View on Web

Leak-Proofing Data In A Connected World

17th Mar,2021

How do we keep our data safe? This question keeps popping up each time we engage on a digital medium. When we check and send mails, perform a transaction online or share our personal bio or professional credentials, we are worried about how secure the data is- consciously or unconsciously. Even before the digital gale swept us, you can recall how cagey you were in sending a letter by postcard and opted for a sealed envelope. That's how **data privacy** is wired into the human psyche. And, as you read this online, you feel secure being part of a secure connection. So, we are talking about 'security of security'. Data encryption counts for all- individuals, private enterprises and the government machinery. Anyone can fall prey to data breaches. Its fall-out, both financial and reputational, can be disconcerting. Picture this- ***a study by IBM says the global average cost of a data breach in 2020 stood at $3.6 million***. This makes data encryption a valued tool in the arsenal of **digital security**.

How Countries Have Enforced Data Encryption

Nations have enacted **data protection laws** or guidelines to encrypt sensitive data in crucial sectors. In the US, for instance, financial data is governed by ‘The Gramm-Leach-Bliley Act (1999) which mandates financial institutions to take up appropriate technical and physical safeguards to protect customers’ personal information from anticipated threats. Like the US, Germany follows the sectoral model to ring fence critical data in health and finance. By contrast, Japan has an overarching law- Act on the Protection of Personal Information’ that subsumes encryption across sectors. In Switzerland, the Federal Act on Data Protection requires that personal data must be protected through adequate technical and organizational measures. India lacks a unified encryption framework but sector regulators have stipulated their own standards. More, the Supreme Court order in January 2020 pronouncing that the ‘Right to Privacy is a fundamental right and an integral part of the Right to life and liberty’ has fixed more accountability on the enforcement machinery. Markets regulator SEBI specifies that data in transit should be encrypted using 128-bit encryption and this encryption is used for internet based trading. The Unique Identification Authority of India (UIDAI) mandates 2048-bit encryption with a dynamic session key for Aadhaar based authentication.

Is Data so Vulnerable?

Sample this- Google uses the strong 256-bit Advanced Encryption Standard (AES) encryption on all its Google Drive servers. And, when the data is in transit between users and Google Drive servers, Google uses the Transport Layer Security (TLS) protocol to protect the data and prevent interception. The data is largely secure. Yet, we hear instances of leakage of passwords of Google drive users. Even the passwords of Facebook users have also been compromised. If this data breach can happen to Google and Facebook, we can well fathom the vulnerabilities of other enterprises or governments too.

Why Governments Should Care About Data Encryption

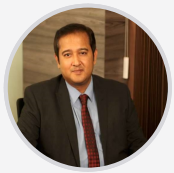
The enormous volume of data that any government manages is unmatched even by the biggest of private conglomerates. Just think- millions of tax payers and their credentials, an immense count of beneficiaries who avail government schemes or almost an entire populace that holds voter identity cards or personal identification documents like Aadhaar! The government, thus, is the custodian of this quotidian data flow on its systems and servers. A single instance of breach and you can imagine the risk of citizen data exposed. To illustrate, two cyber-attacks in 2015 targeting the US Office of Personnel Management (OPM) resulted

in personal data theft that affected 21.5 million Americans. This is where a robust data encryption system can cloak data from hackers and malware attacks. Data needs to be protected at all stages- while at rest (stored in servers or removable devices), in flight or transit or when in use. ***Data encryption helps in authenticating the origin of data, maintain data integrity by ensuring that the contents are not tampered with during transit and also non-repudiation wherein a sender can't disown or deny his message.*** Algorithms are used to encrypt and decrypt data and this checks unauthorized access to data.

Mapping A More 'Data Secure' Digital Future

As we take the digital leap, we run the risk of more sophisticated cyber-attacks that can circumvent security and steal sensitive data. People scarcely trust each other with their personal data. Here, a tamper proof platform like **blockchain** can elevate **data security** to the next level. Owing to its decentralized nature, data on a blockchain platform isn't stored in a single location- this mounts the challenge for a hacker to breach data. Another emerging evolution in data encryption is **homomorphic encryption** which allows users to process data without decrypting it, thus preventing data breaches. As nations trek on the '**Digital Transformation**' route, they need a digital security apparatus that marries compliance with competition and balances regulation with innovation.

The article was first published on Priyadarshi Nanu Pany's **Medium** profile.



AUTHOR:

Priyadarshi Pany

Chairman-cum-Managing Director & CEO