Virtual Identity of Aadhar

- The Unique Identification Authority of India (UIDAI), which is facing criticism in the light of alleged data breaches has announced a new method of identification called Virtual Identity — or VID in short.
- Essentially, the new VID system will hide the Aadhaar number from the authenticating agency, while still confirming the identity of the user.

What is VID? How will it be different from the Aadhaar number itself?

- VID will be a 16-digit number, which will be temporary in nature. So, unlike the 12-digit Aadhaar number that is permanent, the VID will have a certain period of validity, at the end of which it will expire, and the user will have to generate a new one.
- UIDAI is yet to say what the minimum validity period for the VID will be.
- A VID will automatically expire when a user generates a new one, as there can only be one valid VID number against a particular Aadhaar number at any given point in time.
- While it is not compulsory to use or generate a VID, the UIDAI is pitching it as another option for authenticating identity, which it claims is more secure.
- The VID cannot be used by agencies for duplication, and it cannot be generated by the Authentication User Agency (AUA) either.
- When you give your Virtual ID to an authentication agency, say a telecom company or a local government body, they will enter it into the system and then receive a UID token that authenticates it, and provides a limited set of demographic details, such as your name, phone number, address and so on. Simply put, these agencies will now be able to authenticate you without ever actually seeing your Aadhaar number.

How to generate VID:

- Users will be able to generate the VID from the Aadhaar resident portal, Aadhaar Enrolment Centres, and the mAadhaar app on Android.
- UIDAI will implement the VID service only from March 1.
- UIDAI expects all authentication bodies to move to the new VID system latest by June 1, 2018.

Is it more secure?

- The Unique Identification Authority of India claims it will not be possible to derive the Aadhaar number from the Virtual ID. Moreover, different agencies will be given different UID tokens to authenticate the same Aadhaar – meaning they will not simply be able to merge their information and build a picture of the Virtual ID holder.
- A key aspect of the security is that the Virtual ID is temporary and revocable. This means that it matters less if an agency stores your Virtual ID in the hope of profiling you, since Virtual IDs are not permanent and can change. The Unique Identification Authority of India has indicated that it will have an upper time limit for Virtual IDs.

Associated Issues:

- Aadhaar was originally envisioned as a way of improving welfare delivery and providing an identity to those who do not have any. Yet, the poor and the needy, the ones who already find themselves excluded by Aadhaar, now have to make that extra effort to generate a Virtual ID in order to access subsidies or even entry to night shelters.

- Too short a time, say a few months, and it will be a massive inconvenience to those who need Aadhaar the most, since they are unlikely to have access to the mAadhaar app or the time to line up at an enrolment centre just to generate Virtual IDs. Too long a time, and the Virtual ID will just replace the Aadhaar number, allowing conmen to use demographic data connected to the Virtual ID in attempts to defraud Aadhaar holders.
- Despite the introduction of the VID system, there are several privacy issues which remain unresolved. One is that this system neither addresses nor takes into account the sheer volume of Aadhaar numbers that have already been shared. The mandatory linkages of Aadhaar with various services, and the increasingly common use of Aadhaar for KYC has led to Aadhaar numbers already entering into the possession of several entities. The deadlines for many linkages, in fact, is March 31st, the very date from which the Virtual ID system will be made available. As the website database leaks since the last year showed, several Aadhaar numbers have already been compromised. The virtual ID system in no way addresses any of these problems.
- Another issue is that the virtual ID system is optional, and not mandatory. This, again, will limit the impact of this system to reduce Aadhaar number disclosures.
- It is questionable how many people will adopt the Virtual ID system or understand its significance.
- People have in no way been impressed with the need to keep their Aadhaar number a secret. The UIDAI itself has not taken a clear stand on the secrecy of the Aadhaar number, with its statements made earlier that the Aadhaar number is not a ‘secret’ number.
- Sharing the Aadhaar number through a xerox of the Aadhaar card has become one of the most common steps taken by people for KYC and other purposes today.
- The Virtual ID system would be a lot more effective if all Aadhaar holders received new Aadhaar numbers which are masked on the Aadhaar card, and then mandated to use Virtual IDs. Such a large scale overhaul of the Aadhaar system is, however, unlikely.
- Another significant issue with this system is that it does not in any way address the risks involved with the use of biometric data in the Aadhaar ecosystem.
- That data will continue to be used by the same agencies, even if Virtual IDs or limited KYC were to be implemented. This is a bigger risk than that of sharing the Aadhaar number.
- The extent of services linked with Aadhaar, with biometric data as the only bar, will make biometric data the biggest target of cybercriminals.
- It is a huge mistake to think that securing the CIDR alone will resolve problems since people are also giving out biometric data everywhere, everytime they touch something, or even if they just upload a picture of themselves online. Even a high-end camera could easily be used to obtain iris scans of a person.
- There have also been many reports on the abuse of the Aadhaar system. For instance, the UIDAI itself discovered and acted against fake apps being introduced to extract Aadhaar numbers. It is perfectly conceivable to have fake payment apps which extract not just Aadhaar and account numbers, but biometric data as well. Reports have also come out on replay attacks, which allowed malicious players to save and reuse biometric data for fraudulent transactions.
- The most recent development in the Aadhaar issue is the UIDAI’s announcement of new ‘Virtual IDs’, a temporary, virtual ID to be used and shared, in place of the actual Aadhaar number. This move is, on the one hand, a welcome acknowledgment of the privacy and

security issues with Aadhaar, as opposed to the UIDAI’s characteristic denial of privacy allegations. The removal of access granted to officials and the link of database access to biometrics are other good steps. On the other hand, this move can only partially resolve a single privacy issue — that of securing the Aadhaar number.

Way Forward

- If this move of introducing Virtual IDs is the first of a much larger, holistic movement towards better security/privacy in the Aadhaar ecosystem, then it is very welcome. As a stand-alone step, however, it resolves very little. To fully deal with the issues with Aadhaar, a lot more needs to be done. To look at it positively, at the very least, this move is a sign of an acknowledgement of and is a step towards resolving the security and privacy issues with Aadhaar.