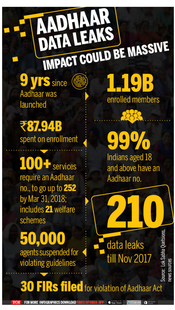
Aadhaar Data Breach

Aadhaar - meaning foundation - was created in 2009 to fight with logistical issues in India.

It was developed as a tool to standardize the process of data collection and ease the distribution of money from government to the citizens of the country, especially the poor people.

Aadhaar is one of the biggest biometric databases on the planet with around 1.2 billion enrollments, covering around %89 of India's population.

In November of 2017, more than 200 government websites were revealed to have published the Aadhaar numbers of citizens along with the names, addresses and bank details.



The Unique Identification Authority of India (UIDAI), the government body that administers Aadhaar, said that in that case the information had been accidentally published by other government departments and was removed as soon as the breach became apparent.

In January of 2018, The Tribune newspaper said its reporters were able to access names, emails, phone numbers and postal codes by typing in 12-digit unique indentification numbers of people in the Aadhaar, after paying an individual about $8.

Also The Tribune team paid $5, for which the agent provided "software" that could facilitate the printing of the Aadhaar card after entering the Aadhaar number of any individual.

However the UIDAI called that news is fake. They also filed a criminal complaint against the newspaper. But that news was true.

In the first six months of 2018, almost 1 billion records were compromised in Aadhaar breach incident, including names, addresses and other personally identified informations.

First discovered time is not clear enough. However breach was disclosed to the public at March 23, 2018.

Aadhaar breach is the largest breach that happened in 2018. Also The WEF Global Risk Report recognized the Aadhar breach as the largest data breach in the world.

		How Many People Affected	Disclosed
1	Aadhaar Breach	1,000,000,000	January 2018
2	Starwood-Marriot Breach	500,000,000	September 2018
3	Exactis Breach	340,000,000	June 2018
4	Under Armour-MyFitnessPal Breach	150,000,000	February 2018
5	Quora Breach	100,000,000	December 2018
6	MyHeritage Breach	92,000,000	June 2018
7	Facebook Breach	87,000,000	September 2018
8	Elasticsearch Breach	82,000,000	November 2018
9	Newegg Breach	50,000,000	September 2018
10	Panera Breach	37,000,000	April 2018

"Securing an entire ecosystem is more important than secure individual databases," said security researcher Srinivas Kodali.

There was no reports of any breach in the core database of Aadhaar. However, it is the third-parties that have acted as weak links.

"The simple parallel that can be drawn is, though Facebook's core database of users information was secure, the data leak happened through third-party developers and organisation like Cambridge Analytica." Kodali said.

In case of Aadhar too, the allegations of breaches have not been on 'Aadhaar database' but rather at insecure government websites and third-parties with API access to the database. "In this aspect, the issue in Facebook and Aadhaar is similar. In both the cases there was no breach of database, but it was third parties that acted as the weakest link. In both cases, it was a legitimate means of access through API that was open for abuse," said Sunil Abraham, executive director, Center for Internet and Society.

Summary

How it happened: The Indian government, which manages the ID database "Aadhaar," ignored repeated attempts by security researchers to secure a database leak caused by an unsecured API endpoint connected to a state-owned utility company. It was only after the vulnerability was publicly disclosed that the government secured the database.

What was included:

- Names
- Unique 12-digit identity numbers
- Information about services they are connected to, such as bank details and other private information

Disclosed to the public: March 23, 2018