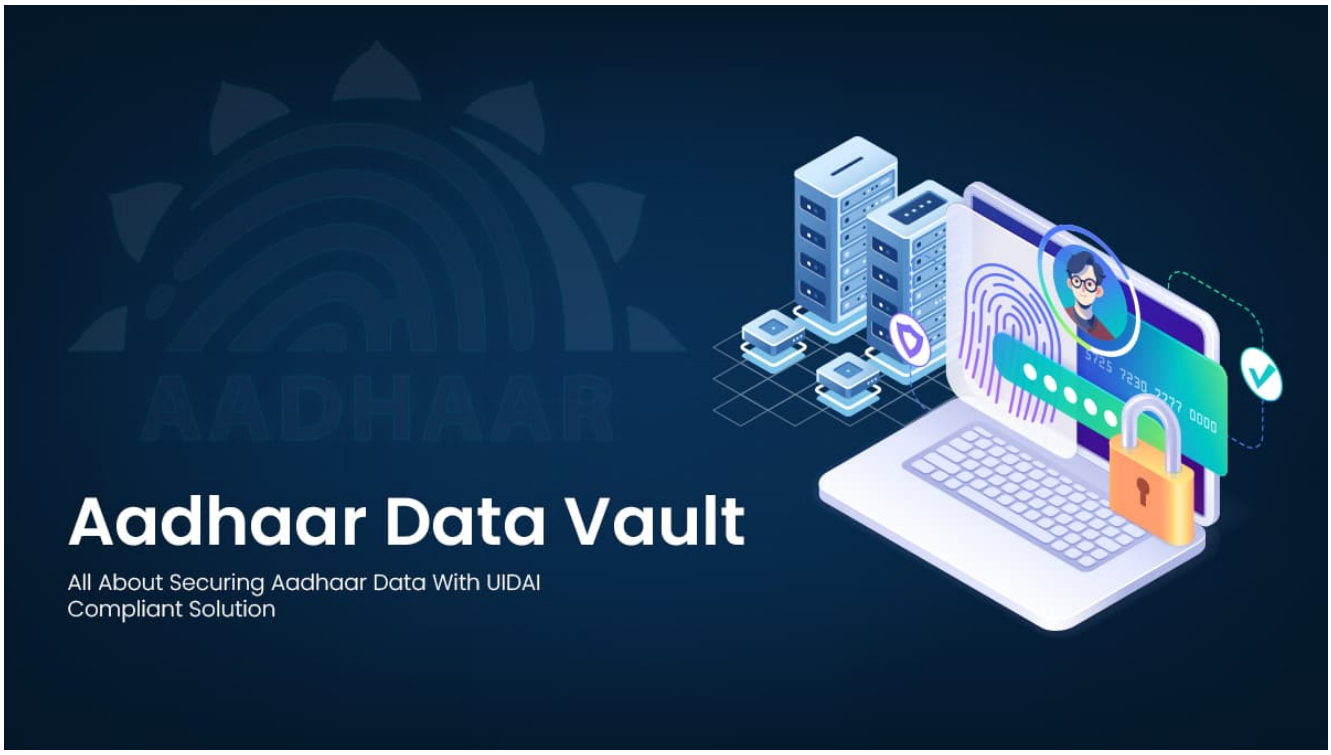
View on Web

Aadhaar Vault – Why Compliance Management is The Master Key

10th Oct,2024

In the annals of technology led disruption, India's Aadhaar program stands as a Colossus that has fundamentally transformed the landscape of citizen identification. With an enrollment of 1.3 billion citizens, Aadhaar has emerged as the world's largest biometric identification system, dwarfing similar initiatives globally. However, the scale of Aadhaar's success has also exposed it to significant vulnerabilities. At its inception, even government officials may not have fully anticipated the potential for data breaches and identity theft on a massive scale. The World Economic Forum's Global Risks Report of 2019 highlighted a chilling reality: "The largest (data breach) was in India, where the government ID database, Aadhaar, reportedly suffered multiple breaches that potentially compromised the records of all 1.1 billion registered citizens."

This revelation brought to light the inherent dangers of managing large-scale biometric and personal data repositories. In response to these vulnerabilities, the Unique Identification Authority of India (UIDAI) has taken proactive measures by mandating that entities storing Aadhaar data must use encrypted Aadhaar vaults. This vault, a centralized and secure repository, is intended to safeguard sensitive information by ensuring compliance with the Aadhaar Act and Regulations of 2016, as well as the UIDAI's 2017 circulars. Organizations tasked with installing Aadhaar vaults face a dual challenge- they must not only implement the necessary encryption technologies but also align their practices with stringent legal frameworks.



Understanding Aadhaar Vault

The **Aadhaar Data Vault (ADV),** is a solution that allows organizations to securely store encrypted Aadhaar numbers. The encryption and decryption of Aadhaar numbers are handled using keys that are stored in a Hardware Security Module (HSM), as required by the UIDAI.

All agencies that store Aadhaar numbers, whether they are Authentication User Agencies (AUAs), KUAs, Sub-AUAs, or other organizations using Aadhaar for internal purposes like attendance or linking with provident funds, must implement the Aadhaar Data Vault. To minimize the use of Aadhaar numbers in the ecosystem, each Aadhaar number is paired with an additional identifier called a Reference Key. This key replaces the Aadhaar number within the organization's system, while the mapping between the Aadhaar number and the Reference Key is securely stored in the Aadhaar Data Vault.

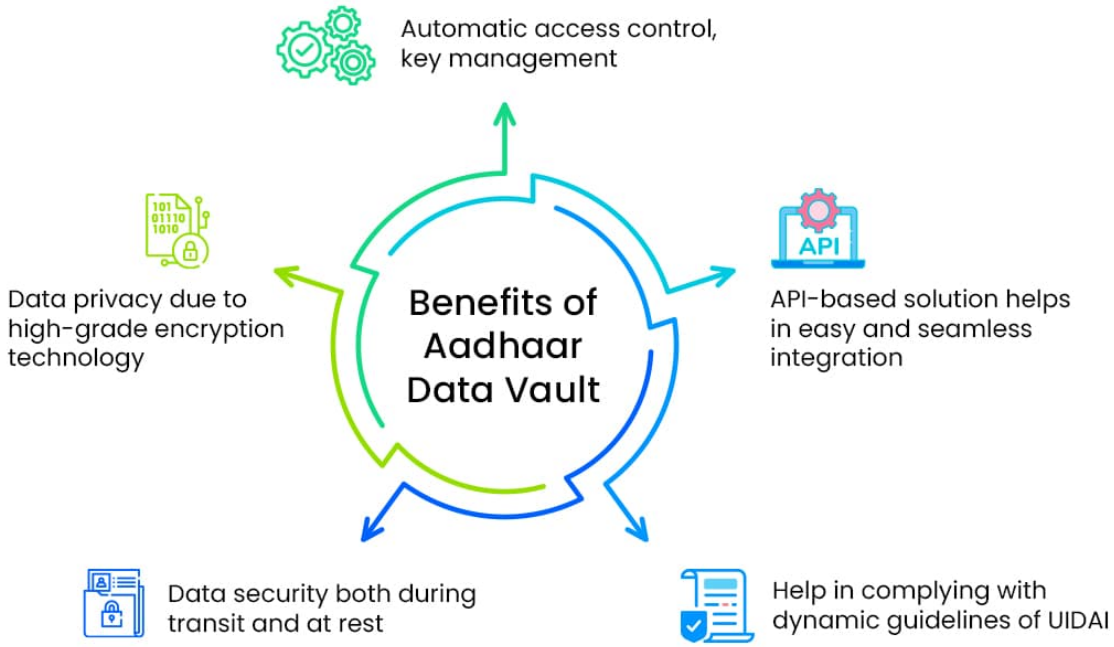
The Holistic Solution- Aadhaar Authentication Framework

The Aadhaar Authentication Framework simplifies the process of verifying genuine beneficiaries. When an authentication request is made through a device, the citizen first receives a notification. Then, the system performs authentication using demographic data, biometrics (such as fingerprints and iris scans), and OTP verification. The AUA handles updates or confirmations and sends the data through the Authentication Service Agency (ASA) to UIDAI for final verification. ASAs use secure, UIDAI-compliant connections to

ensure privacy. This system not only verifies legitimate beneficiaries but also removes fake ones, promoting transparency and efficiency through secure digital authentication.

Changing the equation of encryption with Thales-CSM Tech synergy

CSM Tech, in partnership with Thales, has been instrumental in building the Aadhaar authentication system, a crucial backbone of India's digital identity framework. By integrating Thales' cutting-edge data encryption and security solutions, the system ensures that personal data remains protected while enabling fast, seamless authentication. This guarantees that only eligible beneficiaries can access services. Central to this is the use of Thales Luna HSMs, which provide a crypto-agile infrastructure that balances high-level security with performance. The Luna HSMs ensure that all cryptographic key generation, management, and storage are securely handled within tamper-proof environments, reducing the risk of data breaches. Additionally, Luna HSMs meet UIDAI’s stringent Aadhaar Data Vault requirements, empowering organizations to safeguard and manage Aadhaar data within a secure IT framework.



Successful use cases of Aadhaar Vault compliance management

Bihar Aadhaar Authentication Framework (BAAF): The **BAAF** anchored by the Bihar Aadhaar Vault, strengthens data security, regulatory compliance, and the efficient management of Aadhaar numbers. This enhances the state’s authentication ecosystem,

making it more secure and reliable. Key benefits include:

- Reduced data leaks, safeguarding citizens' sensitive information.
- Full compliance with the Aadhaar Act and the 2017 UIDAI mandate for enhanced encryption in Aadhaar repositories.
- More accurate targeting of beneficiaries, ensuring resources reach the right people.
- Greater transparency in beneficiary data, empowering better decision-making and planning for state welfare schemes.
- These advancements make Bihar’s digital infrastructure more secure and efficient.

Impact: Twenty six departments in Bihar are using the framework, boasting an authenticated base of 596 million users

Odisha Aadhaar Authentication Framework (OAAF): Developed collaboratively by CSM Tech, Thales and the Odisha IT Department, OAAF functions as a centralized authentication gateway. This robust framework allows individual government departments to seamlessly integrate as Sub-Authentication User Agencies (Sub-AUA). OAAF effectively manages the resident data in a digitized, centralized way and in secured manner, thus enhancing Aadhaar security, and incorporating Aadhaar Authentication into various applications. It supports Secure Authentication using Registered Device (RD), Virtual ID (VID), used for privacy protection by introducing an encrypted Aadhaar format and storing of UID token on UIDAI response. The **Aadhaar Data Vault** containing Aadhaar number/data and the referencing system kept in an isolated and highly restricted network zone. Keys used for encryption are stored in Thales Luna HSM only.

Impact Metrics

Government Departments using the framework: 16
Authenticated User Base: 987 Million

Aadhaar Vault has emerged as a pivotal solution in strengthening governance, enhancing compliance, and improving citizen experiences. By securing sensitive data and aligning with stringent regulatory mandates, it significantly reduces the risks of breaches and identity theft. The successful integration of Aadhaar Vault within various states, such as Bihar and Odisha, highlights its impact on creating a more secure, transparent, and efficient authentication system.

AUTHOR:

Jayajit Dash

Senior Manager- Corporate Communications (Marketing)