Aadhaar authentication failure in Supreme Court is a fake issue

RAJESH BANSAL 3 April, 2018

A person giving biometrics for Aadhaar | Wikimedia Commons

It is very clear that the issue is not of the Aadhaar's biometrics platform or its architecture, but that of implementation by state agencies/institutions.

As per my understanding, the current efforts of government authorities are to detail technical aspects of the Aadhaar programme to the Supreme Court.

The presentation made by the UIDAI on various aspects also reportedly included the security of Aadhaar, which is based on 2048-bit encryption of biometric data at source of capture (at the enrollment device). This is the current encryption standard being followed by UIDAI, and without a doubt, it would take billions of years for anyone to decrypt such data.

Having said this, UIDAI, as a trustee of this data, shall also be innovating itself continuously in terms of international security standards as the world of cryptography evolves. Hence, the alleged fear of UIDAI's biometric data being breached or tampered with or stolen at the time of enrolment is nothing but a fallacy for sure.

Now, let's we examine the world of smart cards versus the online biometrics system of Aadhaar. First, most of the smart card applications deployed in India (including banks in the offline version of financial inclusion) captured biometrics data of millions of customers by using proprietary techniques and the data was mostly available with the vendors and could only be burnt on the smart card using the vendors' private keys, unlike Aadhaar, wherein the key pair used to store and encrypt data is owned by the UIDAI.

Second, the data was also stored on the servers of the private vendors in these smart card applications, whereas Aadhaar data is securely stored through registered devices and fully managed by the UIDAI.

Third, in the case of smart cards, all the transaction data of the person is stored on the card itself, and hence it is possible to obtain the entire transaction history, e.g. cash withdrawals/deposits including the device used and the location, etc. In the Aadhaar architecture, UIDAI only knows that a particular Aadhaar number was used by the holder at an institution's device. But UIDAI never knows if the person has withdrawn or deposited money or just placed his/her attendance. Basically, UIDAI does not know the purpose for which Aadhaar authentication has been used by the Aadhaar-holder.

There is hence no reason for people to suspect that the bank account details including deposits/withdrawals can be tracked by UIDAI. Hence, smart card applications are more prone to surveillance than analytics' prognosis of the Aadhaar system.

Fake issues like that of UIDAI CEO being unable to authenticate himself on certain occasions do not hold any ground, as it is patently due to well-known reasons of meagre connectivity of telecom service networks at particular moments, resulting in frequent call drops, which is experienced by us all. The authentication has been successful otherwise. After all, Aadhaar has more than four crore authentications per day. A few stray incidents cannot cast a doubt on a system's performance as a whole.

This reminds me of my experience when serving UIDAI in 2011-12. We were in the field in Ratu block of Ranchi, Jharkhand, where we were doing the first set of pilots for Aadhaar online authentication. I had carried a particular telco's SIM card in some of these areas and started facing issues of non-responding unreliable connection. The villagers around me were amused and showed off their phones with very powerful telecom signal of other telcos. We then switched to BSNL and another company's network, and there was no looking back.

As per media reports, it is also learnt that UIDAI also presented that the authentication is not 100 per cent perfect. Logical! Who can claim to be 100 per cent perfect? The thing to note is that the telecom sector success rate is 97 per cent as compared to 88 per cent for the government. Hence, it is very clear that the issue is not of Aadhaar's biometrics platform or its architecture, but that of ground implementation by some state agencies/institutions.

The solution is to monitor device-level failure rates and then take remedial steps to improve the success rate at ground-level executing agencies. It, once again, reminds me of the first state in which we implemented the full scale rollout of the Aadhaar online biometric authentication in 2013 for disbursal of MGNREGS and old age pensions. To our utter surprise, we started getting a lot of rejections in the first couple of months. Then our team conducted a detailed analysis and found that at some positions, the success rate was recorded at less than 50 per cent and at some other positions more than 95 per cent for people with similar demographics.

We then called the bank(s) concerned and conducted field visits to realise that agents deployed by the bank(s) were keying in the beneficiary Aadhaar number but deliberately using someone else's number.

There was an enabling provision that if biometrics does not authenticate in more than five attempts, a manual payment could be made. Hence, they were siphoning off the money through this method by blaming it on authentication failure.

They were doing something similar in the smart cards as well, but there was no way for the state government to track the failure rate, as most of the reconciliation was offline. We then worked closely with the state government to solve this issue, and the success rate shot up drastically.

This is the exact point UIDAI is perhaps making when they speak about vested interests trying to subvert the Aadhaar system.

About the UIDAI CEO's transaction log being available, one has to note that he had himself submitted his personal authentication history as an example of how it looks like. An Aadhaar-holder can decide to share his/her details with anyone he/she wants to share the details with. This is what a consent-based model is.

It may also be noted that this is an OTP-based facility available to the Aadhaar holder on his/her mobile registered with the Aadhaar database. Such information is not shareable as per the Aadhaar Act without order of the Court and/or in the interest of national security, under the directions reviewed by an oversight committee headed by the cabinet secretary.

Rajesh Bansal is a former assistant director general at UIDAI, and former general manager at the Reserve Bank of India. Views are personal.