ON THIS PAGE

HISTORY OF DATA: FROM CLAY TABLETS TO ZETTABYTES

information was so sacrosanct that only strong, loyal, and wise were entrusted to serve as secret keepers. This was to ensure the security, integrity and governance of the information.

Fast forward to the 21st century, while the basic principles of data generation and management remain the same, the quantum, scale, and speed with which this information is generated and utilized have transformed its management. Every interaction that happens between individuals generates data points. From Aadhar in India, social security number in the USA, to e-health records in European countries, trillions of data points are generated that are personal, permanent, and must be kept confidential, putting a massive load of responsibility on the governments to manage them well.

- India processes more than three billion Aadhaar authentications per month, showing the scale and sensitivity of its digital infrastructure.
- Approximately 402.74 million terabytes of data are created each day, and 181 zettabytes of data will be generated in 2025.
- Videos account for over half of internet data traffic.
- The US has over 2,700 data centers.
- In 2023, India had 888 million broadband users, half a million common service centers and over 4,38,000 PMGDisha training centers.

Today, we are fighting information wars every second. With the advancement of artificial intelligence (AI), these battles have become more challenging with unimaginable consequences if the information is not protected meticulously.

Today, governments have emerged as the primary custodians of sensitive data. As digitalization grows across sectors, vast volumes of citizens' data – measured in data points – are continuously generated, heightening the risk of threat exposure if not managed and protected well.

into an abyss.

The world has witnessed a surge in high impact cyberattacks with geopolitical undertones. In 2020, the SolarWinds breach affected U.S. federal agencies. In 2023, healthcare systems in Australia were crippled due to ransomware attacks. India, too, faced multiple attacks on power grids and defense-related assets.

In light of such developments, all eyes are on governments to protect data from internal inefficiencies and external adversaries. The geopolitical implications have made the situation more complex, and the impact of any breach is profound, jeopardizing national trust, political stability, and digital sovereignty.

The evolving reality demands an urgent reassessment – how and where should governments store and safeguard the invaluable data? The challenge lies in ensuring integrity, confidentiality, and accessibility in the face of rising threats.

CHALLENGES: DATA MANAGEMENT IS NOWHERE CLOSE TO BEING MANAGEABLE

and sometimes insecure data management practices.

If data systems are not designed and maintained with precision, they expose nations to high-risk situations, including data breaches and compromise of sensitive information.

While public cloud platforms offer immense scalability, innovation, and price competitiveness, they also introduce significant concerns about jurisdictional and regulatory complexities. For instance, the US Cloud Act 2018 empowers US government to access the data stored by American cloud service providers, regardless of where it is stored globally.

Governments must carefully assess if cloud providers meet relevant regulatory requirements such as Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR). This has led to concerns about potential conflicts and genuine need for the governments to look for alternatives for managing their digital infrastructure, sensitive data, and reduce reliance on US-based cloud service providers.

As a result, governments are increasingly grappling with a difficult trade-off: on premises infrastructure may ensure greater control and data sovereignty, while public cloud environments promise scalability, cost competitiveness, and ease of management. The duality makes it challenging for stakeholders to make an informed decision on the same and has triggered a major strategic question: How can governments unlock the benefits of both worlds without compromising on either control or capability?

Enter the concept of a sovereign cloud – a hybrid framework designed to address the challenges of data sovereignty and security. It ensures that data remains within the country's borders, under the control of the government. The accountability and

The core principles on which sovereign cloud works are:

1. Data residency
   As per this principle, all the data whether primary, backup, or archival, is stored and processed strictly within the national borders. For example, in case of India, governments must explore options that leverage indigenous infrastructure of owned data centers in major cities like Mumbai, Hyderabad, Delhi, Pune, and so on.

2. Data sovereignty
   Data is subject exclusively to the laws and governance of the host nation, such as the Digital Personal Data Protection Act, 2023, ensuring immunity from foreign legal jurisdictions and extraterritorial subpoenas (e.g. US CLOUD Act). It is protected from foreign jurisdictional claims, ensuring that only local legal frameworks apply to its access, usage, and oversight.

3. Operational sovereignty

   Cloud infrastructure and services are operated, maintained, and monitored by government-owned or certified entities to comply with national standards such as audits, policies, and frameworks. This includes adherence to local audit mechanisms, staffing policies, and operational transparency.

4. Cybersecurity compliance

   The cloud environment must conform to national cybersecurity protocols and standards, such as those defined by CERT-IN (Indian Computer Emergency Response Team), MeitY (Ministry of Electronics and Information Technology), and NIC (National Informatics Centre). This ensures robust protection against cyber threats, data breaches, and unauthorized access.

7. Sustainability and self-reliance

   At its core, sovereign cloud is built on the key fundamental pillars of sovereignty, security, and sustainability. This addresses the balancing issues of data management for the customers and also aligns with the efforts across the nations in building the ability to build, control, and protect its digital future.

Table 1 provides some quick tips for decision-making in this regard.

Attribute	Global public cloud	Government-owned dc	Sovereign cloud
Data residency	May be offshore	Local	Local
Control	Shared	Full	Full (via trusted partner)
Scalability	High	Low	High
Security compliance	Varies	Moderate	High
SME involvement	High	Low	High

Table 1: Making an informed cloud choice

already dared to lead.

A benchmark today for governments across the globe is the Estonia story.

Estonia, a small Baltic nation, transformed itself from a post-Soviet state into one of the most digitally advanced societies in the world. Instead of choosing a traditional path, Estonia leapfrogged into the digital age – digitalizing all government services and launching the world's first e-residency program. While this may sound like a science fiction narrative, Estonia has faced real-world issues around protection, control, and management of data. This is where the sovereign cloud concept proved instrumental. Guided by principles of data residency, legal compliance, security, and public trust, Estonia successfully built a resilient digital backbone.

The sovereign cloud model is undoubtedly a game changer in today's environment, where governments must strengthen control and security over public data, ensure fiscal responsibility, and prepare for the accelerating impact of artificial intelligence.

As technology continues to advance, it will become increasingly difficult to address national data needs through either self-managed data centers or complete reliance on hyperscalers. A hybrid approach needs to be taken to ensure readiness for the next decade.

In countries such as India, where public-private partnerships have worked well as in case of nation-building projects such as Passport Seva and Aadhaar, further strategic collaborations will be crucial to extend the benefits of sovereign cloud models.

In summary, the sovereign cloud offers a proven, robust solution to the core challenges governments face today across data management including security, scale, cost, and

Related reading

The Role of TCS SovereignSecure Cloud™ in India's Digital Journey

TCS in the News | 06 Aug 2025

TCS-RailTel to Build Cloud Solutions using TCS Sovereign Cloud

TCS in the News | 06 Aug 2025

Accelerating India: TCS Launches Next-Gen Capabilities to Power the Country's Ambitions toward Leadership in Deep-Tech

Press Releases | 24 Apr 2025

Sovereign cloud: Setting a strategy for success

White Paper | 05 Oct 2023