data localization mandates.
- **Copyright and Intellectual Property Restrictions**: The protection of intellectual property rights, including copyright, can limit the access of audit agencies to critical sources for evaluating vulnerabilities or detecting potential security loopholes, such as backdoor entries. This poses challenges to the Government of India's Open-Source Policy, which aims to promote transparency and secure access to software and data. The restrictive nature of IP laws hampers the broader adoption of open-source technologies, making it harder for agencies to conduct necessary audits and ensure system integrity. (https://www.meity.gov.in/static/uploads/2024/05/policy_on_adoption_of_oss.pdf)

Encryption Key Control

- Despite the establishment of local data centers, foreign service providers maintain control over the master encryption keys, compromising **India's strategic sovereignty over its data—particularly in sensitive sectors like defense, finance, and healthcare. This leaves critical data vulnerable to potential third-party decryption**

Geopolitical Risks

Dependency on Foreign Infrastructure: Excessive reliance on U.S. cloud providers exposes India to potential geopolitical risks. For instance, during the U.S.-China trade tensions, Chinese companies experienced sudden service disruptions from AWS—a scenario India can ill afford, especially in critical sectors.

Global Lessons: Sovereignty Models

EU's Gaia-X Initiative

- **Federated Sovereignty**: A consortium of European providers ensures GDPR compliance and CLOUD Act immunity.
- **Adoption**: 37% of EU enterprises use sovereign clouds.

China's Localized Cloud Dominance

- **State-Backed Ecosystem**: Alibaba Cloud controls **95%** of China's market, leveraging strict cybersecurity laws and **state-mandated encryption.**

U.S. Hyperscaler Conflicts Worldwide

- **Australia's Encryption Law (2018)**: Forced Apple/Google to share user data, sparking global privacy debates.
- **Brazil's Data Localization Push**: Mandated local storage for healthcare data after AWS leaks.

Shift from Hyperscalers: Technical, Economic, and Operational Drivers

While AWS and Azure remain dominant in the global cloud market, **emerging trends indicate increasing concerns among businesses, especially in regions like India, regarding over-dependence on these hyperscalers.** The following analysis outlines the key factors driving this shift, supported by relevant examples and data.

Cost Efficiency and Pricing Complexity

- **Hyperscaler Pricing Models:** Both AWS and Azure have intricate pricing structures, with Azure ***facing criticism for its over 30 pricing categories, which makes cost optimization difficult without constant monitoring.*** While AWS is considered more transparent, it still faces challenges related to unpredictable billing, especially in hybrid or multi-cloud environments.
- **Domestic Alternatives:** Indian firms, such as NxtGen ECS, have demonstrated up to **3x better price-performance value compared to AWS and Azure in benchmark studies**. These alternatives offer more cost-effective virtual machine (VM) pricing and optimized infrastructure for local workloads. Additionally, the Reserve Bank of India (RBI) is piloting a local cloud platform aimed at providing smaller financial institutions with affordable alternatives, reducing their reliance on hyperscalers.[17]

Data Sovereignty and Regulatory Compliance

- **Localization Requirements**: India's DPDP laws mandate that financial and government data remain within national borders. Hyperscalers like AWS and Azure have invested in Indian data centers (e.g., Mumbai and Hyderabad regions)[18]But domestic providers like NxtGen or RBI-backed solutions ensure stricter compliance with fewer cross-border data risks.
- **Operational Control**: Hyperscalers' global infrastructure may conflict with localized governance needs. For example, the RBI's cloud initiative prioritizes compliance with Indian regulations, avoiding potential conflicts with hyperscalers' multinational policies.

Vendor Lock-In and Ecosystem Flexibility

- **Proprietary Ecosystems**: Azure tightly integrates with Microsoft technologies (e.g., Active Directory, .NET), while AWS offers proprietary tools through its marketplace. Both platforms, however, risk locking businesses into specific architectures, reducing overall flexibility and increasing dependency on a single vendor.
- **Hybrid and Multi-Cloud Strategies**: To mitigate this risk, companies are increasingly adopting hybrid and multi-cloud models. For example, Indian firms leverage a combination of global hyperscalers for their international reach and domestic providers like NxtGen for cost-

[17] https://cio.economictimes.indiatimes.com/news/strategy-and-management/indias-nxtgen-ecs-beats-amazon-aws-ibm-softlayer-microsoft-azure-on-price-performance-norm-study/52853432

[18] https://press.aboutamazon.com/in/2023/5/aws-to-invest-inr-1-05-600-crores-us-12-7-billion-into-cloud-infrastructure-in-india

effective, localized workloads. This strategy enhances redundancy, reduces vendor dependency, and strengthens negotiation leverage.

Performance and Latency

- **Edge Computing Demands:** While hyperscalers like AWS (84 Availability Zones) and Azure (54) offer expansive global reach, latency-sensitive applications—such as those in fintech and healthcare—often gain a performance edge from domestic providers with localized infrastructure. For instance, NxtGen's architecture, leveraging SSD/flash storage and horizontal scaling, has outperformed AWS and Azure in database and web server benchmarks.

Cyber Security Risks & Vendor Lock-in

- A majority of cloud-based software components rely on proprietary technologies. The lack of standardization and limited adoption of open standards restrict the ability to audit source code, increasing the risk of undetected cybersecurity threats or backdoor vulnerabilities.

Economic and Strategic National Initiatives

- **RBI's Sovereign Cloud Initiative**: The Reserve Bank of India is allocating ₹229.74 billion to establish a sovereign cloud infrastructure. This move aims to reduce dependency on foreign cloud service providers, safeguard national data, and ensure that economic value generated by digital infrastructure remains within the country. The initiative is strategically aligned with the rapidly growing Indian cloud market, projected to reach $24.2 billion by 2028.
- **Job Creation and Skill Development**: While global players like AWS are contributing to India's digital ecosystem—backed by a $12.7 billion investment that supports local employment and skilling—homegrown providers such as NxtGen offer a more localized approach. By focusing on managed services and forging partnerships with Indian technology firms, domestic providers are better positioned to support national employment and capacity-building objectives.

Migrating from AWS/Azure costs Indian firms 4x more than using domestic alternatives.

This claim stems from two key factors:

- **Operational Costs**: Migrating workloads from hyperscalers involves data transfer fees, re-architecting applications, and retraining staff. For example, Azure's complex licensing and AWS's egress charges inflate migration costs, especially for legacy systems.
- **Price-Performance Gap**: Studies show domestic providers like NxtGen ECS deliver 3x higher price-performance value than Azure/AWS due to lower VM costs and tailored infrastructure 6. When combined with migration expenses (e.g., downtime, duplication), the total cost for Indian firms can escalate to 4x compared to adopting local solutions upfront.

Key Takeaway

The shift away from hyperscalers marks a strategic recalibration—**balancing the innovation of global providers with the cost-efficiency, regulatory alignment, and control offered by domestic alternatives.** Initiatives such as the RBI's cloud platform and NxtGen's performance benchmarks underscore India's drive toward self-reliance, reflecting a broader global movement toward hybrid and sovereign cloud ecosystems.

Sovereign Cloud: Architecture for India's Digital Independence

Definition and Non-Negotiable Pillars

A sovereign cloud must **ensure strategic control** over Indian data:

- **Data Residency:** All data—both at rest and in transit—must be stored and processed exclusively within Indian borders.
- **Operational Control:** Only Indian entities (e.g., RBI, NPCI) must manage critical infrastructure, including master encryption keys, to ensure end-to-end oversight.
- **Strategic Control:** As detailed in the Annexure (GSR mandate), a Government Community Cloud (GCC) should be mandated for all government data to ensure it is governed under Indian jurisdiction.
- **Legal Immunity:** The sovereign cloud must comply with the **Digital Personal Data Protection Act (DPDPA), 2023**, while remaining immune to extraterritorial laws. Furthermore, contractual liabilities should be borne by Original Equipment Manufacturers (OEMs), not resellers.
- **Data Attainability:** Indian users—individuals or enterprises—must have *attainability* (not just access) of their data. For example, a user should be able to port their email communication data from one provider (e.g., Yahoo) to another (e.g., Gmail) with ease and control.

Strategic Benefits

- **National Security:** Safeguard critical sectors such as defence, healthcare, and citizen services by isolating sensitive workloads from foreign surveillance (e.g., **MeghRaj Government Cloud** implementation).
- **Economic Growth:** Enable creation of up to **2 million jobs by 2030** and support the scale-up of domestic cloud service providers like **Yotta, CtrlS, ESDS, and NxtGen**.
- **Regulatory Alignment:** Strengthen enforcement of data localization mandates issued by RBI and the provisions of the DPDPA, 2023.

Policy Framework: Urgent Interventions

Legislative Reforms

- **Sovereign Cloud Act**: Mandate adoption of GCC for critical sectors (defence, healthcare, finance).
    - Penalties: **5% of global turnover** for non-compliance.
- **Digital Data Classification Policy**: Categorize data into:
    - **Public** (weather data),
    - **Sensitive** (health records, UPI transactions),
    - **Critical** (defence, nuclear)

Data Classification and Sovereign Cloud Mandates, Open Standards

Data Classification Frameworks in India

India's ***Digital Personal Data Protection Act (DPDPA), 2023*** categorizes information broadly as "digital personal data," with sector-specific implications in areas such as healthcare, defence, and finance. However, it lacks explicit and enforceable classifications. A more structured data classification framework could include:

- **Sensitive Data:** Includes Aadhaar-linked health records, financial transactions, and biometric identifiers.
- **Critical Data:** Comprises defence intelligence, national security datasets, and key government administrative records.

Initiatives such as the *National Digital Health Mission (NDHM)* and *Meghraj (GI Cloud)* underscore the importance of localized storage for health and government data. However, these frameworks

currently fall short of mandating compliance from the private sector, limiting their overall effectiveness in securing critical national information.

Recommendations

- **Implement a Data Classification Framework**: Establish a comprehensive Data Classification Policy under the Digital Personal Data Protection Act (DPDPA), categorizing data into three tiers—**Public**, **Sensitive**, and **Critical**—based on its nature and potential impact on national interest and individual privacy.

- **Mandate Sovereign Hosting for High-Risk Data**: Require that all **Sensitive and Critical Data**—including but not limited to healthcare records, defence-related information, and citizen identification data—be stored exclusively on **Sovereign Cloud Infrastructure** (Government Community Cloud or equivalent). This infrastructure must:
    - Be located within India,
    - Use encryption keys held solely by Indian entities,
    - Operate with Indian IP addresses to ensure jurisdictional control and data sovereignty.

Case Study: Healthcare Data Sovereignty

- The **Digital Information Security in Healthcare Act (DISHA) 2018** defines "digital health data" as electronic health records requiring stringent protection
- However, hospitals like **AIIMS and private chains still rely on foreign VPCs (e.g., AWS GovCloud),** risking exposure under the U.S. CLOUD Act
- **Solution**: Mandate DISHA-compliant healthcare providers to migrate to local sovereign clouds, which isolates data and enforces military-grade encryption

Hybrid Governance for Foreign Partnerships

Conditions for Collaboration:

- **Joint Ventures:** Mandate profit-sharing and technology transfer mechanisms, drawing inspiration from models like the *Microsoft–Jio* partnership. This mirrors China's strategic approach to foreign cloud service providers, where local partnerships are required to ensure value retention and domestic capacity building.
- **Indian-Controlled Encryption:** All encryption keys to be held and managed exclusively by RBI-regulated digital custodians, ensuring sovereign oversight over data security and minimizing foreign surveillance risks.

Diplomatic Measures

- Negotiate **CLOUD Act exemptions** with the U.S., modelled on the EU-U.S. Data Privacy Framework.
- Similar to **DPI Stack**, create and promote the **Indian Open Cloud Stack** for Developing Countries.

Roadmap to 2030: From Crisis to Global Leadership

Building a Trusted Sovereign Cloud Ecosystem

Lessons from Telecom: The "Trusted Source" Model

India's telecom sector mandates procurement from **Trusted Sources** under the National Security Directive (2021). A similar framework can be adopted for cloud services:

- **Trusted Cloud Service Providers (TCSPs)**: Onboard Indian startups and firms (e.g., **Tata Communications**, **Utho**, **CtrlS**) meeting criteria like:
  - Full data residency within India.
  - Indian-held encryption keys and localized operational control
  - Compliance with TRAI's proposed **Industry Body for Cloud Service Providers**
- **Phased Implementation**:
  - **Phase 1 (2025–2027)**: TCSPs handle 50% of government and critical sector workloads.
  - **Phase 2 (2028–2030)**: Expand to private sector compliance, covering 70% of sensitive data

Similar to the provisions under CRO 2021, all electronics and IT products such as CCTVs are required to undergo physical security audits and be certified as per Indian Standards by an accredited Indian laboratory to safeguard national security. Given that CCTVs are a mandatory component of data centres, it is imperative that other critical hardware elements within data centres are also brought under the ambit of CRO or a similar regulatory framework. Such a mechanism should mandate physical audits irrespective of the type or mode of cloud services provided, whether Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS), including both Virtual Private Cloud (VPC) and Government Community Cloud (GCC) deployments.

Import Substitution and Scaling Indian Cloud Providers

- **Policy Incentives**:
  - **Tax Incentives:** Provide a 50% GST rebate for Indian sovereign cloud providers to promote local innovation and competitiveness.
  - **Preferential Procurement:** Mandate that government agencies allocate 30% of their cloud service budgets to Indian start-ups, ensuring a steady demand for domestic providers.
  - **Public-Private Partnership (PPP) Models:** Design scalable PPP projects to foster collaboration and enable long-term growth for Indian cloud providers.
- **Scaling for Global Markets**:
  - Indian cloud providers such as **Utho** (offering services at 60% lower cost than global hyperscalers) and **CtrlS** (operating Tier-4 data centers) can leverage the cost-effective, frugal innovation model pioneered in India. By targeting developing markets in **Africa** and **Southeast Asia**, they can offer scalable cloud solutions tailored to these regions' needs, driving growth and global market penetration.

Sovereign Cloud as a Catalyst for the Start-up Ecosystem

Opportunities for Service Providers

- **Affordable, Customized Solutions**: Domestic cloud service providers such as ESDS, Yotta, and NxtGen are offering tailored, sovereign cloud solutions for SMEs, which help reduce reliance on global hyperscalers.
- **Access to Funding**: Service providers can leverage the ₹10,000 crore Fund of Funds for Startups (FFS) to support research and development in emerging technologies like cloud-native AI, edge computing, and quantum security.

Benefits for Service Seekers

- **Cost Efficiency:** Utho offers transparent pricing, enabling Indian businesses to save approximately 60% compared to AWS and Azure.
- **Simplified Compliance:** By utilizing sovereign clouds, startups can seamlessly navigate cross-jurisdictional challenges, such as conflicts between the U.S. CLOUD Act and the Data Protection and Privacy Act (DPDPA) of India.

Phase 1 (2025–2027): Foundational Sovereignty

- **Policy Architecture:** Establish a robust framework for implementing regulatory and policy tools to realize Data Swaraj.
- **Infrastructure Development:** Build over 50 hyperscale data centers through the ₹300 billion National Cloud Mission.
- **Workforce Empowerment:** Train 500,000 professionals in sovereign cloud architecture under Skill India 2.0.
- **Migration Strategy:** Transition 50% of government workloads to Indian sovereign clouds (e.g., Meghraj, Tata GCC, ESDS GCC).

Phase 2 (2028–2030): Market Dominance

- **Domestic Control:** Enable Indian providers to capture 70% of critical sectors.
- **Global Expansion:** Export sovereign cloud solutions to Africa and ASEAN, targeting $50 billion in revenue.

Strategic Recommendations for India's Sovereign Cloud Ecosystem

Problem Statement

The rapid growth in computing demands, driven by AI, big data, and digital services, has led to an increasing reliance on foreign-owned cloud providers. These proprietary platforms not only foster vendor lock-in and impose high exit costs, but also pose considerable risks to national data sovereignty. **To mitigate these risks, leveraging the GSR (Government of India's Service Delivery) or the Electronic Service Delivery Rules, 2011** is essential for ensuring data sovereignty, particularly for sensitive data. (Further details on the GSR/Information Technology - Electronic Service Delivery Rules, 2011 and their scope for ensuring data sovereignty are provided in the annexure.)

The current cloud market landscape lacks a level playing field for Indian enterprises and start-ups, compelling them to adopt an OPEX-heavy model with **limited flexibility and bargaining power**. Furthermore, the absence of interoperable, open-source, and federated cloud solutions continues to **stifle innovation and cost efficiency.**

Compounding this challenge are **concerns around data monetization, the repurposing of Indian data to develop AI tools by foreign cloud providers, high data egress costs, and growing geopolitical risks—**all of which heighten India's digital vulnerability. In today's interconnected world, control over digital infrastructure is as vital as energy security, underpinning governance, commerce, and innovation. Without timely intervention, India risks ceding control over its **Digital Public Infrastructure (DPI), compromising its AI-driven future and national security**.

Comparing U.S. and Indian Government Cloud Strategies: A Divergence in Security, Compliance, and Data Sovereignty

- **Dedicated Government Clouds in the U.S.:** Leading U.S. cloud providers, such as AWS and Microsoft, offer specialized Government Community Clouds (e.g., AWS GovCloud, Microsoft GCC). These are purpose-built to comply with stringent federal standards for security, data sovereignty, and regulatory compliance. Operations are restricted to U.S. personnel, ensuring tight control over sensitive data.
- **National Security Priority:** These dedicated environments guarantee that critical government data remains within U.S. borders. With enhanced security protocols and compliance frameworks, they significantly mitigate the risk of unauthorized access or data breaches.
- **India's Preference for VPCs over GCCs:** In contrast, Indian government cloud procurement often favors Virtual Private Clouds (VPCs) for their flexibility and cost-efficiency. While offering data isolation, VPCs are typically preferred over establishing a dedicated Government Community Cloud or mandating GCCs for all public sector deployments.
- **Jurisdictional Risks and Data Control:** A key concern with VPCs—especially when hosted by foreign providers—is that critical elements such as encryption keys, administrative controls, and backup mechanisms may reside under foreign jurisdiction. This exposes government data to potential external interference or compromise.
- **Clarifying Liability:** Presently, the liability for data breaches or loss lies with resellers. However, this burden should logically rest with the Original Equipment Manufacturers (OEMs), who maintain control over the core infrastructure and are best positioned to ensure its security.

Hypothesis

An open, federated, and market-driven cloud ecosystem—rooted in open standards and interoperable frameworks—will empower India to:

- **Safeguard data sovereignty** by retaining critical infrastructure within Indian jurisdiction.
- **Boost market competition** by reducing reliance on dominant foreign cloud providers.
- **Enable cost-effective multi-cloud strategies** that optimize compute and storage expenditures.
- **Foster innovation** through an open ecosystem that supports AI, data analytics, and emerging technologies.
- **Align with Digital Public Infrastructure (DPI) principles** to build a scalable, resilient, and interoperable cloud architecture.
- **Curtail the outflow of foreign reserves** by decreasing net imports of cloud services.
- **Facilitate dynamic optimization** of costs and services across diverse cloud platforms for enterprises.

Strategic Steps to Address the Issue

1. Architect an Open, Interoperable Cloud Marketplace

1.1 Develop Standardized APIs for Decentralized Infrastructure

- **Establish Unified APIs**: Design and implement standardized APIs for compute, storage, and networking services to enable seamless integration across domestic and international cloud service providers (CSPs).
- **Implement a Federated Cloud Model**: Adopt a federated approach—similar to the Open Network for Digital Commerce (ONDC)—to allow government agencies and enterprises to dynamically choose CSPs based on their specific workload requirements.
- **Leverage Proven Interoperability Frameworks**: Draw insights from successful interoperability models such as the Microsoft-Oracle partnership, which facilitates integrated workloads across multi-cloud environments.
- **Promote Agile Multi-Cloud Strategies**: Encourage businesses to adopt flexible multi-cloud architectures that support dynamic workload migration based on real-time factors like pricing, availability, and performance.

- **Enable Automated Price Discovery and Cost Optimization**: Develop a real-time cost optimization engine that aggregates pricing across providers and enables automated workload shifting to the most cost-efficient environment.

Key Policy Interventions

- **Mandate Government Community Cloud (GCC)**: Require all government data to be hosted exclusively on the Government Community Cloud to ensure sovereign control and data security.
- **Standardized Model RFP for Cloud Services**: Develop and implement a model Request for Proposal (RFP) aligned with open standards to promote interoperability, transparency, and vendor neutrality.
- **Certification Requirement for Cloud Professionals**: Institute a mandatory certification for cloud professionals under an Indian Cloud Certification framework to build domestic expertise and ensure compliance with national standards.
- **Restrict Foreign Access to Cloud Databases**: Prohibit access to government cloud databases by foreign entities, individuals, or from foreign locations to uphold data sovereignty and prevent extraterritorial data breaches.
- **OEM Accountability in Contracts**: Ensure that contractual liabilities are directly borne by Original Equipment Manufacturers (OEMs), rather than delegated to resellers, to enhance accountability and service integrity.

1.2 Open-Source Ecosystem Development

- **Establish the Indian Open Cloud Software Foundation** to:
  - Oversee the governance and evolution of key open-source cloud components (e.g., Kubernetes, Apache Kafka).
  - Develop a robust talent pipeline through an "India Cloud Stack Certification" program.
- **Forge strategic partnerships** with global entities such as the Cloud Native Computing Foundation (CNCF) to ensure Indian cloud services align with international open-source standards.
- **Launch government-backed innovation grants** to incentivize start-ups to build, scale, and operate managed cloud services leveraging open-source stacks.
- **Allocate a minimum of 30% of government cloud procurement budgets** to Indian open-source SaaS providers, stimulating domestic innovation and competition.
- **Develop community-driven cloud standards**, modelled after the Linux Foundation's governance framework, to facilitate collaboration across industry, academia, and open-source contributors.
- **Introduce a nationally recognized "Indian Cloud Certification" framework**, akin to AWS, Azure, and GCP certifications. Make this certification mandatory for all Cloud Service Providers (CSPs) offering services to government entities.

2. Build a Distributed, Sovereign Data Infrastructure

2.1 Micro Data Center Parks and Inter-Networking

- Establish over **50 micro data center parks** across the country, modeled on the successful Software Technology Parks of India (STPI) framework, offering shared digital infrastructure.
- Enable **subsidized inter-networking between these parks** to lower cloud service costs and enhance data accessibility for startups, MSMEs, and public institutions.
- Designate **data centers as critical infrastructure under India's National Data Center Policy**, granting them access to low-interest financing and targeted tax incentives.
- Mandate **colocation of sensitive government and enterprise data within these parks**, with encryption keys exclusively managed by Indian entities under RBI oversight.

- Prioritize **Tier-2 and Tier-3 cities for park development** to deliver low-latency, high-bandwidth services, boosting digital capacity for healthcare, manufacturing, agriculture, and other key sectors.

2.2 Edge Computing and Latency Optimization

- Collaborate with telecom providers such as Jio, Airtel, and BSNL to **deploy edge compute nodes at 5G towers**, enabling real-time processing of AI and IoT workloads.
- Promote **decentralized AI processing to enhance traffic management, predictive maintenance, and autonomous systems** across sectors such as telecom, logistics, and smart cities.
- **Incentivize private sector investment** in regional data centers to support high-performance computing with reduced latency and improved data sovereignty.

3. Financial and Policy Instruments to Catalyze Growth

3.1 Funding Mechanisms

- **Sovereign Cloud Infrastructure Bonds:** Introduce 10-year tenure bonds with a 6% yield to finance the development and expansion of large-scale sovereign cloud infrastructure.
- **Computing Credits for Investors:** Provide partial returns to bond investors in the form of computing credits, enabling start-ups and SMEs to access sovereign cloud services at subsidized rates.
- **National GPU Procurement Pool:** Establish a centralized government-led procurement program for high-performance AI chips (e.g., NVIDIA H100), enabling bulk purchasing to reduce unit costs by 30–40%.
- **Targeted Financing for Digital Adoption:** Develop government-backed financing instruments—such as low-interest loans or credit guarantees—to support SMEs and start-ups in transitioning to and leveraging sovereign cloud infrastructure.

3.2 Incentivizing Private Participation

- Provide **subsidies for compliance** costs by covering 50% of certification fees (e.g., ISO 27001, GDPR) for Indian cloud service providers.
- Establish a **Fast-Track Compliance Cell** within MeitY to expedite regulatory approvals for Indian cloud startups.
- Mandate that by 2027, **at least 40% of government cloud spending be allocated to domestic cloud providers**.
- Transition the **Meghraj Government Cloud's workloads** from foreign cloud service providers to Indian sovereign cloud solutions, such as Tata Communications' GCC.

4. Global Collaboration and Standards Leadership

4.1 Federated Sovereignty Frameworks

- Collaborate with **Gaia-X**, the EU's decentralized cloud governance model, to promote global cloud interoperability while ensuring adherence to India's sovereignty requirements.
- Forge a strategic partnership with the **DOME Consortium**, Europe's leading decentralized cloud initiative, to drive international policy alignment in cloud governance.
- Advocate for the formation of a **BRICS Sovereign Cloud Alliance** to create a robust global alternative to U.S. and EU cloud dominance, leveraging Brazil'sagritech, India's AI, and China's advanced AI computing power.

4.2 Robust Security Strategy for Sovereign Cloud

A comprehensive security strategy is essential for establishing a **resilient and trustworthy sovereign cloud infrastructure**. From the outset, security should be integrated into every layer of the cloud architecture. The following key security components must be incorporated into the implementation roadmap:

- **Data Security & Sovereignty**: Prioritize encryption, effective key management, and ensure full regulatory compliance with frameworks such as RBI guidelines, CERT-In standards, and other relevant local and international regulations.
- **Zero Trust Architecture**: Implement a Zero Trust model with stringent identity and access controls, adhering to best practices in Identity and Access Management (IAM) to ensure that trust is never assumed, even within the network perimeter.
- **Threat Detection & Incident Response**: Deploy Security Information and Event Management (SIEM) systems, Endpoint Detection and Response (EDR) tools, and real-time monitoring capabilities to proactively detect, respond to, and mitigate potential security threats.
- **Secure DevOps (DevSecOps)**: Integrate security measures directly into the CI/CD pipeline, enabling automated security testing and mitigation of vulnerabilities throughout the software development lifecycle.
- **Disaster Recovery & Business Continuity**: Establish geo-redundant infrastructure, immutable backups, and automatic failover mechanisms to ensure continuous operations and rapid recovery in case of disruptions.

The security strategy and its roadmap (as outlined in the Annexure) must take these critical elements into account to build a resilient, compliant, and future-proof sovereign cloud ecosystem**.**

Threat Modelling Approach for Cloud Infrastructure

Threat modelling is crucial in proactively identifying vulnerabilities and mitigating risks in the cloud so that has to be incorporated while establishing a secure cloud. We can use STRIDE, MITRE ATT&CK, and DREAD methodologies for comprehensive risk assessment.

A. STRIDE Threat Model for Cloud Environments

Threat	Risk in Cloud	Mitigation Strategies
Spoofing	Identity-based attacks, unauthorized API access	MFA, IAM, RBAC, OAuth 2.0, SAML
Tampering	Data manipulation in transit/storage	End-to-end encryption, HMAC, integrity checks
Repudiation	Lack of logs for accountability	Immutable logs, SIEM, centralized audit logs
Information Disclosure	Data leaks due to misconfigurations	DLP, classification policies, and tokenization
Denial of Service (DoS)	DDoS on cloud services	Rate limiting, autoscaling, CDN protection
Elevation of Privileges	Unrestricted API access, misconfigured IAM	Just-in-Time access, Zero Trust, identity federation

B. MITRE ATT&CK for Cloud Threat Mapping

Tactic	Technique	Mitigation

Initial Access	Compromised credentials, phishing	MFA, passwordless authentication
Execution	Malicious scripts, serverless abuse	Restrict execution privileges, Lambda/Function security
Persistence	Cloud service account hijacking	IAM role audits, least-privilege policies
Privilege Escalation	API key exposure	API security gateways, key rotation
Defense Evasion	Log manipulation	Immutable logging, SIEM
Exfiltration	Data exfiltration via cloud storage	CASB, DLP, geofencing

Implementation Roadmap for Cloud Security

Phase	Key Actions	Security Controls
Phase 1: Architecture & Planning	Design cloud security controls	Zero Trust, micro-segmentation, IAM policies
Phase 2: Deployment & Hardening	Implement security baselines	CIS Benchmarks, infrastructure hardening, secure CI/CD
Phase 3: Monitoring & Response	Set up security monitoring	SIEM, XDR, UEBA, cloud logging
Phase 4: Compliance & Risk Management	Align with regulations	RBI, CERT-In, ISO 27001
Phase 5: Continuous Security Improvement	Conduct threat modeling	STRIDE, ATT&CK, DREAD, regular pen testing

The Samaaj, Sarkaar, Bazaar Approach to Open Cloud Computing

- **Samaaj (Community):** Form an **Indian Open Cloud Software Foundation** to standardize and govern **open-source cloud infrastructure**.
- **Sarkaar (Government):** Create **policy incentives for domestic data centers**, including **high-bandwidth interconnects** and **low-cost access to AI/ML infrastructure**.
- **Bazaar (Market):** Encourage **private companies to build and operate sovereign cloud services**, similar to **how RedHat powers Linux-driven enterprise solutions**.

Conclusion: A Digital Quit India Movement

India's reliance on foreign cloud services represents a modern form of colonization, undermining its digital sovereignty. To counter this, India must prioritize developing sovereign cloud infrastructure, following the same principles that propelled its success in space (ISRO) and nuclear technology, to position itself as a global cloud powerhouse. The time for **Data Swaraj (self-rule)** is now—before geopolitical tensions erode the nation's autonomy.

To secure its digital economy, critical data, and national security, India must **urgently invest in domestic cloud infrastructure**. **By fostering local cloud providers, building open and federated cloud networks, and enforcing robust data localization policies,** India can reduce dependence on foreign cloud giants and cultivate a competitive, resilient, and sovereign digital ecosystem.

DATA SWARAJ for SECURE DIGITAL INDIA

This is a call to action for policymakers, industry leaders, and citizens alike to protect **the nation's digital future and embrace Data Swaraj**. India must ensure global connectivity while maintaining full strategic control over its data. Now is the moment for India to take a leadership role in shaping Global Data Governance Architecture, managing data flows across borders, and defining the governance framework for state, non-state actors, and individuals alike.

Annexure A: Cloud Orchestration Layer

Total Control & Customization

Why it matters:

- **Tailored to Business Needs:** Pre-packaged orchestration solutions often come with fixed workflows that may not align with organisations unique infrastructure requirement (e.g., manufacturing-specific ERP, Banking related CBS needs). Building your own orchestration layer allows **custom automation** tailored to Indian organisations operations.
- **Granular Policy Control:** We can implement **custom security**, **resource quotas**, and **data handling** rules to align with internal governance and **regulatory compliance**.

"Our orchestration layer allows us to align cloud automation precisely with our infrastructure workflows, ensuring that business-specific processes are handled securely and efficiently—something off-the-shelf solutions cannot offer."

Enhanced Security & Data Sovereignty

Why it matters:

- **Data Control:** Public cloud orchestration solutions may store or process metadata outside your jurisdiction. **Building your own** keeps critical data flows in-house, ensuring **data sovereignty** and compliance with regulations (e.g., **DPDP, MeitY, RBI, ISO, etc**).
- **Custom Security Checks:** Implement **custom security postures** like vulnerability scanning, privileged access control, and specific encryption protocols.

"By developing our orchestration layer, we maintain full ownership of sensitive data, ensure compliance with industry regulations, and minimize the risk of third-party exposure."

No Vendor Lock-Ins

Why it matters:

- **Avoid Vendor Lock-in:** Custom orchestration supports **multi-cloud** and **on-premise** workloads seamlessly. This prevents dependency on a single provider like AWS, Azure, or SAP RISE.
- **Cloud Agnosticism:** Facilitate workload movement between **private data centers** and **public clouds** (e.g., manufacturing ERP on private infrastructure, analytics on public cloud).

"Our orchestration layer provides the flexibility to manage workloads across multiple clouds and on-premise environments, protecting us from vendor lock-in and optimizing cloud costs."

Cost Efficiency & Resource Optimization

Why it matters:

- **Optimized Resource Usage:** Custom orchestration enables **dynamic scaling**, cost-aware scheduling, and **intelligent workload balancing**—avoiding overprovisioning and reducing **cloud waste**.
- **Avoid Third-Party Costs:** Third-party orchestration tools come with **licensing** and **usage fees**. Building your own avoids long-term vendor costs and limits expenses to internal development.

"By building our layer, we reduce recurring licensing costs while optimizing resource allocation, saving both in operational overhead and infrastructure expenses."

Workflow Automation & Operational Efficiency

Why it matters:

- **Custom Automation Pipelines:** Create task-specific automation workflows (e.g., automated disaster recovery for critical workloads, ERP backup snapshots).
- **Faster Innovation:** Automate environment provisioning for **development, testing, and production**—accelerating software delivery and operational agility.

"A custom orchestration layer accelerates deployment, enables environment-specific automation, and enhances overall operational efficiency—giving us a competitive edge in manufacturing innovation."

Improved Monitoring & Reporting

Why it matters:

- **Custom Metrics Collection:** Collect and monitor **business-specific KPIs** (e.g., resource consumption per ERP module, performance of manufacturing workloads).
- **Incident Response:** Implement **real-time alerting** and **custom dashboards** tailored to your infrastructure for faster troubleshooting.

"A homegrown orchestration layer allows us to track tailored operational metrics and respond rapidly to infrastructure issues, critical for minimizing downtime in manufacturing."

Long-Term Strategic Independence

Why it matters:

- **Future-Proofing:** As technology evolves, you can **extend** the orchestration layer without waiting for external vendor updates.
- **Innovation Control:** Freedom to integrate with **new tools** (AI, IoT, Industry 4.0) without restrictions imposed by third-party orchestration.

"Owning our orchestration layer future-proofs our IT strategy, giving us the freedom to integrate with emerging technologies and control the pace of innovation."

Key Considerations

1. **Risk Mitigation: Data security** and **compliance** are strengthened by reducing third-party dependencies.
2. **Cost-Benefit Analysis:** Compare long-term savings vs. the initial development investment.
3. **Scalability & Agility:** custom orchestration will **scale** with business growth and **adapt** to future tech trends.
4. **Proof of Concept (PoC):** Suggest starting with a **PoC**.

Final Recommendation Statement

Building our orchestration layer gives us full control over infrastructure, optimizes costs, and aligns with our long-term strategy to remain independent of vendor constraints. It not only protects our intellectual property but also accelerates innovation in critical manufacturing workflows.

Annexure B: Standardisation Protocols

Government data is a strategic national asset that requires stringent security, accessibility and compliance measures. The collection, processing and storage of this data involve substantial efforts and its integrity and availability are crucial for governance and citizen services.

As government departments increasingly adopt cloud computing for scalability and efficiency, there is a pressing need to establish a robust framework to ensure that government data remains accessible, secure and retrievable, especially when using cloud services provided by non-Indian Cloud Service Providers (CSPs).

Challenges faced due to non-standardization

1. **Complexity**: The lack standards themselves increase complexity in managing the Cloud and require a deep understanding of technical and regulatory requirements.
2. **Need of Cloud OEM specific Certifications**- Having multiple OEM certifications due to vendor specific non-standard nomenclature and services becomes exhaustive and counter-productive.
3. **Resource Constraints**: Implementing these non-standard services often requires significant resources, including time, money, and skilled personnel.
4. **Compliance**: Ensuring compliance with multiple standards and regulations can be difficult, especially for organizations operating in multiple jurisdictions.
5. **Vendor Lock-In**: Organizations may face challenges when trying to switch cloud service providers due to proprietary technologies and data migration complexities.
6. **Security Risks**: Maintaining robust security measures in a dynamic cloud environment is a constant challenge.
7. **Data Privacy**: Adhering to data privacy regulations, such as GDPR, requires meticulous management of where and how data is stored and processed.
8. **Integration Issues**: Integrating existing IT infrastructure and applications with cloud services can be complex and may require extensive planning and redesign.
9. **Performance Issues**: Ensuring consistent performance and avoiding service disruptions can be challenging.
10. **Cost Management**: Managing costs effectively while adhering to standards can be difficult, especially with complex pricing models.
11. **Lack of Expertise**: Organizations may lack the necessary expertise to fully understand and implement the services.

Standardization & Audit Mechanisms

To uphold transparency and compliance, government agencies should establish well-defined auditing mechanisms:

- **Standardized Backup & Sharing Protocols:** Data sharing and migration should be based on open standards to enable seamless interoperability and prevent vendor lock-in.
- **Third-Party Audits:** CSPs providing cloud services to government entities must be subject to independent audits conducted by the Standardization Testing and Quality Certification (STQC) agency or another designated government body.
- **Use of Indigenous Technology:** Cloud service providers should be evaluated on their integration and utilization of indigenous cloud technologies, promoting the use of secure, locally developed solutions.

Standardization of cloud services from various Cloud Service Providers (CSPs) for public procurement has further benefits:

- **Interoperability**: Standardization ensures that different cloud services can work together seamlessly, allowing for easier integration and data exchange between systems.
- **Security**: With standardized protocols, it's easier to implement consistent security measures across different cloud services, reducing the risk of vulnerabilities.
- **Cost Efficiency**: Standardization can lead to economies of scale, reducing costs for both the government and CSPs2.
- **Compliance**: It simplifies compliance with regulatory requirements, as standardized services are more likely to meet established standards and guidelines.
- **Vendor Neutrality**: It promotes fair competition among CSPs, ensuring that procurement decisions are based on merit rather than vendor-specific advantages

Need for Secure Government Cloud Data & Backup Management

Government departments often leverage cloud solutions from global CSPs due to their advanced infrastructure and service offerings. However, relying solely on non-Indian CSPs raises concerns regarding data sovereignty, security, and long-term accessibility. To mitigate risks, government agencies must implement measures to ensure:

1. **Data Sovereignty:** Government data should remain within Indian jurisdiction to comply with national data security policies and ensure protection against unauthorized foreign access.
2. **Data Backup on Indian Cloud:** A structured policy should mandate that all government data stored on non-Indian CSPs is periodically backed up on an Indian cloud infrastructure to ensure retrieval and restoration whenever required.
3. **Uninterrupted Accessibility:** Data should always be processable and accessible on Indian cloud infrastructure, ensuring continuity of government operations even in cases of contract expiration or sudden termination.
4. **Legal and contractual guardrails:** Responsibility for data breaches currently falls on resellers, even though OEMs, who build and maintain the infrastructure, should be held accountable.

Exit Management Framework

One of the key aspects of cloud adoption is the formulation of a robust exit management strategy that safeguards government data even when cloud service agreements conclude. The framework should include:

- **Strong Contractual Provisions:** Every cloud service contract should explicitly define the government's right to obtain the latest backup of its data at any given time, including upon contract expiration or abrupt termination.
- **Ensuring Seamless Data Handover:** Government agencies must receive structured data backups in standardized, open formats that facilitate smooth migration to an alternative cloud infrastructure.
- **Compliance & Monitoring:** CSPs must comply with stringent exit protocols, ensuring data retrieval without loss or corruption.

Public IP Address Allocation & Compliance

To further secure government cloud operations, CSPs must ensure that all public IP addresses used in cloud services for government entities are sourced from regional internet registries (RIRs) relevant to India, such as the Asia-Pacific Network Information Centre (APNIC). The use of IPs allocated from non-regional registries such as RIPE (Europe) or ARPA (U.S.) introduces risks related to jurisdictional control, potential foreign monitoring, and compliance challenges.

Risks of Using Non-Regional Public IPs:

- **Jurisdictional Issues:** Public IPs assigned from foreign RIRs may be subject to foreign legal and regulatory oversight, potentially compromising data security.
- **Risk of Data Interception:** Traffic routed through international registries increases exposure to external monitoring and surveillance risks.
- **Regulatory Compliance Challenges:** Using non-APNIC IPs may violate national data policies, leading to governance issues and potential service disruptions.

Benefits of Ensuring APNIC IP Usage:

- **Enhanced Data Sovereignty:** Public IPs registered with APNIC ensure government data traffic remains within legally protected regional boundaries.
- **Better Regulatory Control:** Indian authorities retain oversight over traffic originating and terminating within Indian jurisdictions.
- **Improved Security & Performance:** Localized routing reduces latency and security threats associated with foreign interception.

Conclusion

The strategic importance of government data necessitates a comprehensive cloud management framework that ensures sovereignty, security, and seamless transition mechanisms. By implementing policies mandating data backups on Indian cloud infrastructure, enforcing well-defined exit management protocols, standardizing audit procedures, and ensuring that public IP addresses comply with APNIC allocation, the government can mitigate risks associated with foreign CSP reliance while ensuring uninterrupted governance and data security. These measures will establish a resilient and self-reliant cloud ecosystem, reinforcing India's commitment to data security and digital sovereignty.

Annexure C: Recommendations for Enhancing Cloud Service Interoperability and Data Portability according to ISO/IEC 19941

To facilitate seamless migration between cloud service providers (CSPs), it is essential to address **digital identity management** and **data portability** challenges. When transitioning to a new cloud service, either digital identities must be recreated with the same values and format in the target system, or all references to these identities across data, metadata, software, and applications must be updated to align with the new system. Establishing **reliable identity mapping frameworks** across all domains ensures accurate correspondence and smoother transitions. Standardizing the **packaging and encoding formats** for infrastructure data artifacts is also crucial, as it reduces the complexity and cost of data export, mapping, and import during migration. However, CSPs may not always offer identical services or data models, making interoperability more challenging. To mitigate this, there is a pressing need to develop **uniform data interchange standards** to minimize switching costs and ensure data artifacts are consistently supported across cloud platforms.

Improving **API interoperability** is another critical area of focus. Cloud services operate through three key interfaces—**service, administration, and business interfaces**—yet industry-wide standards for these interfaces remain limited, making cross-platform compatibility difficult. This is particularly true for **application capabilities** where there is little agreement on the behavioral and semantic aspects of APIs. It is often possible to manually connect non-interoperable services, but such solutions are inefficient and resource-intensive. Establishing **common interoperability frameworks** and identifying **interoperability points** across services can streamline integration efforts. Policy interoperability is equally important, especially in terms of **data residency and jurisdictional regulations**. This includes not only where data is stored and processed but also the nationality and location of personnel accessing the systems. For example, certain regulatory requirements—such as allowing government inspectors physical access to servers—may be incompatible with public cloud environments where infrastructure

is virtualized and shared. Clear, standardized guidelines for regulatory compliance across cloud environments are essential to align with jurisdictional policies while maintaining operational efficiency.

When a CSC wants to switch to a different cloud service, the CSC needs to be able to take their data artefacts from the original cloud service and move them to the target cloud service. The switching cost will include exporting, mapping, and importing the data into the target application capabilities type cloud service, and that cost is a function of how well the data models and interchange formats of the two-cloud services line up. Standardizing these interchange formats greatly reduces switching costs. However, CSPs might not support the same type of cloud service with identical data artefacts.

Table 7 — Example considerations for data policy portability

Topics	Considerations
Data use rights	a) Verify that the proposed data port complies with any license restrictions that may be in place, such as: 1) audio/visual media licensed from a commercial content provider; 2) mapping or other commercial data licensed from a data provider.
Service use rights	a) Verify that the target cloud service to be used meets legal requirements for handling the data being ported, such as: 1) Certified for handling health data; 2) Meets required privacy standards or regulations, e.g. ISO/IEC 27001 with ISO/IEC 27018; 3) Meets government procurement rules.
Data location	a) Verify that the target cloud service stores data in appropriate jurisdiction(s) to meet organization/customer/regulatory requirements and obligations.
Processing location	a) Verify that the target service processes the data in appropriate jurisdiction(s) to meet company/customer requirements and obligations.
Third party processing	a) Verify that any third-party processing is well-understood and that the third party also meets the requirements and obligations, and will continue to do so.
Jurisdiction	a) Verify whether the porting of data changes the applicable jurisdiction(s) from that of the source system and investigate any legal consequences of any such change.
Contract	a) Take appropriate legal advice. b) Keep and maintain appropriate audit trails. c) Understand any contractual limitations that exist in relation to the data being ported.
Security and privacy	a) Verify that the target environment provides the necessary security and privacy controls to meet the policies of the CSC with respect to the data being ported.

- For example, if some vendor acceptance criteria require allowing government inspectors to have physical access to the vendor's servers, it probably will not work in a public cloud environment, where such servers are virtual and likely move around, sharing hardware with other customers
- Other Points
  - Encryption key handling can include key storage services and the use of hardware encryption modules.
  - For cloud services involving a very large volume of customer data, transfer might be offered through the transfer of data on physical media
  - The application code for the cloud service is installed and operated by the CSP; the code does not come from the CSC. For this reason, there is no porting of an application to or from a cloud service of this type.

Snapshot of the GSR/ Information Technology (Electronic Service Delivery) Rules, 2011

- **Facilitation of Public Service Delivery**: The Rules aim to modernize and streamline the delivery of public services through electronic means. These include services like filing applications, issuing licenses and certificates, and facilitating electronic payments. This system ensures faster processing, reduced physical paperwork, and improved transparency in government service delivery.
- **Framework for Secure Digital Transactions**: By mandating encryption and electronic signatures, the Rules ensure that digital transactions and records are secure, authentic, and tamper-proof. This enhances trust among users of electronic service delivery systems.

- **Establishment of Accountability Mechanisms**: Service providers and authorized agents are required to maintain accurate records of transactions and follow government-specified standards for service delivery. Provisions for audits and inspections ensure compliance and accountability in electronic service delivery systems.
- **Creation and Maintenance of Digital Repositories**: The Rules mandate the creation and archival of repositories for electronically signed records, ensuring secure and organized storage of all licenses, permits, certificates, and approvals issued electronically.
- **Promotion of Digital Accessibility**: The use of electronically enabled kiosks and similar mechanisms widens access to digital services, enabling inclusion for citizens who may not have personal access to digital infrastructure.
- **Regulation of Service Charges and Financial Management**: The Rules empower the government to specify service charges and ensure that transactions comply with financial codes. It mandates transparent accounting and the issuance of receipts detailing service charges.
- **Audit and Oversight of Systems**: The Rules emphasize the periodic audit of service providers' systems, focusing on security, confidentiality, and performance. This ensures adherence to best practices and prevents misuse of personal data.
- **Adaptability to Change**: The government can notify new services for electronic delivery and update the list of authorized agents and signing authorities, allowing flexibility in adapting to emerging needs and technologies.

Key Insights and Notable Provisions

- **Provision for Transparent Pricing**: Service providers must display and itemize service charges on receipts, ensuring transparency for users.
- **Secure Management of Cryptographic Keys**: The Rules emphasize stringent management of cryptographic keys and electronic certificates to prevent unauthorized access.
- **Audit Trails for Repository Changes**: Changes to digital repositories must include time-stamped records of modifications, ensuring accountability for all updates.
- **Special Stationery for Security**: Security-enhanced stationery for certificates, licenses, and receipts adds an additional layer of authenticity.
- **Penalty for Unauthorized Data Disclosure**: Service providers can face penalties under Section 45 of the IT Act for disclosing personal data without authorization.
- **Dynamic Notification System**: The government can update services and signing authorities through regular notifications, enabling adaptability.

Strategic Insights: Scopes of Information Technology (Electronic Service Delivery) Rules, 2011 to Address Data Sovereignty and Recommendations for Enhancement

Introduction

India's reliance on international cloud service providers like AWS, Azure, and Google, coupled with their compliance with foreign jurisdictions and encryption key control, challenges the notion of true data sovereignty. While the **Electronic Service Delivery Rules, 2011** provide a foundational framework for localizing sensitive data and ensuring government control, certain provisions can be strengthened to address gaps and enhance compliance with India's data sovereignty goals.

Current Provisions Addressing Data Sovereignty

1. Local Data Repositories (Rule 5)

- **Provision**: The Rules mandate the creation, archival, and maintenance of repositories for electronically signed records, ensuring that sensitive government-issued data remains stored within Indian jurisdiction.

- **Impact**: Ensures physical data localization and reduces dependency on foreign-owned cloud infrastructure for critical government data.
- **Enhancement Opportunity**:
  - Mandate that repositories must be hosted on servers owned and operated by Indian entities or under Indian legal control.
  - Require periodic compliance certifications from cloud providers hosting repositories.

2. Encryption Standards and Key Management (Rule 3(3))

- **Provision**: The government can determine encryption methods and the management of sensitive electronic records, ensuring confidentiality during electronic service delivery.
- **Impact**: Enables the government to set national encryption standards, reducing reliance on foreign encryption protocols and key management systems.
- **Enhancement Opportunity**:
  - Make it mandatory for cloud service providers hosting sensitive data to adhere to encryption standards specified by the Indian government.
  - Require that encryption keys for sensitive data remain accessible only to authorized Indian entities.

3. Service Provider Accountability (Rule 7)

- **Provision**: Service providers must maintain accurate accounts of transactions and comply with government audits to ensure adherence to the rules.
- **Impact**: Establishes a compliance mechanism, allowing the government to oversee how service providers handle sensitive data.
- **Enhancement Opportunity**:
  - Require service providers to disclose their data processing and storage locations, as well as the jurisdictions they operate in.
  - Mandate that sensitive data hosted by cloud providers be stored only in India, with all data transfers subject to government approval.

4. Audits for Security and Confidentiality (Rule 8)

- **Provision**: Regular audits assess the security, confidentiality, and functionality of service providers' systems, ensuring compliance with Indian standards.
- **Impact**: Provides a mechanism to identify and rectify compliance issues and ensure data sovereignty objectives are met.
- **Enhancement Opportunity**:
  - Mandate third-party audits specifically focused on compliance with data sovereignty norms, including encryption, localization, and data transfer policies.
  - Impose penalties for cloud providers that fail to comply with localization or sovereignty-related audit findings.

5. Notification of Services and Signing Authorities (Rule 4)

- **Provision**: The government can notify services to be delivered electronically and designate signing authorities for different classes of certificates and jurisdictions.
- **Impact**: Centralizes control over electronic service delivery mechanisms, ensuring that sensitive operations remain under Indian jurisdiction.
- **Enhancement Opportunity**:
  - Expand the scope to explicitly include cloud service providers, requiring them to align with notified services and follow data sovereignty guidelines.
  - Specify requirements for metadata storage and jurisdiction to prevent unauthorized analysis by foreign entities.

6. Security Procedures for Repositories (Rule 5(4))

- **Provision**: The Rules mandate security protocols for managing repositories, including cryptographic key storage, access restrictions, and audit trails.
- **Impact**: Ensures sensitive data is stored securely and access is traceable, reducing the risk of unauthorized access or manipulation.
- **Enhancement Opportunity**:
  - Require that all repositories adopt advanced encryption methods aligned with India's standards, with key management restricted to Indian authorities.
  - Mandate multi-layered security protocols, including real-time threat monitoring and incident reporting, for all cloud providers handling government data.

Strategic Enhancements to Align Cloud Providers with Data Sovereignty

1. Mandatory Compliance with Indian Encryption Standards

- Cloud service providers must adopt Indian-approved encryption protocols and ensure that encryption keys remain under Indian jurisdiction. This prevents data from being decrypted or accessed under foreign laws, such as the U.S. CLOUD Act.

2. Data Processing and Storage Transparency

- Providers must declare all locations where data is processed or stored and ensure compliance with Indian data localization laws. Periodic compliance audits should verify adherence to these declarations.

3. Sovereign Metadata Management

- Extend localization requirements to metadata, as its analysis can reveal critical patterns and insights. Mandate that metadata associated with government services be stored and analyzed only within India.

4. Incentivizing Indigenous Cloud Infrastructure

- Encourage the development of domestic cloud service providers through government-backed initiatives and partnerships. Offer incentives for Indian companies to build sovereign cloud solutions that comply fully with Indian laws.

5. Strengthened Audit and Compliance Mechanisms

- Mandate third-party audits of cloud providers' systems, focusing on their compliance with data sovereignty norms, encryption standards, and localization requirements. Non-compliance should result in penalties and potential disqualification from handling sensitive data.

6. Explicit Ban on Foreign Data Transfers

- Prohibit the transfer of sensitive government data or metadata to foreign jurisdictions unless explicitly approved by the government. Implement strong enforcement mechanisms to detect and prevent unauthorized transfers.

Conclusion

The **Electronic Service Delivery Rules, 2011**, provide a foundational framework for addressing data sovereignty, particularly for sensitive and government data. However, to fully realize India's sovereignty objectives, enhancements are needed to address gaps in encryption, localization, and compliance mechanisms. By mandating cloud service providers to adhere to stricter guidelines, including Indian encryption standards, metadata localization, and robust audit requirements, the government can strengthen its control over sensitive data, reduce reliance on foreign entities, and ensure the secure and sovereign management of India's digital assets.

Annexure D: The security strategy and roadmap for Cloud

Data Security & Encryption Standards

To protect sensitive data, our cloud infrastructure must incorporate strong encryption mechanisms across all data states:

- **End-to-End Encryption:** Encrypt all data in transit, at rest, and in use using industry standards (e.g., AES-256). Implement Key Management Services (KMS) to centralize encryption management.
- **Encryption Key Ownership**: Unlike hyperscalers, where key management is often tied to the service provider, we must retain full control over encryption keys (Customer- Supplied Encryption Keys - CSEK) to meet compliance and sovereignty requirements.
- **Confidential Computing:** Implement secure enclaves to process sensitive workloads in an isolated environment, ensuring data remains protected even from privileged administrators.

Identity and Access Management (IAM) Best Practices

A **Zero Trust** model must be enforced to **restrict access and minimize attack surfaces**:

- **Zero Trust Approach:** Every request, regardless of origin, must undergo authentication and authorization. Implement **fine-grained access controls** for all cloud resources.
- **Principle of Least Privilege (PoLP):** Adopt **Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC)** to ensure users and services only have the minimum required permissions.
- **Multi-Factor Authentication (MFA):** Enforce **MFA for all admin and privileged accounts**, reducing the risk of credential-based attacks.

Supply Chain Security & Third-Party Risks

Given that cloud environments often rely on **third-party software and integrations**, we must **secure the supply chain**:

- **Third-Party Cloud Dependencies:** Reduce reliance on external cloud dependencies by **hosting critical APIs, SaaS, and PaaS services within our controlled environment**.
- **Software Supply Chain Attacks:** Implement a **Software Bill of Materials (SBOM)** to track dependencies and detect security vulnerabilities in third-party components.

- **Regular Compliance Audits:** Conduct **periodic security audits** to ensure adherence to **ISO 27001, SOC 2, RBI, and CERT-In** guidelines.

Regulatory Compliance & Incident Response Readiness

Our cloud infrastructure must align with **local regulations** and have an **effective incident response strategy:**

- **Data Residency Compliance:** Ensure that **logs and sensitive workloads remain within India** to comply with RBI, SEBI, and CERT-In regulations.
- **Cloud-Specific Incident Response:** Develop **cloud-native incident response playbooks** to address breaches, **ransomware**, and **insider threats**.
- **Continuous Monitoring & SIEM:** Deploy **Security Information and Event Management (SIEM) solutions** (e.g., Q-Radar, SentinelOne, CrowdStrike EDR) to detect **anomalous activities in real-time**.

Secure DevOps & API Protection

Security must be **integrated into the development pipeline** to prevent vulnerabilities from reaching production:

- **Shift Left Security:** Embed security into **CI/CD pipelines** by leveraging **SAST (Static Analysis), DAST (Dynamic Analysis), and IaC (Infrastructure as Code) scanning** tools like Checkov or Prisma Cloud.
- **API Security:** Implement **Web Application Firewalls (WAF)** and **API Gateways** to protect against threats such as **API abuse, broken authentication, and injection attacks**.
- **Runtime Protection:** Deploy **Cloud Workload Protection Platforms (CWPP)** to monitor containers and microservices in real time.

Shadow IT & Insider Threats

Unmonitored cloud usage can introduce **security gaps and compliance risks**:

- **Unauthorized Cloud Usage:** Prevent **unsanctioned deployments** by restricting access to **approved cloud services** and enforcing strict **network segmentation**.
- **Data Loss Prevention (DLP):** Use **Cloud Access Security Brokers (CASB)** (e.g., Netskope, Microsoft Defender for Cloud Apps) to **monitor and control sensitive data movements**.
- **Behavior Analytics:** Implement **User and Entity Behavior Analytics (UEBA)** to **identify insider threats and compromised accounts**.
- There should be a policy on access to data stored on Indian Data Centres/Cloud outside the geographical boundaries should be of India, either through VPN or any other means to ensure that strategic control and data sovereignty are not compromised.

Business Continuity & Disaster Recovery (BC/DR)

A **resilient cloud infrastructure** must ensure **high availability and rapid recovery** from disruptions:

- **Geo-Redundancy:** Distribute workloads across **multiple cloud regions or data centers** to prevent a single point of failure.
- **Immutable Backups:** Maintain **air-gapped and immutable backups** to protect against **ransomware and data corruption**.
- **Failover Testing:** Conduct **regular disaster recovery drills** to validate **automated failover mechanisms and data restoration procedures.**

*****

B-DIA
Bharath Digital Infrastructure Association

KNOWLEDGE PARTNERS

rishihood university

I·D·F

CONSOCIA ADVISORY

ABOUT B-DIA

Bharath Digital Infrastructure Association is an outcome of GoI vision of making India Digitally Sovereign and suggestions form stakeholders, especially govt, to create unified voice of Indian Tech Industry with Nation First at it's core evolution of Indian Tech Industry from being traders to OEMs. The Indian tech industry has made significant strides in technology and services, positioning itself at par with global tech giants. However, to fully realize its potential and address the critical challenges of digital sovereignty and strategic control, a paradigm shift is essential. Recognizing this need, B-DIA was formed with a startup-like mindset, fostering an out-of-the-box approach, innovation-driven advocacy, and a commitment to integrity and values. Its foundation is firmly aligned with the Government's approach towards digital data protection and self-reliance, ensuring India's leadership by promoting Indian companies in the global digital landscape.

PHONE
+91 9818882078

ADDRESS
Westend Marg (Ground Floor, Near Saket Metro), Lane No. 1, Saidulajab, Saiyad Ul Ajaib, New Delhi, Delhi 110030.

EMAIL
contactus@bdia.in