AADHAAR SECURITY BREACHES: HERE ARE THE MAJOR UNTOWARD INCIDENTS THAT HAVE HAPPENED WITH AADHAAR AND WHAT WAS ACTUALLY AFFECTED

Despite the number of reports over the last couple of years, UIDAI has maintained that the Aadhaar server and the biometric data is safe.

TECH2 NEWS STAFF SEP 25, 2018 19:34:06 IST

Editor's note: *This copy was published on 24 January, 2018. It is being republished in light of the Supreme Court's verdict on the constitutionality of Aadhaar likely being pronounced tomorrow.*

Aadhaar Database is one of the largest government databases on the planet, where a 12 digit unique-identity number has been assigned to the majority of the Indian citizens. This database contains both the demographic as well as biometric data of the citizens.

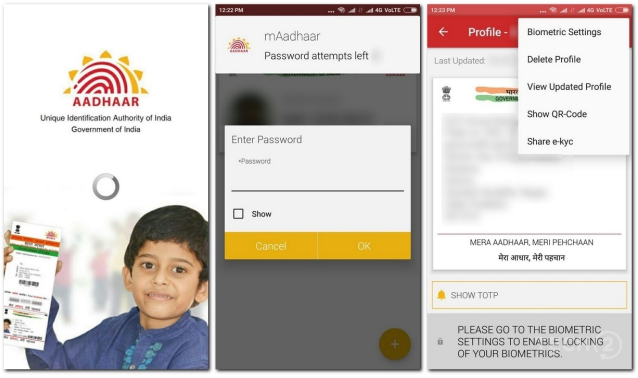
A file photo of Aadhaar registration. Reuters

With the sheer amount of private and confidential data amassed in one singular database, it is no surprise that Aadhaar and Unique Identification Authority of India (UIDAI), the authority that established the database, continue to be the focus of attention whenever there is any security shortcoming.

Irrespective of the number of complaints and objections against the program, the government of India has made it mandatory in almost all the facets of public life. Despite the number of reports over the last couple of years, UIDAI has constantly maintained that the server and the data itself, especially **biometric data is safe**. We are not contesting the claims by the authority. However, we do think that the number of security incidents has increased in past few years and we wanted to highlight everything major that has happened.

App-based flaws

Most recently, the entire controversy around Aadhaar and privacy concerns, captured centre stage after a French security researcher **pointed the flaws in** the mAadhaar app that is available on the Google Play Store. What is striking is the fact that this is not the first time when the issue has been raised about a government mobile app with flaws that can potentially allow attackers to access the Aadhaar database while accessing the demographic data.



An IIT graduate was arrested for **illegally accessing the Aadhaar database** back in August 2017 for accessing the database between 1 Jan and 26 July without authorisation. He created an

app called 'Aadhaar eKYC' by hacking into the servers related to an 'e-Hospital system' that was created under the Digital India initiative. The eKYC app would then route all the requests through those servers.

Government Websites

Over the last one year, there have been multiple instances of Aadhaar data leaking online through government websites. The most recent case was when an RTI query pushed UIDAI to reveal that about **210 government websites made** the Aadhaar details of people with Aadhaar, public on the internet. The report pointed out that the data was removed from the websites but it also did not mention about the time frame of the leak of the data.

The problem was so rampant that **a simple google search** would reveal thousands of databases along with demographic data including Aadhaar numbers, names, names of parents, PAN numbers, mobile numbers, religion, marks, the status of rejection of applications, bank account numbers, IFSC codes and other information.

Google. Pixabay

Three **Gujarat-based websites** were also found disclosing Aadhaar numbers of the beneficiaries on their websites. Last but not the least, a website run by Jharkhand Directorate of Social Security leaked **Aadhaar details about 1.6 million** people living in Jharkhand due to a technical glitch.

Centre for Internet and Society (CIS) also pointed out that **about 130 million Aadhar numbers** along with other sensitive data were available on the internet. The reason for the data leak was narrowed down to four government-run schemes ranging from National Social Assistance Programme by the Ministry of Rural Development, the National Rural Employment Guarantee Act (NREGA), also by the Ministry of Rural Development, Daily Online Payment Reports under NREGA by the government of Andhra Pradesh and the Chandranna Bima Scheme, also by the government of Andhra Pradesh.

Third party leaks

There have been a number of leaks when it comes to demographic data. Sometimes the leak happens because of a picture is tweeted to showcase the infrastructure such as the

time when Aadhaar card application of **MS Dhoni leaked** on the internet. The reason for the leak of the form was that the CSC e-governance Services India Ltd tweeted the picture of the machine with Dhoni's form still on the screen with a bulk of personal details visible. This prompted UIDAI to blacklist CSC e-governance services for 10 years.

Aadhaar registrations

UIDAI has also regularly shut down '**fraudulent websites**' and mobile apps that claim to provide Aadhaar services to users as done almost a year back. It also **blocked about 5,000 officials** from accessing Aadhaar portal after it was reported that the portal was accessed without any authorisation.

It is almost amusing to note that it was not the first time that UIDAI blacklisted officials or operators. Back in 2017, it **blacklisted about 1,000 operators** and filed FIRs against 20 individuals for malpractice. The report did not point at any security issues but did state that charging for Aadhaar was illegal.

The most recent case was the investigative story done by a journalist from *The Tribune*, who uncovered a racket wherein you could get access to the Aadhaar data if you **paid a sum of Rs 500** to certain individuals on a closed WhatsApp group.

Misuse of Aadhaar

A report from a year ago implied that several parties illegally tried to store the biometric data and **conduct multiple transactions** using the same fingerprint. UIDAI detected the problem when it found multiple transactions done using the same fingerprint. The official who spoke on conditions of anonymity to *Livemint*, said that this would not have been possible without storing biometric data.

Image: Airtel

The story is not over about the misuse of Aadhaar as the organisation **suspended the eKYC license** of Bharti Airtel and Airtel Payments Bank after they violated the Aadhaar Act which barred the company from opening bank accounts of their customers without undertaking any informed consent from them.

Duplicate Aadhaar cards

Apart from the usual fear associated with hackers breaching the Aadhaar database, the menace of fake Aadhaar cards is also a problem for UIDAI. According to a **report last year, a gang in Kanpur** was running a racket in order to generate fake Aadhaar cards. UIDAI stated that its systems detected abnormal activities and filed a complaint accordingly. It clarified that the big scam to generate the fake cards was foiled by the system and it did not affect the database of the processing system.

What is interesting is that **UIDAI refused to disclose** the number of fake or duplicate Aadhaar cards in circulation citing the threat to national security. So much for transparency and accountability on the part of UIDAI and the government.

Demographic data on sale

A recent investigation by *The Tribune* uncovered that anonymous individuals were **ready to sell the Aadhaar card details of any individual** with an Aadhaar number against the payment of a sum of Rs 500. An additional Rs 300 would also let you print out these Aadhaar cards. The investigating team was able to get a Login ID and username that allows the team to check details of any of the

users in the database. What was surprising to note is that the 'agents' were running a racket using messaging platforms as WhatsApp to reach out to potential buyers.

Access to the Aadhaar demographic data is not the only issue here. An additional Rs 300 could also let the 'agent' with a login ID and username to print any Aadhaar card after entering the card number. The report also pointed out that the agents hacked into the website of Government of Rajasthan to gain access to the software. According to the report, the investigator was able to gain immediate access to particulars of all the users listed by UIDAI including name, address, photograph, email ID as well as the mobile phone number.

Other claims

The claims about unauthorised access to the Aadhaar database is not limited to the websites in the country. According to a **previous report last year**, WikiLeaks tweeted claiming that CIA might have access to the database as well.

The series of tweets claimed that CIA was using Cross Match Technologies to access Aadhaar database as this company was one of the first suppliers of biometric devices certified by the UIDAI. The report claimed that CIA was using Express Lane, a covert information collection tool to ex-filtrate the data collection.

TAGS

AADHAAR | AADHAAR DATA LEAK | AADHAAR NUMBER | AADHAAR SPECIAL | BIO-METRIC DATA

Find latest and upcoming tech gadgets online on Tech2 Gadgets. Get technology news, gadgets reviews & ratings. Popular gadgets including laptop, tablet and mobile specifications, features, prices, comparison.

ALSO SEE

NEWSTRACKER

Aadhaar data breach: UIDAI refutes media reports, says biometric information safe and secure, no leakage occurred

Jan 04, 2018

NEWSTRACKER

Aadhaar database access found to be sold on WhatsApp for Rs 500; UIDAI official

Jan 04, 2018

CRITICALPOINT

Aadhaar Virtual ID is a proactive move to fix privacy holes but might be useless without

Jan 12, 2018

Illegal agencies and operators will be blacklisted and get punishment for up to 3

Mar 24, 2017

CRITICALPOINT

Aadhaar's new Face Authentication system opens up a Pandora's box of problems

Jan 16, 2018

NEWSTRACKER

No Aadhaar data breach has been recorded since its inception, claims

Jan 15, 2018

SCIENCE

SHARKS

Shark teeth lost in Antarctica millions of years ago recorded Earth's climate history

Jul 13, 2021

HEAT WAVE

Rising temperatures can cause heat waves: Here are three tips to prevent heat stroke

Jul 13, 2021

DINOSAURS

Earth was home to billions of T-rex over lakhs of generations, suggests new study

Apr 16, 2021

CORONAVIRUS HUG

Nurse embracing patient in Brazil wearing 'hug curtain' wins World Press Photo

Apr 16, 2021

Site Index