Done?	Accessed By	Article Title	Journalist Name	Publishing House	Article Summary	Website/Link	Date of Publishing	PDF Filename (IndianExpress_SrinivasJanyala_17April2019)	Comments (if any)
Yes	Prakhar	Aadhaar Security Breaches	Tech2 News Staff	First Post	This article covers a set of attacks: 1) An IIT graduate hacked into Aadhaar illegally and accessed the database without authorization between Jan 1 and July 26. He created an app called 'Aadhaar eKYC' by hacking into the servers related to an 'e-Hospital system'.		Sep 25, 2018	FirstPost_Tech2Team_25September2018	
Yes	Prakhar	UIDAI reveals 210 govt websites made Aadhaar details public, did not specify when breach took place	-	First Post	Approximately 210 websites of central government, state government departments including educational institutes were displaying the list of beneficiaries along with their name, address, other details and Aadhaar numbers for information of general public. The data could be even serached online on google by just querying for Aadhaar number.	https://www.firstpost.com/india/uidai-reveals-210-govt-websites-made-Aadhaar-details-public-did-not-specify-when-breach-took-place-4217597.html	Nov 19, 2017	FirstPost_-_19November2017	
Yes	Prakhar	Three Gujarat websites including government portal made Aadhaar details public	Ashish Chauhan	Times of India	Three official Gujarat websites have been found flouting Aadhaar Act and publicly disclosing Aadhaar numbers of beneficiaries on their websites. Deputy chief minister Nitin Patel, on Sunday, said he was unaware of the issue. The three errant websites are that of Gujarat government, Director of Developing Caste Welfare of the state and Gujarat University. In these, lists of beneficiaries along with their names, addresses and Aadhaar details have been displayed publicly.	https://timesofindia.indiatimes.com/city/ahmedabad/three-gujarat-websites-including-govt-portal-made-Aadhaar-details-public/articleshow/62406648.cms	Jan 8, 2018	TimesOfIndia_AshishChauhan_8January2018	
Yes	Prakhar	Aadhaar biometric data breach triggers privacy concerns	Suranjana Roy, Komal Gupta, Apurva Vishwanath	LiveMint	The UIDAI filed a police complaint on 15 February 2017 against Axis Bank Ltd, business correspondent Suvidhaa Infoserve and e-sign provider eMudhra, alleging they had attempted unauthorized authentication and impersonation by illegally storing Aadhaar biometrics. A case of Aadhaar data breach has caused privacy concerns and raised questions over the security of biometric data in possession of the Unique Identification Authority of India (UIDAI).	https://www.livemint.com/Industry/IKgrYL5pg3eTgfaP253XKI/Aadhaar-data-breach-triggers-privacy-concerns.html	Feb 25, 2017	LiveMint_Suranjana Roy_25February2017	
Yes	Prakhar	UIDAI Blacklists Centre That Leaked Aadhaar Details of M S Dhoni for 10 Years	-	Outlook	Aadhar "Receit" of MSD was leaked. The Aadhaar official who posted this has been blacklisted. There have been multiple such incidents with the entities being invariably backlisted by UIDAI acc the CEO	https://www.outlookindia.com/newswire/story/uidai-blacklists-centre-that-leaked-Aadhaar-details-of-m-s-dhoni-for-10-years/967445	Mar 29, 2017	Outlookindia_-_29Match2017	
Yes	Prakhar	UIDAI suspends eKYC licence of Bharti Airtel, Airtel Payments Bank over violation of Aadhaar Act	PTI	EconomicTimes	Allegedly of Bharti Airtel using the Aadhaar-eKYC based SIM verification process to open payments bank accounts of its subscribers without their 'informed consent'. UIDAI also took strong objection to allegations that such payments bank accounts are being linked to receive LPG subsidy. Their eKYC was temporarily suspended after their reponce to multiple of UIDAI concerns was untasifactory.	https://economictimes.indiatimes.com/news/politics-and-nation/uidai-suspends-airtel-airtel-payments-banks-e-kyc-licence-over-Aadhaar-misuse/articleshow/62096832.cms	16/December/2017	EconomicTimes_PTI_16December2017	
Yes	Prakhar	Rs 500, 10 minutes, and you have access to billion Aadhaar details	Rachna Khaira	The Tribune	It took just Rs 500, paid through Paytm, and 10 minutes in which an "agent" of the group running the racket created a "gateway" for this correspondent and gave a login ID and password. The hackers seemed to have gained access to the website of the Government of Rajasthan, as the "software" provided access to "Aadhaar.rajasthan.gov.in", through which one could access and print Aadhaar cards of any Indian citizen. People on payment through Paytm were being given apps to form 'fake Aadhaar cards'.	https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-Aadhaar-details/523361.html	4/January/2018	TheTribune_RachnaKhaira_4January2018	
Yes	Prakhar	WikiLeaks hints at CIA access to Aadhaar data, officials den	Rachel Chitra	Times of India	Because of the aborementioned system, CIA can have all the Aadhaar data: The OTS (Office of Technical Services), a branch within the CIA, has a biometric collection system that is provided to liaison services around the world -- with the expectation for sharing of the biometric takes collected on the systems. But this 'voluntary sharing' obviously does not work or is considered insufficient by the CIA, because ExpressLane is a covert information collection tool that is used by the CIA to secretly exfiltrate data collections from such systems provided to liaison services. ExpressLane is installed and run with the cover of upgrading the biometric software by OTS agents that visit the liaison sites. Liaison officers overseeing this procedure will remain unsuspicious, as the data exfiltration disguises behind a Windows installation splash screen. The core components of the OTS system are based on products from Cross Match, a US company specializing in biometric software for law enforcement and the Intelligence Community. The company hit the headlines in 2011 when it was reported that the US military used a Cross Match product to identify Osama bin Laden during the assassination operation in Pakistan.	https://timesofindia.indiatimes.com/india/wikileaks-hints-at-cia-access-to-Aadhaar-data-officials-deny-it/articleshow/60228184.cms	26/August/2017	TimesOfIndia_RachelChitra_26August2017	
Yes	Preetha	Fingerprints, Aadhaar and Law Enforcement – A Deadly Cocktail Is in the Making	Anand Venkatanarayanan	The Wire	UIDAI denied NCBR's claims to accessing the Aadhaar database. Writer claims that the Aadhaar DB can still be used in order to carry out 1:1 searches. Such an architecture makes the legal construct of "consent and purpose limitation"	https://thewire.in/tech/Aadhaar-fingerprints-ncrb-police-investigations	16/August/2019	TheWire_AnandVenkatanarayanan_16August2019	-
Yes	Vineet	UIDAI: Police suspicion that Aadhaar data stolen was unfounded	Sreenivas Janyala	Indian Express	UIDAI said that it's CIDR and servers are completely safe and fully secure and no illegal access was made to its CIDR and no data has been stolen from its servers. But the Hyderabad Police believe that the AP Govt and TDP have leaked information.	https://indianexpress.com/article/india/uidai-police-suspicion-that-Aadhaar-data-stolen-was-unfounded-5681179/	17/April/2019	IndianExpress_SrinivasJanyala_17April2019	-
Yes	Vineet	Indane Leaked Millions of Aadhaar Numbers, Claims French Researcher	The Wire Staff	The Wire	A security lapse on the part of Indane has exposed millions of Aadhaar numbers, according to an analysis Baptiste Robert (Eliot Alderson). A part of the website that is only supposed to be available to dealers and distrubtiors, was left open and public. Using this, 11000 dealer's details have been exposed. Using the dealer details, 5.8 million Indane customers details were scraped. However, Indane rejects all these claims.	https://thewire.in/tech/indane-leaked-millions-of-Aadhaar-numbers-claims-french-researcher	19/Februrary/2019		
Yes	Swagam	Fake Aadhaar card network busted in Kanpur	Omar Rashid	The Hindu	The accused accessed the fingerprint impressions of authorised Aadhaar enrolment operators on the UIDAI system. They would then print out the fingerprints on butter paper. After this, the accused would create artificial fingerprints using polymer resin. Additionally, the accused would bypass the biometric norms of the UIDAI with fingerprint copies and tamper with the source code of the UIDAI application client (software used by Aadhaar enrolment agencies) to create a fake application client. They would then bypass the operator authentication process to create fake Aadhaar cards. The hackers would send the client application to unauthorised operators for a sum of Rs.5,000 each, police said.	https://www.thehindu.com/news/national/uttar-pradesh-police-busts-fake-Aadhaar-card-network/article19660140.ece	11/September/2017	TheHindu_OmarRashid_11September2017	**Similar attack**
Yes	Rohan	Aadhaar Operator's Biometrics Stolen & Misused, UIDAI Documents Prove	Yes	Huffington Post	Tech-support emails accessed by HuffPost India showthe UIDAI has confirmed that Sheokhand's credentials were used in multiple places in a single day, on at least one other day, November 8 2018. For this reason, on Nov 13 2018, the UIDAI barred Sheokhand from working as an enrolment operator for five years. Yet strangers continue to try to use his digital fingerprints in different banks across the country.	https://www.huffingtonpost.in/entry/Aadhaar-operators-biometrics-stolen-misused-uidai-documents-prove_in_5c6cf9a4e4b0e2f4d8a0ae2a	20/February/2019	HuffingtonPost_RachnaKhaira_20February2019	
Yes	Rohan	7.8 Crore Citizens' Aadhaar Data Stolen And Misused, Threat To National Security Too	Prithvi Raj	The Logical Indian	It Grids (India) Pvt Ltd, a Hyderabad based IT company has been booked for illegally holding possession of 7.8 crore records of Aadhaar data and misusing the same. IT Grids is the same company which built the "Seva Mitra" app, the official Telugu Desam Party app. The special investigation team discovered that IT GRID had been hosting the Aadhaar number and related identity information of citizens in Amazon Web Services, a US-based company, thereby giving Amazon access to our nation's confidential data	https://thelogicalindian.com/awareness/sensitive-data-stolen/	18/April/2019	TheLogicalIndian_PrithviRaj_18April2019	
PARTIAL	Rohan	Aadhaar PRIVACY ISSUES EXTEND BEYOND THE SECURITY OF ITS BIOMETRIC DATABASE	Abhishek Puri	First Post	telecom regulatory chief Mr R.S. Sharma's details linked to his aadhar released, Sharma has claimed, and he's probably right, that no harm could come to him if his Aadhaar details were to be made public.	https://www.firstpost.com/tech/news-analysis/Aadhaar-privacy-issues-extend-beyond-the-security-of-its-biometric-database-4848791.html	25/September/2018	FirstPost_AbhishekPuri_25September2018	Not directly an attack but a lot of details and accounts were made based on just the aadhar numbe
Yes	Rohan	Big data breach! Aadhaar software hack raises major security concerns		Buisness today	A software patch, which can be bought for as little as Rs 2,500 - reportedly allows unauthorised persons, based anywhere in the world, to generate Aadhaar numbers.	https://www.businesstoday.in/current/economy-politics/Aadhaar-software-hack-uidai-data-ghost-entries/story/282260.html	11/September/2018	BusinessToday_-_10September2018	
	Preetha	The 360 Degree Database	Anand Venkatanarayanan	Medium	Talks about SRDH's. The UIDAI basically states that state govts do NOT store biometrics to maintain a lean DB. This apparently, isn't true. Once KYR and KYR+ data of the residents along with the Aadhaar numbers are available in SRDH, they can be shared with private entites for other purposes. SRDH's are apparently NOT covered in the Aadhaar Act. Odisha, TN and Haryana are some states that do maintain an SRDH.	https://medium.com/karana/the-360-degree-database-17a0f91e6a33	6/December/2017	Medium_AnandVenkatanarayanan_6December2017	This seems legit.
Yes	Preetha	How a SIM Card Operator in Hyderabad Apparently Created His Own Aadhaar Database	Anand Venkatanarayanan	Wire	SIM card provider apparently set up his own CIDR. This article makes a reference to the fingerprint moulds used in the UP hack attack. The only solution that UIDAI currently offers against identity takeover attempts using publicly available documents is what it calls "biometric locking", which requires a permanent phone number always attached to the Aadhaar number.	https://thewire.in/tech/Aadhaar-database-breach	2/July/2018	TheWire_AnandVenkatanarayanan_2July2018	Should discuss biometric locking
Duplicate	Dhruv	Aadhaar details of 7.82 crore from Telangana and Andhra found in possession of IT Grids (India) Pvt Ltd	Srinath Vudali	Times Of India	It was found that IT Grids (India) Pvt Ltd was in possession of 7,82,21,397 records of Aadhaar data (in a structure similar to that of CIDR) belonging to Telangana and Andhra Pradesh for the purpose of Seva Mitra App belonging to Telugu Desam Party. The app is suspected to be using stolen voters' information and Aadhaar data of the state governments of Telangana and AP for voter profiling, etc. The police says that the accused has illegally accessed the CIDR or the SRDH. A case was filed against IT Grids by UIDAI.	https://timesofindia.indiatimes.com/city/hyderabad/Aadhaar-details-of-7-82-crore-from-telangana-and-andhra-found-in-possession-of-it-grids-india-pvt-ltd/articleshow/68865938.cms	13/April/2019	TimesOfIndia_SrinathVudali_13April2019	Does UIDAI filing a case imply a real breach? Why else would UIDAI file a case? At the same time, our analysis suggests that there is no way to access CIDR at all. Did the accused find a tech loophole in the system?
No	Preetha	Indane leaked millions of Aadhaar numbers: French security researcher	IANS	Economic Times	Elliot found out data from 11000 dealers Due to a lack of authentication in the local dealers portal of Indane.	https://economictimes.indiatimes.com/news/politics-and-nation/indane-leaked-millions-of-Aadhaar-numbers-french-security-researcher/articleshow/68058639.cms	19/February/2019	EconomicTimes_IANS_19February2019	Do we know enough about the technical DB to know if Indane's system had a flaw? Moreover is it Aadhaar's fault if Indane's system was the reason the leak happened in the first place? Is UIDAI obligated to set certain guidelines for outsourcing data with its partners?
Yes	Preetha	Aadhaar data: French hacker exposes flaws in its Android app, asks people not to use it	-	Business Today		https://www.businesstoday.in/current/economy-politics/data-breach-french-hacker-exposes-flaws-Aadhaar-deadline-android-app-do-not-to-use-it/story/272626.html	15/March/2018	BusinessToday_-_15March2019	
Yes	Preetha	UIDAI CEO Gave The Supreme Court His Aadhaar Logs, Now Twitter Knows Everything About Him	-	Huffington Post	Anand Venkatanarayanan was able to track Pandey(CEO of UIDAI)'s movements, wrt his bank transactions and OTP linkages with just his Aadhaar number. Article does not however, go in depth.	https://www.huffingtonpost.in/2018/03/29/uidai-ceo-gave-the-supreme-court-his-Aadhaar-logs-now-twitter-knows-everything-about-him_a_23398180/	29/March/2019	HuffingtonPost_-_29March2018	Need to follow up.
Yes	Vineet	Scroll Investigation: How your Voter ID was linked to Aadhaar without your knowledge or consent	Abhishek Dey	Scroll	Election Commision of India used dubious methods to link citizen's voter cards to their Aadhaar Cards. Such acts are deemed unconstituitional after the SC struck this practice down in response to a PIL. This led to many names being deleted in the electoral roll if the name did not tally with the Aadhaar Registry.	https://scroll.in/article/914123/scroll-investigation-you-may-not-even-know-how-your-voter-id-was-linked-to-Aadhaar	Feb/26/2019	Scroll_AbhishekDey_29Februrary2019	Does not explain how the names got deleted. Little shady with the causality.
Yes	Preetha	SBI alleges Aadhaar data breach; UIDAI says database fully secure	-	Times Of India	State Bank of India (SBI) officials have expressed concern over breach of Aadhaar data, alleging that logins and biometrics of their Aadhaar operators have been misused to generate fake Aadhaar cards.	https://www.timesnownews.com/business-economy/economy/article/sbi-alleges-Aadhaar-data-breach-uidai-says-database-fully-secure/355877	Jan/29/2019	TimesOfIndia_-_29January2019	
Duplicate	Vineet	Aadhaar details of enrolment operator stolen and misused, show UIDAI records: Report	Scroll Staff	Scroll	The biometrics of an Aadhaar operator were being misused to get false entries pushed to the CIDR. UIDAI does not know how someone is using digital copies to login into the enrolment client. The operator was fined.	https://scroll.in/latest/913978/Aadhaar-details-of-enrolment-operator-stolen-and-misused-show-uidai-records-report	20/Feb/2019	Scroll_Staff_20Feb2019	Basic attack. Social engineering attack. How does one stop this?
Duplicate	Preetha	Fingerprints, Aadhaar and Law Enforcement – A Deadly Cocktail Is in the Making	Rachna Khaira	Huffington Post	A software patch allows unauthorised persons, based anywhere in the world, to generate Aadhaar numbers at will, and is still in widespread use for as little as 2500. The patch was assembled by grafting code from older versions of the Aadhaar enrolment software—which had fewer security features— on to newer versions of the software. UIDAI did not respond to HuffPost's mails	https://www.huffingtonpost.in/2018/09/11/uidai-s-Aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472/	11/September/2018	HuffingtonPost_RachnaKhaira_11September2018	This article talks big based on a presumed "patch". We do not know what the patch looks like or what it does.
Yes	Preetha	About 500 missing children traced through Aadhaar: UIDAI	PTI	Live Mint	There are children being traced thanks to their Aadhaar numbers according to CRY. But how?	https://www.livemint.com/Politics/6oJjtwMdUn4I9Axn5y9sjO/About-500-missing-children-traced-through-Aadhaar-UIDAI.html	24/November/2017		But how? Discuss how it is possible for an external agency to get the childrens' Aadhaar numbers
Yes	Preetha	Cracked Aadhaar enrollment and updation software for sale on the black market: Report	Vidyut Kale	Media Nama	Aadhaar enrollment operators use a software provided by the UIDAI, called ECMP (Enrollment Client Multi Platform), to collect or update an individuals information in the Aadhaar database.	https://www.medianama.com/2018/05/223-cracked-Aadhaar-enrollment-and-updation-software/	1/May/2018		The article does not go into details of how such a software could be accessed and made copies of
Yes	Preetha	How trustworthy are the entries in the Aadhaar Database?	Anand Venkatanarayanan	Media Nama	Talks about several possible bribing methodologies. Could be interesting to discuss for our security breach table.	https://www.medianama.com/2017/09/223-how-safe-is-the-Aadhaar-database/	28/September/2017		
Yes	Preetha	Fake documents, forged gazetted letters used to enrol for Aadhaar	-	The New Indian Express	There are two potential methods possible. While one method involved presenting forged gazetted letters as identity proof, the other helped people enrol using fake documents. In a separate case of vishing scam involving Aadhaar, a person was duped of `39,000 after the victim was asked to provide his Aadhaar number and ATM number to seed Aadhaar to his bank account.	http://www.newindianexpress.com/states/karnataka/2017/dec/16/fake-documents-forged-gazetted-letters-used-to-enrol-for-Aadhaar-1728704.html	16/December/2017		Discuss if forged document submission is still possible for Aadhaar generation. What is the work around?
Yes	Preetha	Aadhaar's Dirty Secret Is Out, Anyone Can Be Added as a Data Admin	Meghnad Bose	Quint	The Quint found that completely random people like you and me, with no official credentials, can access and become admins of the official Aadhaar database (with names, mobile numbers, addresses of every Indian linked to the UIDAI scheme). But that's not even the worst part. Once you are an admin, you can make ANYONE YOU CHOOSE an admin of the portal.	https://www.thequint.com/news/india/exclusive-Aadhaar-dirty-secret-out-add-anyone-as-data-admin	4/January/2018		Looks like a bunch of clickbait tbh. I dont think this is very feasible. Must discuss
Yes	Preetha	Pak National with Aadhaar Card Arrested from Jaisalmer Air Base	-	Quint	Pakistani dude had Aadhaar card. Does not discuss how he got it	https://www.thequint.com/news/india/pakistani-national-with-Aadhaar-card-arrested	4/January/2018		Article doesn't state how the fake Aadhaar card was made.
Yes	Preetha	This Uzbek National Was Arrested Last Year With An Aadhaar Card Believed To Be Forged. It's Still Valid On The UIDAI Website	Gopal Sathe	Huffington Post	The Bhubaneshwar police told Odisha local news site Ommcom that the Aadhaar was likely forged. However, HuffPost checked the Aadhaar number on the UIDAI website, where it was verified as belonging to a woman between 20-30 years, from Delhi, with a phone number ending in the same last three digits as the one that the Bhubaneshwar police found with Asalina.	https://www.huffingtonpost.in/2018/07/10/this-uzbek-national-was-arrested-last-year-with-an-Aadhaar-card-believed-to-be-forged-its-still-valid-on-the-uidai-website_a_23478403/?utm_hp_ref=in-Aadhaar-card	10/July/2018		Does not say HOW the forged Aadhaar card was made. So it's being done but we do not know how.
Yes	Preetha	Aadhaar Card Issued to a Dog, Owner Arrested	-	Outlook	Tommy Singh.	https://www.outlookindia.com/newswire/story/Aadhaar-card-issued-to-a-dog-owner-arrested/905109	3/July/2015		Can't happen anymore can it? What changed? Further investigation in to the enrollment agency is needed
Yes	Preetha	Aadhaar card tampering racket busted in Surat	Yagnesh Bharat Mehta	Times Of India	The accused Hiren Prajapati, 26 and Prashant Pradhan, 20, were accused of cheating biometrics using arubber thumb.	https://timesofindia.indiatimes.com/city/surat/Aadhaar-card-tampering-racket-busted/articleshow/62781626.cms	5/February/2018		Similar case to Swagam's thing. Basically biometric fudging seems like a repeated bust against Aadhaar
Yes	Preetha	In Two Villages In UP And Rajasthan, Aadhaar Cards Have A Story To Tell: Almost Everyone's Born On The Same Day	Adrija Bose	Huffington Post	A lot of people got birthdays on the same day owing to technical goofup. More likely an enrolling agent got lazy	https://www.huffingtonpost.in/2017/05/24/in-two-villages-in-up-and-rajasthean-Aadhaar-cards-have-a-story_a_22106535/?utm_hp_ref=in-Aadhaar-card	24/May/2017		Quite possible. This one's on the enrolling agent.

Article Title	Attack Name/S.No.	Is the alleged attack a breach of Confidentiality?	Is the alleged attack a breach of Integrity?	Is the alleged attack a breach of Availability?	Is the alleged attack legitimate given what we know about the UIDAI infrastracuture? (Yes, No, Unsure)	Reason	Comments
An IIT graduate has been arrested for illegally accessing the Aadhaar database: Report	An IIT graduate has been arrested for illegally accessing the Aadhaar database: Report	Yes	No	No	Yes	UIDAI took action against this attack, which suggests that it is legitimate. However due to lack of information in the article about how this attack was carried out, we cannot rate on the basis of our understanding of the Aadhaar system.	
UIDAI reveals 210 govt websites made Aadhaar details public, did not specify when breach took place	UIDAI reveals 210 govt websites made Aadhaar details public, did not specify when breach took place	Yes	No	No	Yes	We know that this is a legitimate attack since the UIDAI has confirmed this breach of data confidentiality through an RTI (Right to Information) request. It is important to note that the UIDAI itself did not leak this data. It was posted on the websites of over 200 central government, state government and educational instututes. It is still unclear as to how they had accessed the Aadhaar data.	
Three Gujarat websites including government portal made Aadhaar details public	Three Gujarat websites including government portal made Aadhaar details public	Yes	No	No	Yes	The Ministry of Electronics and Information Technology confirmed the attack. Even though this is not an attack on UIDAI, this would not have happened had Aadhaar not existed.	
In Two Villages In UP And Rajasthan, Aadhaar Cards Have A Story To Tell: Almost Everyone's Born On The Same Day	In Two Villages In UP And Rajasthan, Aadhaar Cards Have A Story To Tell: Almost Everyone's Born On The Same Day	No	Yes	No	Yes	Human error in a large-scale and multistakeholder system is definitely possible. In this case, the enrollment officer did not fill in the details correctly for some people who had submitted their date of birth documents.	
This Uzbek National Was Arrested Last Year With An Aadhaar Card Believed To Be Forged. It's Still Valid On The UIDAI Website	This Uzbek National Was Arrested Last Year With An Aadhaar Card Believed To Be Forged. It's Still Valid On The UIDAI Website	No	Yes	No	Yes	The Aadhaar card is meant for citizens and residents. This can be considered as an attack if the documents given during enrollment are fake/forged. That information has not been provided in the article.	The Act further defines residency as, "An individual who has resided in India for a period or periods amounting in all to 182 days or more in the 12 months immediately preceding the date of application for enrolment."
Pak National with Aadhaar Card Arrested from Jaisalmer Air Base	Pak National with Aadhaar Card Arrested from Jaisalmer Air Base	No	Yes	No	Unsure	Same as above. In addition, we don't know if this Aadhaar card was valid on the UIDAI website. For all we know, this could be a Photoshopped copy of this Aadhaar.	Same as above
Fake documents, forged gazetted letters used to enrol for Aadhaar	Fake documents, forged gazetted letters used to enrol for Aadhaar	No	Yes	No	Yes	There is a possibility of human error or laziness that can seep in resulting in people with fake documents being enrolled in the Aadhaar system.	
SBI alleges Aadhaar data breach; UIDAI says database fully secure	SBI alleges Aadhaar data breach; UIDAI says database fully secure	No		No	Yes	Both UIDAI and SBI agreed to the fact that "multiple station IDs" that were attributed to one enrollment operator. This itself can allow for the creation of multiple fake Aadhaar enrollments.	
UIDAI Blacklists Centre That Leaked Aadhaar Details of M S Dhoni for 10 Years	Leak of MSD's Aadhaar Data	Yes	No	No	Yes	Human error with regards to the enrollment officer/agency	
Rs 500, 10 minutes, and you have access to billion Aadhaar details	Illegal access to the data	Yes	No	No	Yes	UIDAI sued The Tribune for exposing this attack and getting access to this leaked data. This suggests that it is a real attack on the database.	
WikiLeaks hints at CIA access to Aadhaar data, officials deny	CIA having all Aadhaar biometric information	Yes	No	No	No	If the biometric hardware has no way of communicating over the internet (which is the case), it's not likely that the Aadhaar software will send the information over to the CIA.	
Indane Leaked Millions of Aadhaar Numbers, Claims French Researcher	Same as the title	Yes	No	No	Yes	Same as above	
Fake Aadhaar card network busted in Kanpur	Hackers bypassed the fingerprint biometric system by successfully copying legitimate fingerprints.	No	Yes	No	Yes	Tampering of the source code is possible with physical access to an enrolment client and an operator's fingerprints.	
Aadhaar Operator's Biometrics Stolen & Misused, UIDAI Documents Prove	Hackers got the biometric of an Aadhaar enrollment agent.	No	Yes	No	Yes	Same as above. In addition, the accused are not selling a tampered version of the source code to others.	
Big data breach! Aadhaar software hack raises major security concerns	A software patch, which can be bought for as little as Rs. 2,500 - reportedly allows unauthorised persons, based anywhere in the world, to generate Aadhaar numbers.	No	Yes	No	Unsure	It is unlikely that the iris scanner can be fooled with a photograph of a registered operator. If at all this is possible, it would require a photograph of an operator in a very specific pose, which would be difficult to obtain.	
How a SIM Card Operator in Hyderabad Apparently Created His Own Aadhaar Database	Property papers which have all the Aadhaar relevent information can be acquired for extremely low rates by anyone and used to check the Aadhaar database.	Yes	No	No	Yes	He got the information from other sources but the Aadhaar infrastructure should be strong enough to not accept biometrics that are not live.	
Aadhaar data: French hacker exposes flaws in its Android app, asks people not to use it	Aadhaar data of a person can be seen if one has physical access to someone's device. There is a certain level of tech expertise required to access this information.	Yes	No	No	Yes	The video shows how this is possible.	
Cracked Aadhaar enrollment and updation software for sale on the black market: Report	Aadhaar data of enrolement agents like biometrics is bypassed along with their geolocation to mimic their behaviour in order to produce fake Aadhaar data.	No	Yes	No	Unsure	It is unlikely that the iris scanner can be fooled with a photograph of a registered operator. If at all this is possible, it would require a photograph of an operator in a very specific pose, which would be difficult to obtain.	
Aadhaar's Dirty Secret Is Out, Anyone Can Be Added as a Data Admin	Any admin can add someone else as an admin who has the right to see any information as stored in the Aadhaar database. This new admin then has the right to do the same.	Yes	Yes	Yes	Yes	Access to Aadhaar details after enrollment or updation requires acccess to the CIDR. Therefore, this alleged breach points to an insider attack. In their review, Agarwal et. al. emphasised the Inadequate protection against insider attacks on CIDR data. Thus making this attack a possibility.	
Aadhaar card tampering racket busted in Surat	Someone got Aadhaar login details of an enrolment operator along with their finger print. They then sold it to two people who used those login details to update Aadhaar details and charged money for it.	Yes	Yes	No	Yes	Since the enrollment officer is the focal point of information entry/updation, it is possible for this alleged attack to take place if the login details (incuding fingerprint) of the officer is forged	
Aadhaar Card Issued to a Dog, Owner Arrested	A dog was issued an Aadhaar number by an enrolment agency supervisor.	No	Yes	No	No	This attack needs multiple breaches to be performed: faking fingerprints, failed de-duplication, human error (negligence). This seems to be like just an Aadhaar on which someone has Photoshopped a dog's face.	
Aadhaar biometric data breach triggers privacy concerns	Aadhaar biometric data breach triggers privacy concerns				No		Privacy
UIDAI suspends eKYC licence of Bharti Airtel, Airtel Payments Bank over violation of Aadhaar Act	Illegal opening of bank account				No		Privacy
Fingerprints, Aadhaar and Law Enforcement – A Deadly Cocktail Is in the Making	Police has partial Aadhaar access for biometric scans of criminals	Yes	No	No	Unsure	Access to the Aadhaar database, apart from the necessary UIDAI authorities must be gotten only for special cases through a judicial process. If this is met, then this should not be considered an attack. The Srikrishna draft mentions these cases but since it has not been passed yet, we cannot be sure whether to term this as a legitimate attack.	Privacy
Aadhaar Privacy Issues Extend Beyond the Security of Its Biometric Database	Cyber Cafes in particular being allowd to gather Aadhaar information and store it in their 'secure' database for an year is a clear breach of privacy/	Yes	No	No	No		Privacy
UIDAI CEO Gave The Supreme Court His Aadhaar Logs, Now Twitter Knows Everything About Him	The CEO (unintentionally) proves that Aadhaar is actively keeping track of any authentication done by any AUA, internal or otherwise.	No	No	No	Yes	This attack shows that, although "CIA" is not breached, questions can still be raised about the very concept of Aadhaar in providing the government a way to track the activities of the citizens of India.	Privacy
Scroll Investigation: How your Voter ID was linked to Aadhaar without your knowledge or consent	This is not an attack on Aadhaar. The Election Commission linked some voter ID cards to Aadhaar numbers but that does nothing to anyone.	No	No	No	No	Aadhaar numbers were retrieved by the Election Commission from people who were enrolling for Aadhaar.	Privacy
About 500 missing children traced through Aadhaar: UIDAI	This is not an attack on Aadhaar, but it does suggest that Aadhaar is tracking us	Yes	Yes	No	No		Privacy
UIDAI: Police suspicion that Aadhaar data stolen was unfounded	The government has information of all people in Telangana	Yes	No	No	No	The company had stored aadhaar details of multiple residents. Although we do not know whether this data has come from the UIDAI's CIDR or not, it is safe to say that access to these multiple aadhaar details should be considered as an attack.	Privacy
TOTAL		10	8	1	16		

Attack Name	Threat Actor	Cost (Time and Resources) - Low, Medium, High	Level of Safeguard by UIDAI infra. against this attack	Feasibility (ease of repeating by the threat actor given cost and safeguard)	Comments	Mitigation Strategy	Bucket Kind/Attack Type		
An IIT graduate has been arrested for illegally accessing the Aadhaar database: Report	Technical Expert	Medium	Low	Medium	The cost is medium because not everyone can perform the attack while it doesn't require an emmense amount of resources. The Level of feasibility is Low because UIDAI didn't ensure that its partner had the data in a secure structure. Leading to many possible vulnerabilities in future systems.	Enforcing strict security standards for UIDAI partner institutions. If these organisations store Aadhaar data, it must be done so after encryption and with approriate security measures.	Server Hacking		Server Hacking = Hacking UIDAI partne org. storage
UIDAI reveals 210 govt websites made Aadhaar details public, did not specify when breach took place	Unsure	Unsure	Unsure	Unsure	Unsure about the metrics since the appropriate information was not made public.	Unsure	Infrastrcture Loophole		Infrastructural Loophole = Going through estabilished UIDAI channels to access private information.
In Two Villages In UP And Rajasthan, Aadhaar Cards Have A Story To Tell: Almost Everyone's Born On The Same Day	Enrolment Agent	Low	Low	Medium	The level of safeguard is low since is little scope to rule out attacks (or, mistakes) by enrollment officers in the current Aadhaar Architecture	Log data entered by the enroling officers, which are under random external audits so as to ensure, or minimise, the fear of human error. Have stricter measures for a registrar to be able to enrol citizens and accepting documents.	Infrastructure Loophole		Subpar Hardware = UIDAI approved hardware fooled by external entities into approving false biometrics.
SBI alleges Aadhaar data breach; UIDAI says database fully secure	Technical Expert	Medium	Medium	Low	The cost is medium since the threat actor would need access to an enrollment officers login and biometrics as well as be a technical expert. Level of safeguard is medium because UIDAI can detect this due to multiple IDs being created.		Server Hacking, Infrastructure Loophole		
Indane leaked millions of Aadhaar numbers: French security researcher	Technical Expert	Medium	Low	Medium	Same as attack 1	Same as attack 1	Server Hacking		
UIDAI Blacklists Centre That Leaked Aadhaar Details of M S Dhoni for 10 Years	Enrolemnt Agent	Low	Medium	High	The level of safeguard is medium since the contract of the agency has been cancelled and further investigation is underway to look for further fines.	Higher level of fines to disincentivize such errors.	Infrastructure Loophole		
Rs 500, 10 minutes, and you have access to billion Aadhaar details	Technical Experts or individual with access to login credentials or a high ranking official gone rogue	High	Low	Low	This attack requires login information of personnel high up in the heirarchy of UIDAI. Moreover, there needs to be access to the account of those who can assign more accounts that can see others' information.	The authentication to go into the system as a root (which it seems these people had) should only be allowed after mutiple changing real time authentications like OTP or iris scans.	Server Hack		
Fake Aadhaar card network busted in Kanpur	Technical Expert	Medium	Medium	Low	The cost is medium since the person needs access to the biometric information of an enrollment agent along with the technical expertise to be able to fool the GPS system	Better hardware should be used. The fingerprint scanner should be of better quality and iris scanner should be more often employed since it is harder to fool.	Infrastructural Loophole, Subpar Hardware		
Medium: The report suggests it costs around Rs.100 to perfrom the attack, however, it takes *significant time to retrieve and make digital signatures out of physical property documents*	Experts in Biometric hacking	Medium	Low	Medium	The attack was detected by UIDAI and was also dealt with. What could've been better would be to detect who actaully used this person's information.	Better biometric hardware and better security for Aadhaar operators so their accounts are secure.	Infrastructural Loophole, Subpar Hardware		
How a SIM Card Operator in Hyderabad Apparently Created His Own Aadhaar Database	Digitally Literate Citizen	Medium	Low	Medium	The cost is medium. The report suggests it costs around Rs.100 per aadhaar number to perfrom the attack, however it takes some effort to make a digital copy of physical signatures. The attack is fecilitated by Aadhaar but it is not an attack on Aadhaar. The fingerprint sensors need to be more sophisticated since basic moisture-sensing sensors have been circumvented in a similar way in the past as well (Apple). For a person who is not performing a targetted attack, the feasability is medium since it is relatively easy to collect this information from physical documents. However, that requires significant time and effort.	The digital scanners should be of a higher quality and preference should be given to iris scanners since iris scans are not commonly found or easily replicable.	Subpar Hardware		
Aadhaar data: French hacker exposes flaws in its Android app, asks people not to use it	A hacker; a tech-savvy person who can replicate the video in real life	Medium	None	Low	The cost is medium since the person should have physical access to the device, their password, and the phone should have the app and Aadhaar data. The level of safeguard is none since we are unsure whether UIDAI has fixed this issue. The feasibility is low since getting physical access to the phone and knowing their password is not very probable. In addition, if someone has this information, they have much more of a person's information available to them than just Aadhaar. This includes: their phone number, their emails, their location history (which includes their house location).	Make better apps. The feel of the app itself shows the quality of developers that have developed it.	Server Hack		
Fake documents, forged gazetted letters used to enrol for Aadhaar	People having personal contacts with Gazetted Officers.	Low	None	High	The cost is low since if the gazetted officer gives in, it is very easy to be inducted into the CIDR even if the person is illegitimate. The level of safeguard is none because they assume that a Gazetted Officer's signature on a document is legitimate. It is very feasible since this attack is based on conections with a Gazetted Officer, which is quite probable. It is important to note that this is not UIDAI's mistake but that Gazetted officer's mistake.	This document mentions that the verifier does not need to verify the document if a notary or gazetted officer has attested it. This rule may need to be changed to regain control over legitimacy of documents. https://www.uidai.gov.in/images/handbook_verifier_6122013.pdf	Infrastructure Loophole		
This Uzbek National Was Arrested Last Year With An Aadhaar Card Believed To Be Forged. It's Still Valid On The UIDAI Website	Foreign nationals wanting proof of Indian residentship	Low	Low	Medium	This is a legitimate attack only if fake documents proving residentship were provided during enrolment. The cost, level of safeguard and feasibility is according to this assumption.	Ensure multiple document verification checks during enrolment. Documents of residentship cannot be taken at face value.	Infrastructure Loophole		
Aadhaar card tampering racket busted in Surat	Anyone with access to an enrolment officer	Medium	High	Medium	The cost is medium since it requires the operators login details and a ruber stamp impression of their biometrics. The level of safeguard is high since the location of each enrolment officer is tracked for each enrolment that is made. If teo enrolments are made simultaneously from two different places, then it will be flagged.	Regular changing of login details of enrolment operators and harsh punishments if they are found to give out their data. Better quality biometric hardware that cannot be fooled by rubber stamps, at least for the enrolment operators.	Infrastructure Loophole, Subpar Hardware		
Three Gujarat websites including government portal made Aadhaar details public	Anyone with access to these websites	Low	Low	High	This is as issue caused due to the lack of security of UIDAI's partner organisation (the Gujarat websites in this case). Since Aadhaar information was made public, anyone with access to the internet and to these sites could potentially view and store them for malicious purposes.	The UIDAI should ensure that its agencies are keeping Aadhaar details more secure. Essentially, they should not be stored in plain text and be only available to concerned parties. A citizen 'A' should not get access to the information of citizen 'B'.	Infrastructural Loophole		
UIDAI: Police suspicion that Aadhaar data stolen was unfounded	Third Party Organisation	Low	Medium	Medium	The safeguard is medium since UIDAI has the ability to know when and where its partner organisations are using this data. Feasability is low since these partner organisations risk a lawsuit with UIDAI if caught.	There should be stricter rules on the use of this data. Just having the data shouldn't mean it can be used for purposes other than the ones agreed with UIDAI. Significant punitive measures should disincentivize the misuse of this data.	Infrastructural Loophole		
Aadhaar’s Dirty Secret Is Out, Anyone Can Be Added as a Data Admin	Insider Attack (Administrator)	Low	Low	Low	We do not know who exactly is an admin of this system and what is the official procedure in the background to make someone else an admin.	The process of making an admin could be decentralised and be based on majority votes to ensure one agent cannot compromise it.	Infrastructural Loophole		

Privacy Breach Name	Threat Actor	Reason	Breach Type	Mitigation Strategies
Aadhaar biometric data breach triggers privacy concerns	Authentication Agent/UIDAIs Partner organisation	The identity of a resident was derived using an illegal copy of the Aadhaar database that was stored by the partner organisation. Since the identity of the resident was compromised and misused (through multiple illegal authentication requests), we consider this a privacy breach.	Illegal Storage	For this not to be a privacy breach, the partner organisation must not be able to hold or copy the data given during authentication unless UIDAI provides them with the same (with resident consent). Therefore, data captured by the biometric and input devices should be immediately encrypted such that partner organisations cannot identify any specific individual in the database. Alternatively, an One-Time-Password (OTP) should be sent to the registered number for each authentication request.
UIDAI suspends eKYC licence of Bharti Airtel, Airtel Payments Bank over violation of Aadhaar Act	Authentication Agent/UIDAIs Partner organisation	The parnter organisation had identified individuals and created new bank accounts for the same without informed and explicit consent. Similar to above.	Illegal Storage	Same as above.
Fingerprints, Aadhaar and Law Enforcement – A Deadly Cocktail Is in the Making	Centre/State Government Agencies	The National Crime Records Bureau (NCRB) was seeking permission for limited access to biometrics in the aadhaar database to investigate crime and trace unidentified bodies. Although these are genuine use cases, there is a threat of state surveilence that can be used to identify and trace any resident who's information is in the system.	Database Access	For aggregated analysis, differential privacy algorithms should be used. In cases wherin it is imperitive to identify the person there should be a legal procedure even if the requesting entity is a high ranking official. Structural measures should be maintained to prevent the tracing of these individuals even after the police has used the information for the purpose requested. This is a case of serveillance and cannot/shouldn't come under the purview of UIDAI themselves.
UIDAI CEO Gave The Supreme Court His Aadhaar Logs, Now Twitter Knows Everything About Him	Internal Agent	UIDAI requires AUAs to store authentication logs for over two years which can be extended to five years if needed. A high ranking official in the UIDAI can get access to this information, which they did.	Log Access	To get access to Authentication data, there should be a legal procedure even if the requesting entity is a high ranking official. This is a case of serveillance and cannot/shouldn't come under the purview of UIDAI themselves.
The National Electoral Roll Purification and Authentication Programme aimed to use Aadhaar linking to remove duplicate names from voter lists. The linking of these two IDs could lead to linkage attacks that threaten individual privacy.	Centre/State Government Agencies	The parnter organisation had identified individuals and linked their voter and Aadhaar IDs for the same without informed and explicit consent. Similar to breach 4.	Database Access	Same as Breach 4
Three Gujarat websites including government portal made Aadhaar details public	UIDAI Partner organisation	The organisation did not encrypt the data while storing, which could lead to the identification of individuals in the publicly accessible database.	Database Access	Higher penalty for storing Aadhaar information in plaintext so as to disincentivize these actions. Random audits should done by UIDAI and external agencies.
How a SIM Card Operator in Hyderabad Apparently Created His Own Aadhaar Database	Digitally Literate Citizen	By creating his own database using information from physical records, he was able to identify individuals and create SIM cards in their name through Aadhaar verification.	Physical Records	Aadhaar numbers shouldn't be mentioned on physical records.
UIDAI Blacklists Centre That Leaked Aadhaar Details of M S Dhoni for 10 Years	Enrollment Agency	One instance of the database was made public with the identity of the individual.	Physical Records	This can be attributed to human error. Awareness on privacy and digital identity can help mitigate this.
About 500 missing children traced through Aadhaar: UIDAI	Centre/State Government Agencies	This is definitely a positive use case for Aadhaar, but it poses the risk of state surveilence.	Database Access	This will always be a privacy breach since the purpose is to identify the individual.
UIDAI: Police suspicion that Aadhaar data stolen was unfounded	Third Party Organisation	The organisation had illegally stored Aadhaar information that can be used to identify an individual in the database.	Illegal Storage	The agency got this information through some UIDAI partner organization. The organization should not be allowed to dilvuge any Aadhaar information without proper authentication.