View on Web

Building Trust in India's Digital Ecosystem with Aadhaar Vault

1st Oct,2022

In India's burgeoning digital ecosystem, Aadhaar is more than a 12-digit credential. Beyond a valid proof of identity for every resident Indian, Aadhaar as a digital identifier has redrawn the contours of citizen-centric governance and deepened financial inclusion through last-mile connectivity. The massive push for Aadhaar has seen its usage climbing over the past few years. It's true that Aadhaar has stemmed frauds and leakages in our vulnerable landscape. Paradoxically, it is the same Aadhaar that has spawned incidents of data breaches and identity thefts, risking citizen's privacy.

Data breaches are inevitable when your volume of digital transactions swell and there are no ample safeguards to secure data. Today, any digital authentication is unthinkable without Aadhaar that is seeded to your mobile number, your PAN Card, voter ID card, bank account, etc. Just think the sensitive personal and demographic information that is at stake when something goes amiss in the loop of digital validation.

According to a report by the Comptroller & Auditor General of India (CAG), the Unique

Identification Authority of India (UIDAI) issued over 4.75 lakh Aadhaar cards with similar biometric data since 2019. To protect the Personally Identifiable Information (PII) of citizens, UIDAI has come up with the concept of digital locker for securing Aadhaar credentials – Aadhaar Vault.

Before we debate on how foolproof Aadhaar Data Vault is, let us understand how it works.

Demystifying Aadhaar Vault

An Aadhaar data vault stores Aadhaar numbers in an encrypted format and generates reference numbers to access them, complying with the guidelines of UIDAI. Typically, any cohesive Aadhaar Data Vault solution should consist of four key components:

Tokenization Manager:

It's like a powerful machine that creates a unique code, or "Reference Key," for each Aadhaar number. This tool is designed to handle sensitive information very carefully. It's the first stop for all the important data, and its job is to encrypt the data and keep it safe in a special place called the Data Vault. Once the data is encrypted and stored, the Tokenization Manager creates a Reference Key for it. This Reference Key helps keep track of the data as it moves around the organization, from one computer program to another, and eventually to the databases where it will be stored.

Data Vault:

It is like a big storage room where all the information is kept. Inside the Data Vault, the Aadhaar number, its encrypted version, and the corresponding Reference Key are stored securely. The Reference Key can be used and shared within the organization as needed, but the encrypted Aadhaar data stays locked away in the Data Vault where it's safe.

Hardware Security Module (HSM):

It's responsible for creating, storing, distributing, and managing the encryption keys used to protect the data. It also takes care of things like updating and changing the keys without causing any interruptions or downtime.

Bulk Transformation Utility:

It's a handy tool that can convert Aadhaar numbers to Reference Keys and vice versa using a special file format called CSV. This makes it easier to work with a lot of Aadhaar numbers at once.

How to Make Aadhaar Vault a Secure ID Locker?

The UIDAI has got a stringent mandate of securing the country's massive digital ecosystem with Aadhaar vault. However, the vault in its present form can be susceptible to data leakages. A recent audit by CAG found that data stashed in the Aadhaar vault can be vulnerable. The central auditor has recommended to UIDAI to develop a new policy for storing data to ensure its protection and to reduce the amount of unnecessary data taking up valuable space. This policy would help mitigate the risks associated with data vulnerability and protect against potential breaches. Additionally, it would help to eliminate redundant or unnecessary data, which can take up valuable space and cause data saturation. By weeding out unwanted data, the UIDAI can improve the efficiency and effectiveness of its data storage and ensure that only the most important and relevant data is retained.

Periodic audits of the Authentication Service Agency (ASA) and Authentication User Agencies (AUA) - trusted partners of UIDAI for providing Aadhaar services, can also help to contain data breaches. To comply with regulations set by the UIDAI, Requesting Entities (REs) and ASAs must have their operations and systems audited by an Information Systems Auditor who is certified by a recognized body. This audit should take place annually to ensure that all operations and systems are in compliance with UIDAI regulations. By conducting regular audits, REs and ASAs can ensure that they are operating in a secure and compliant manner, protecting the privacy and security of users' Aadhaar information.

Vaulting The Digital Economy

When built and used right, Aadhaar Vault can spell an array of benefits for the larger digital ecosystem. It can be the key to unlocking the full potential of India's digital economy and driving its transformation into a fully digital society. By instilling trust in the digital space, Aadhaar Vault paves the way for seamless digital transactions and unlocks limitless possibilities for growth and innovation.

This blog was originally published in Priyadarshi Nanu Pany's LinkedIn account.

AUTHOR:

Priyadarshi Pany

CEO & President