# Analytical study of Privacy and Security ways of Aadhar

Mugdha Patil

*A Student from Podar World College, BA Hons. in business Management, Mumbai, India*

**ABSTRACT**

*This study examines the role Aadhar plays in the lives of the recipients while investigating the privacy and security issues the system entails. This paper will take into account an analysis of the Aadhar system and its various privacy and security requirements. The Author will consider the ongoing debate about the privacy of biometric data and un-granted access to Aadhar data to provide with appropriate recommendations and possible solutions. The study also works around the issue of authentications and verification without consent and other cracks in the Aadhar Project with the assistance of risk assessment. In doing so the Author has made use of SWOT and model development to reach a satisfactory conclusion. These type of analysis has assisted the Author to identify the issue with the original Aadhar model and address them by suggesting the adoption of few modern techniques from the technical point of view and a change in system framework in the modern digital setting. This study also attempts to identify various gaps in the system and recommend a plan of action and process change that can be appointed to enhance the success rate of the project. As the report revolves around the privacy and security of Aadhar, issues like UIDAI and central repository are broken into its constituent parts to understand how they interrelate to one another. Issues such as legal framework, human error in the system and poor model structure are elaborated and explored to examine different ways in which the legal and privacy framework can be constructed. The study lastly has conducted a systematic review of reports, articles, newspapers and government reports relating to Aadhar to understand means of evasion and various consequences inadequate privacy has on the citizens of India.*

**Keyword**- *Privacy, security, SWOT, recommendation, identification, verification*

## 1. Introduction

The Aadhaar project is arguably the world's largest biometric identification system, and from a beginning, the system was designed to do good. Aadhaar, as described by (Shinde, 2018) was designed to cut out the middleman, eradicate corruption and to ensure the subsidized goods and services were reaching the deserving recipients.

Soon, the cracks in the project started to appear. The Aadhaar database started showing some serious security holes, and it's been draining data steadily for a long time now. The project's large-scale collection of data raises multiple questions related to whether the government is capable of safeguarding the massive amounts of data that is collected. In this extract, the Author has explained various possible measures that can be adopted by the UIDAI who is responsible for issuing of Aadhar numbers and maintaining their biometric and demographic data in a Central Identities Data Repository (CIDR).

### 1.1 Background

Aadhaar has perhaps been the most ambitious digital identity project and the world's largest biometric identification system in history. The project was designed to do good, however is now turning into somewhat of a large scale nightmare, creating a situation where the state can easily infringe upon its citizen's right to privacy. The Indian government, in May, publicly made known that it will be compulsory for residents to add their Aadhaar details to their accounts and in failing to do so will give the banks power to invalidate them. Additionally, transactions of 50,000 Rupees and above will also need individuals to be authenticated and verified with an Aadhaar card.

Everything from your bank accounts, private micro-payment systems, airline, and telecom companies, and more are demanding an Aadhaar card to ascertain the resident's identity. With raised demands for Aadhaar authentication will

come to the risk of abuse. Like, the recent alleged Reliance Jio data hack, when a recent report by (D'Mello, 2018) claimed that sensitive details, like mobile and Aadhaar numbers, of millions of subscribers, were leaked online.

What started as a unique identification number to streamline the distribution of welfare to the needy has now turned into a project that can arm the government with sensitive data of all the Indian residents. The heart of this issue is the quantity of data that is being accumulated as a part of the scheme and the many privacy and security concerns generated as a result of it.

The large-scale collection of data and the binding of said data with almost all services raises a fitting question: Is the government capable of safeguarding the massive amounts of data collected as part of the Aadhaar project?

The hotly debated topic of Aadhaar the privacy has struggled to make any progress, with proponents claiming that Aadhaar is safe while the opponents claiming, Aadhaar necessarily violates privacy. Any discussion involving Aadhar does not fail to precisely enumerate the possible ways in which privacy of the residents may be breached. Moreover, this enumeration is based on an in-depth analysis of policy, legal and data security considerations. Privacy breaches in a large setup like Aadhaar can happen through authentication and identification without consent. This can include illegal profiling by correlation of identities across different data silos and through illegal use of data stored in the central repository by the UIDAI. All other types of privacy compromises are segmented from or are special cases of the above. The responsibility should be on the designers of the system to convince its users that there are reasonable protections against these potential attacks.

**1.2 Role of UIDAI**

The Unique Identification Authority of India (UIDAI) according to (Role of Biometric Technology in Aadhaar Enrollment, 2018) is a statutory authority under the Ministry of Electronics and Information Technology and is responsible for the issuing of Aadhaar numbers. The UIDAI collects resident's demographic and biometric information to issue unique Aadhaar numbers. It provides an Aadhaar number to each resident and maintains their biometric and demographic data in a Central Identities Data Repository (CIDR). The UIDAI controls the central repository and provides identification and authentication services with yes/no answers.

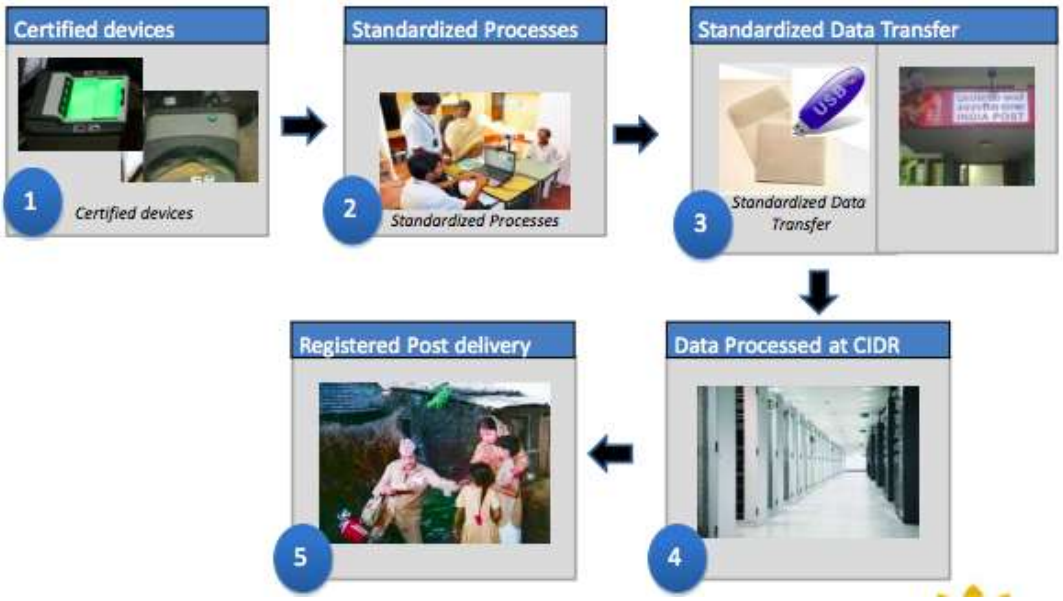


**Fig -1:** Aadhar Enrollment Process

As specified by (uidai.gov.in, 2016) the UIDAI conducts Aadhaar enrolment using a tiered model of Registrars and Enrolment Agencies. It enters into agreements with the Registrars. Registrars are entities which are recognized by the UIDAI for the purpose of enrolling the residents. Examples of Registrars are departments of the central or state government, banks, or public sector organizations.

Furthermore, as stated by (Agrawal, Banerjee and Sharma, n.d.), an Authentication User Agency (AUA) provides services to Aadhar card holders while connecting to the CIDR and uses Aadhaar authentication to validate the users and enables their services. In this federated model an AUA may choose to use only Aadhaar identification, or also authentication in conjunction with their own legacy identification and authentication systems. An AUA is required to enter into a formal contract with UIDAI to be able to use Aadhaar authentication services.

**1.3 Flawed Design**

Aadhaar system is based on a centralized database called the Central Identities Data Repository that stores every resident's demographic and biometric information in a centralized database. Additionally, supported by (Scroll.in, 2018), centralized databases are also vulnerable to errors and misuse by custodians of the database. The storage of resident's demographic and biometric information in one centralized database has made all the data vulnerable to exploitation, making it an attractive target for hackers and identity thieves.

In 2005, researchers came out with a report in the context of identity theft, the report also stated that it will be impossible to guarantee the security of such an expansive database. This in the long term will be proved as a problem as this database will be accessed millions of times daily and be involved in the exchange of a large amount of valuable information.

**1.4 SWOT Analysis**

Strengths: The unique identification numbers will take into account the database of the poor and the marginalized people, mostly living in the rural areas. The numbers will, for the first time, provide an identity to those who need it the most.

Weaknesses: The Aadhar project and UIDAI are unconstitutional as it is neither supported by any law nor it has any safeguards for protecting the civil liberties of citizens. To begin with, UIDAI said that UID number would be optional but now the government has made it mandatory. Additionally, the government has been suppressing public inputs, objections and suggestions, this has just been proving the points that Aadhar and UIDAI are most offensive tools of civil liberty violations in India.

Opportunities: The Aadhar project, running into thousands of crores, offers many opportunities for IT hardware as well as software companies that will run the system. The equipment at each enrolment centers costs about 3 lakh Rupees by multiply this by 350-400 is equal to what it costs for a single district. In effect, enrolment in a single district will cost between 10 crore Rupees and 12 crore Rupees. This does not include the cost borne by the State machinery in actually getting people to enroll, the logistics or the administrative expenses. The government can also increase their reach by the introduction of smart cards.

Threats: Aadhar card will enable every personal detail of individual to be available at any point. Hackers will now find it a lot easier to steal any personal information of any individual which may be used for any wrong purpose. Besides hacking, corruption in the government can also provide a potential incentive for an official to leak any kind of information from the database. Also, human error can limit the success of the project, with actually very few ways of eliminating human error.

## 2. Risk Identification

The information above probed the Author to further concentrate on four main risks Aadhar casts on its users. These risks have been explained below in detail while possible solutions have been recommended by the Author.

The Aadhar project collected the biometric and demographic data of 1036 million residents and strategized to store the data in a centralized database. This centralized database which is referred to as Central Identities Data Repository, due to its vast collection of personal information has made itself vulnerable to exploitation. Experts also believe that when it comes to the centralized database, the question is not whether it can be hacked but when. The flawed design has created vulnerability to identity fraud along with identity theft. Such a situation is a hub for hackers and will keep attracting more. When all the personal information is linked to the Aadhar, it is an open feast for hackers once inside the system. The system allows no mode, form of a barrier from attacks from an insider and little barrier from attacks from an outsider. In context of identity theft, according to (The Identity Project An

assessment of the UK Identity Cards Bill and its implications, 2018) it is impossible to guarantee the security of such a vast database. As a result, Aadhar database due to its size has given intrusion into the private lives of Indians. The unsafe and risky mass of database that connects fingerprints to their demographics and financial data has opened up its avenues to multiple illegal and unethical trading of identities.

Moreover, as Aadhaar data gets linked with various banking apps, credit cards, mobile connections, and other services, there are transactional data logs that are associated with authentication. Even when these logs are passive in nature by way of simple "yes/no" mode of authentication, these transactions nonetheless capture 'personal data' as they concern with one's day-to-day activity and behavior. So this transactional data that comprises of people's personal choices and consumption patterns need to be protected in addition to justifying the biometric Aadhaar data.

While Aadhar uses linkage that is 'one-way', it still cannot prevent intrusion on a person's privacy. When artificial intelligence casts a major threat to the privacy of this data, human link in this system can be equally as threatening. Criminals can still use man-in-the-middle attack strategy to insert themselves into the data transfer channels to either manipulate or extract data.

Another concern that pertains to privacy and security in Aadhaar is the blurred line between verification and authentication. Inability to understand the difference between the two is what leads to the identification of individuals without consent. Aadhar being a national identity project, Author believes that the subtle difference between identity verification and authentication is not well understood. This ignorance has led to confusions in policy making and deployment.

Besides, in February, as reported in (scroll.in, 2018) six employees of Reliance Jio (telecom service provider) were arrested for the deceptive use of fingerprints to activate and sell SIM cards. There were also reports by (medianama.com, 2017) about Axis Bank and other associations storing and using biometric data without authorization. Another report indicates that personal information, including Aadhaar numbers, can be obtained without any risk through a simple online search. In a time where Aadhaar is rapidly becoming a key for citizens to access every essential service, claims about poor security nudge the Government of India to promote further rigorous analysis.

Any robust identification mechanism can be able to prevent or provide an adequate remedy to the problem of identity theft. Identity theft occurs when an individual's identity is wrongfully used, without the individual's authorization or consent usually to commit crimes. In the case of Aadhaar, the design of the system entails and application are likely to make identity theft easier. Unfortunately, even the legal framework renders inadequate to address these issues.

A related concern that has been highlighted throughout the years is that even if the data is secure, with Aadhaar-enabled Payments System, the Aadhaar project has created vulnerability to identity fraud for the residents. The idea behind Aadhar-enabled Payment Systems as reported by (Khera, 2017) is, as Prime Minister Narendra Modi put it, "Your thumbprint is your bank". However, the major underlying issue is that fingerprint impressions can be easily reproduced. For instance, recently (Qazi, 2017) from Hindustan Times reported that 200 students in Mumbai replicated their fingerprints on a widely-used resin to fudge biometric attendance. These easily harvestable biometric traits and publicly-available Aadhaar numbers will increase the risk of banking fraud to a large extent. Also emerging financial technology infrastructure which is established on Aadhaar and biometrics, Aadhar project will further open its doors to identity theft.

It has been proven again and again that in the Indian environment, the failure to enroll with fingerprints is as high as 15 percent due to the prevalence of a huge population dependent on manual labor. These are essentially the poor and marginalized sections of the society. So, while the poor do indeed need identity proofs, Aadhaar is not the right way to do that. Keeping this is mind below are some recommendations and measures that can be taken to improve Aadhar as a tool for authentication a person's identity.

## 3. Recommendation

### 3.1 Human Error

Although all the data is stored in the repositories and maintained encrypted within the UIDAI, the decryption key to is stored within the same system. Even when the biometric data is not stored as it is received, criminals can still make use of a man-in-the-middle attack to obtain what is desired. Whilst discussing the welfare of digital data, technology makes a core part of the argument. However, the system is inclusive of human error, and its error margin makes it the weakest link in the chain. Thus, it is vital to take into account the human error and design a plan to control the possibility of this error.

For effective protection against the insider attack it is important to make sure that no manual inspection of data is possible. The existing system can introduce a completely independent third party inspection under different administrative control. These independent inspectors could play a part in online auditing and manual auditing. These auditors would be required to follow a strict policy framework to turn in a trustworthy report on underlying computing, network and storage infrastructure.

### 3.2 Legal Framework

The Author believes that the above recommendation will require careful analysis and rigorous evaluation; and that the technological, legal and policy frameworks will play an important part. Policy and legal frameworks will need to be greatly strengthened through discussions, taking into account different views and informed choices to evolve the current effective national security scheme.

The Government needs to make it possible to ensure those card holders are completely protected from manual inspection by the UIDAI or the Government or any other individual, thereby preventing unauthorized surveillance. The current Legal and Privacy protection does not demand that data should not be collected, stored or used by any non-government entities, but that there should be provable guarantees that the data cannot be used for any purpose other than those that have been approved. The legal framework, in turn, should be suitably enhanced with facilities to protect the privacy of individuals and society using an advanced information technology setting. Also, the legal framework is in demand for stricter legal actions and that the citizens should be made well aware of the consequences if the legalities are not followed correctly.

### 3.3 Model Recommendation

After identifying the gaps in the system the Author will now recommend a few changes and improvements that the UDAI and the government can bring in the system. These changes are outlined with the intent of addressing privacy and security challenges raised by the project. These recommendations include technological change, the introduction of new technology to complement the existing system, better political base or the introduction of a new system.

The model created by the Author can help directly or indirectly address these concerns. The model takes into account the terms of factors such as identity, authentication, service-level agreements and privacy. The model further incorporates how those factors are dealt with from a people, process and technology perspective.

The system will be presented as a lock while the key is broken into two parts. Anyone who wishes to unlock the system to access any personal information will need both the parts of the key. The first part of the key will include a password which will be kept with the cardholder. This password will be unique to every citizen and will be known to that person only. The second part of the key will be the chip the card will contain. This electronic chip will contain the user's biometric information of the fingers and the other sensitive information like residential address, bank account information, phone number after their Aadhar is linked to these services. The main goal of this model is to divert the system from being exceedingly dependable on easily replicable and harvestable information like biometrics and publicly-available Aadhar numbers. Where a finger print can be replicated, this system will be founded on passwords and pins that will be known to a particular resident. Passwords will further reduce banking frauds that are caused by easy harvesting of biometric traits as these verification codes will be known only to a distinct card holder.

The other part of the system is the AUA. The AUA to access any information of a citizen will require the card users to scan the chip which is present on the card and once successfully scanned, will need the user to enter their unique password. This method will take care of identity verification and authentication. Each resident will be able to

provide an identity proof using the card while authenticating oneself answering the question, 'proof of the claim of identity'. The Authentication processes using this system is a conscious process that will require active participation by every resident further reducing the risks of identity theft and unethical trading of identities.

The card will be synced with the UIDAI files. That is, in case of any transactions happening using the card will automatically get updated on the repositories. However, cannot be seen by any third party. Be the case of any unusual activity taking place using the card such as large amount being transferred to and from one's account the file manager will be notified. If the manager finds the activity suspicious, the citizen will be inquired about the transactions or any suspicious activity, and the resident will have to abide by the law.

Furthermore, the Unique Identification Authority of India (UIDAI) is responsible for providing the basic identification and authentication services. That is the UIDAI provides each resident with a unique identifier (Aadhaar number) and maintains their biometric and demographic data in a Central Identities Data Repository (CIDR). To reduce the risk of possible intervention of the third party, the biometric data of the residents will be stored in different repositories. Information that will get updated on the system will be stored on a different server according to the type of information fed into it. That is, the demographic attributes of a cardholder will be stored in a different repository while the biometric information (fingerprints and iris scans) will be stored in a different repository. Each repository will require a password to be accessed. As to gain access to personal information of any individual a verification code will be required, each resident can be in control of when, where and how his/her personal information is being used. This way each cardholder will be required to be physically present while his/her information is being accessed.

Originally, after the enrollment with the UIDAI, the residents can present the unique identification number to an AUA to avail Aadhar authentication services. However, with this system, each resident would have to pass through a series of steps adding layers and filtering out the risk of identities being stolen. And while a printout or a photocopy is a valid ID card, this would change the requirement due to the smart chip embedded in the card.

Overall, this model concentrates on four independent principles. One, it will enable the citizens to own their personal data, without the intervention and consent of a third party. Two, it keeps the data confidential. Three, there should be an adequate amount of contractual understanding among the Unique Identity Authority of India (UIDAI—which issues Aadhaar) as the hub and the public. And four, the hubs should possess sturdy end-to-end security, connectivity and access measures among the hub and spokes.

## 4. CONCLUSIONS

The Autor has analyzed the Aadhar system to produce findings that will possibly have positive implications on the existing processes the Aadhar follows. The study has taken into context various risks and cracks the system showcases and used them as guidelines to build suitable recommendations. These findings are categorized into three different parts. Each recommendation is designed to address the risks that have been identified in the study and are summarized in the table below.

| Issue | Recommendation |
|---|---|
| Human Error (Manual Inspection) | • Inspection under the administrative control<br>• No manual Inspection of data is possible<br>• Independent third-party inspection<br>• Online Auditing and Manual Auditing<br>• Following strict policy framework |
| Legal Framework | • Protected from manual inspection by the UIDAI or Government<br>• Preventing unauthorized surveillance<br>• Prevention of collection of data by non-government entities<br>• Enhancement of privacy framework Stricter policy framework<br>• Stricter legal actions |
| Poor system | • The Inclusion of pins and passwords for citizens<br>• Inclusion of electronic chip in Aadhar card |

| | |
|---|---|
| | • Diversion of the system from biometric data<br>• Scanning of the electronic chip during transactions<br>• Aadhar Card to be synced with UIDAI files<br>• Personal information to be stored in two different repository<br>• Repositories to require passwords to be accessed<br>• Filter out the risk of identities being stolen |

**Table-1:** Summary of Recommendations

In order for a single identifier to work across all domains, to include individuals of all working class to surrender their personal information will require multiple alterations. Recommendations such as conversion of current Aadhar card into a smart card may allow the users to use it across all domains. Secondly, a precise legal frame which takes into account the proper authentication and verifications processes and meticulous rules will further improve the success rate of the project. Also, inspection of human error and elimination may save the system from insider attacks.

One major drawback for India is that the Aadhaar is not a smart card. The introduction and production of such a card would be expensive, but the citizens will benefit much more than Aadhaar in its current form. With this, at least some discussions over biometric authentication would be put to an end, as a number of government services, can be stored in the smart card itself. A choice is another important factor here in the system. Lack of privacy with the current Aadhar system does not allow the citizens to be in power with their data. Citizens unable to choose when and what services to use for Aadhaar strips the user of the control and exposes them to more risk in terms of security and privacy.

However, only so much can be done to protect citizens from illegal access to their personal information. Perhaps the most important question that needs answering is who should have the right to verify an individual's identity and under what circumstances?

## 5. Bibliographies

Shinde, J. (2018). Trending stories on Indian Lifestyle, Culture, Relationships, Food, Travel, Entertainment, News & New Technology News. [online] indiatimes.com. Available at: https://www.indiatimes.com/technology/news/how-does-aadhaar-compare-with-other-id-systems-in-the-world-how-to-secure-its-leaky-database-276972.html [Accessed 17 Sep. 2018].

D'Mello, G. (2018). Trending stories on Indian Lifestyle, Culture, Relationships, Food, Travel, Entertainment, News & New Technology News. [online] indiatimes.com. Available at: https://www.indiatimes.com/technology/news/reliance-jio-says-it-s-not-hacked-aadhaar-data-not-leaked-but-online-users-insist-otherwise-325533.html [Accessed 17 Sep. 2018].

Role of Biometric Technology in Aadhaar Enrollment. (2018). [online] New Delhi, pp.7-15. Available at: http://www.dematerialisedid.com/PDFs/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf [Accessed 17 Sep. 2018].

Agrawal, S., Banerjee, S. and Sharma, S. (n.d.). Privacy and Security of Aadhaar: A Computer Science Perspective. [ebook] New Delhi. Available at: http://www.cse.iitd.ernet.in/~suban/reports/aadhaar.pdf [Accessed 17 Sep. 2018].

Scroll.in. (2018). Explainer: Aadhaar is vulnerable to identity theft because of its design and the way it is used. [online] Available at: https://scroll.in/article/833230/explainer-aadhaar-is-vulnerable-to-identity-theft-because-of-its-design-and-the-way-it-is-used [Accessed 18 Sep. 2018].

https://uidai.gov.in/images/the_aadhaar_act_2016.pdf (2016). THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016. New Delhi.

The Identity Project An assessment of the UK Identity Cards Bill and its implications. (2018). [online] The Department of Information Systems, the London School of Economics and Political Science. Available at: http://www.lse.ac.uk/management/research/identityproject/identityreport.pdf [Accessed 18 Sep. 2018].

Khera, R. (2017). The Different Ways in Which Aadhaar Infringes on Privacy. [online] The Wire. Available at: https://thewire.in/government/privacy-aadhaar-supreme-court [Accessed 18 Sep. 2018].

Qazi, M. (2017). You will be glued to this: Mumbai college's students trick biometric system. Hisdustan Times. [online] Available at: https://www.hindustantimes.com/mumbai-news/you-will-be-glued-to-this-mumbai-college-s-students-trick-biometric-system/story-W64f1jdMtecxKDml2DakeI.html [Accessed 18 Sep. 2018].

Author, G. (2017). Why UIDAI and Aadhaar will not be fixing basic issues in the system. [online] MediaNama. Available at: https://www.medianama.com/2017/03/223-aadhaar-basic-issues/ [Accessed 18 Sep. 2018].