CHAPTER 2: AADHAAR ARCHITECTURE
AADHAAR ARCHITECTURE
With more than 1.14 billion residents enrolled, Aadhaar is the world’s largest national digital identity platform. Aadhaar’s database and applications are supported by a complex ecosystem of processes and actors. Research can play an important role in strengthening Aadhaar’s technical and operational architecture.

An estimated 1.5 billion people around the world cannot prove their identity. Lack of formal identification can deny individuals access to entitlements such as social safety nets, voting rights, and basic financial products. An unidentified population also inhibits the state’s capacity for effective governance. Targeted design and delivery of government services rest on a state’s ability to identify (who are you?) and authenticate (are you who you say you are?) individuals. Private enterprise, too, relies on establishing identity for the provision of a range of services.

The goals of identity systems—to uniquely identify individuals and to do so efficiently—may be well served by emerging digital technologies. Digital identity platforms have the potential to increase coverage, accuracy, efficiency, and convenience relative to traditional paper-based methods. This potential has led nations across the world—from Germany to Ghana—to adopt digital identity as a key policy instrument. At the same time, digital identities also raise important concerns for individuals’ privacy and security.

India, too, has seen an evolution in identification systems. Paper-based forms of identification are gradually giving way to digital forms of identity. The most ubiquitous among these is Aadhaar—a digital biometric identity backed by a unique number. With more than one billion residents enrolled, Aadhaar is both the largest form of digital identity in India as well as the largest national digital identity project in the world. Aadhaar is increasingly shaping how individuals and institutions interact in modern India.

In this Chapter, we provide an overview of what Aadhaar is, how it has evolved, the processes and operating systems that enable its uses, and areas of research that are pivotal to the Aadhaar project. With this overview, we aim to fulfil two important functions. One, we provide a granular understanding of the operational aspects of Aadhaar enrolment, authentication, and payment systems. In doing so, we hope to enrich policy research and discussion of Aadhaar’s applications, data quality, and security. Two, we provide historical and operational insight into how the world’s largest digital identity database was created, and how it operates today. This aims to serve as an important background reading for researchers and practitioners involved with Aadhaar’s applications. In addition, this Chapter may benefit those researching or working to strengthen Aadhaar’s architecture, or those working on developing similar identity systems in other parts of the world.
What is Aadhaar?

Aadhaar means “foundation” in Sanskrit and other Indian languages. It is a unique biometric form of identification backed by a 12-digit random number. The Unique Identification Authority of India (UIDAI)—a statutory authority under the Ministry of Electronics and Information Technology—is responsible for issuing Aadhaar numbers.7 Every Indian resident8 is entitled to one. The UIDAI collects residents’ demographic and biometric information, and issues unique Aadhaar numbers in turn. There are currently more than 1.14 billion Indian residents in the Aadhaar database, far exceeding the enrolment numbers of other identity databases in India.9,10

Aadhaar is distinct from traditional identity systems such as voter identification and ration cards11 in two important ways: its utility across sectors and use-types, and its underlying technology enabling unique identification. First, it provides a cross-functional proof-of-identity and address, which is valid across states, sectors, and uses. While certain forms of identity such as the ration card are accepted as general proofs-of-identity in India, they were designed to perform a specific function—in this case, to identify individuals to receive a food subsidy. According to the UIDAI, an all-purpose identity proof has the potential to increase user convenience, lower transaction costs for service providers, and reduce the time spent in identity verification.12

Second, Aadhaar is designed to employ individuals’ biometrics, which are inherently unique.13 This aids in creating a database with almost no duplicates,14 and in accurately verifying identities. Most traditional identity platforms in India are paper-based and suffer from varying degrees of duplicate identities.15 Duplicates in identity databases can be misused to siphon resources from their intended uses.16 Additionally, paper-based identities are liable to theft and forgery, impeding the accurate authentication of individuals for service delivery. The UIDAI aims to use Aadhaar to plug these gaps.17

Evolution of Aadhaar

In the early 2000s, two distinct government identity projects were taking shape. In 2003, the Government of India was contemplating preparing a national register of Indian citizens, and issuing Multi-purpose National Identity Cards (MNICs) based on the registry.18 This project aimed at collecting a range of demographic and biometric information from individuals to provide a “credible identification system” that could streamline public and private service delivery.19

Between 2006-2008, the Registrar General of India (in charge of conducting the national census) was engaged in creating the National Population Register and issuing MNICs. Cards were issued to around 1.2 million citizens in about 12 districts.20

In parallel, the government approved a separate unique identity project for below-poverty-line families in 2006.21 A vision document was prepared, and a proposal was submitted to the erstwhile Planning Commission (reconstituted as NITI Aayog) for approval.

In recognition of the overlap between the two identification projects, the government constituted an Empowered Group of Ministers (EGoM) to combine the two.22 Subsequent to the decision of the EGoM, the UIDAI was constituted as the agency responsible for issuing Aadhaar numbers. The UIDAI was established by an executive order in 2009, and initially functioned as an attached office of the Planning Commission.23

Aadhaar enrolment began the next year, in 2010. Since then, it has increased steadily, with 85 percent of India’s population (roughly 1.14 billion of 1.3 billion individuals) enrolled.24 In Figure 2.1, we demonstrate the increase in cumulative enrolment in Aadhaar between 2011 and 2016.

As Aadhaar enrolment increased, the legal framework of the project underwent changes. Later in 2010, a few months after the first Aadhaar number was issued, the government introduced legislation to provide statutory backing to the Aadhaar project. The legislation was not passed by Parliament. In 2016, however, the
Enrolment ecosystem

The UIDAI conducts Aadhaar enrolment using a tiered model of Registrars and Enrolment Agencies.\textsuperscript{26,27} It enters into agreements with Registrars, which are entities recognised by the UIDAI for the purpose of enrolling residents. Registrars are commonly departments of the central or state government, banks, or public sector organisations. An example of a Registrar could be the Rural Development Department of a state government, or a public-sector insurance company such as the Life Insurance Corporation of India. Registrars carry out enrolment themselves, or appoint Enrolment Agencies to do so.

Enrolment Agencies may take two forms: third-party private entities empanelled by the UIDAI based on technical and financial capabilities, or existing offices of the Registrar. Enrolment Agencies receive payment from Registrars for successful Aadhaar generation. These agencies are required to use devices and follow technical processes delineated by the UIDAI. Enrolment Agencies set up Enrolment Centres, which function as touch-points for resident enrolment.

The UIDAI is also meant to partner with civil society organisations and community networks to broaden the reach of these enrolment touch-points and enable enrolment of marginalised populations.\textsuperscript{28} As of May 2017, according to the UIDAI, there were 113 Registrars and 482 Enrolment Agencies.\textsuperscript{29}

Enrolling residents

To enrol in the Aadhaar database, an individual must provide the demographic and biometric information detailed in Figure 2.2.

Of the requirements listed in Figure 2.2, name, gender, date of birth, and residential address are verified against existing documents. The UIDAI has published a list\textsuperscript{30} of acceptable proofs-of-identity, date of birth, and address. An individual’s biometrics (fingerprints,
iris scans, and photograph) are captured at the time of enrolment. In addition to the aforementioned mandatory demographic and biometric information, individuals can optionally provide their mobile telephone number and email ID.

There are avenues to enrol for individuals unable to provide proofs-of-identity. These include being vouched for by a head of family or an appointed “introducer” from one’s locality (both of whom must have an Aadhaar number and valid identity documents of their own). A UIDAI response to a Right to Information request from 2015 states that about 219,000 Aadhaar numbers were generated through the introducer facility. This suggests that about 0.02 percent of individuals enrolled as of 2015 did not possess either their own proofs-of-identity and address, or proofs belonging to a head of family, before Aadhaar enrolment.

Whether and how individuals may enrol if they are unable to provide the required demographic or biometric information, the enrolment procedure for children under five, and other enrolment details are presented in Appendix 2.1.

### Transfer of enrolment information to the Central Identities Data Repository (CIDR)

Upon enrolment, the personal information of residents must be sent to the CIDR in an encrypted form by the Enrolment Centre supervisor within 20 days. The most common method for transferring data is the Secure File Transfer Protocol (SFTP)—an international benchmark. If this option is unavailable, centre supervisors may send encrypted data to the CIDR on portable hard disks through carriers such as India Post.

### De-duplication and issuance of Aadhaar

The CIDR compares the incoming enrolment data of every individual with others enrolled in the Aadhaar database to identify and vet duplicates. This process, known as de-duplication, employs three steps. The goal is to identify genuine duplicates, while minimising false rejection of enrollees (incorrectly denying someone an Aadhaar number on the grounds that she or he is already enrolled).

1. **Demographic de-duplication** is used to identify “trivial duplicates” or cases of duplicates arising from error or ignorance. An example of such a duplicate, as per the UIDAI,
would be an individual who mistakenly re-submits enrolment data at a centre having already done so. Demographic de-duplication is also used for children under the age of five years, as biometric data is not captured for them (see Appendix 2.1 for the enrolment procedure for this age group). 27

2. **Biometric de-duplication** is the primary method of identifying duplicates. The UIDAI contracts with three vendors that provide automatic biometric identification systems (ABIS), which purportedly improve data accuracy. If one ABIS identifies a duplicate, it has to be verified by another ABIS, thereby increasing accuracy. Additionally, working with three vendors offers greater capacity for de-duplication and Aadhaar generation per day. Finally, the use of multiple vendors ensures that in case an individual vendor must be replaced, the system of de-duplication can continue.

3. **Manual adjudication** takes place if step two has resulted in identifying a duplicate. In this process, the duplicates are checked to assess if a process-related issue has led to the duplication (for example, mixing of enrolment operator and resident biometrics). Finally, each case is analysed manually and a human expert makes the final decision.

If a resident’s data clears the de-duplication process, a 12-digit Aadhaar number is generated.

The CIDR then issues a letter (commonly referred to as an “Aadhaar card”) with an individual’s Aadhaar number and demographic data and delivers it to the resident. Residents who have submitted their email address during enrolment may also download e-Aadhaar, which contains the same demographic information as an Aadhaar card. The e-Aadhaar also contains the date of Aadhaar generation and date of download, and is digitally signed by the UIDAI. The e-Aadhaar is equivalent to the printed Aadhaar letter delivered by the UIDAI. 28

If enrolment is unsuccessful, the resident and the enrolling Registrar are informed of the reason for rejection and steps to be taken post-rejection. 29

In Figure 2.3 below, we summarise the chain of events that must take place for an individual to receive an Aadhaar number from the UIDAI.

### Figure 2.3: Steps in Aadhaar enrolment from data capture to resident receiving Aadhaar 40

STAGE 1
Enrolment Agency captures residents’ demographic and biometric information

STAGE 2
Enrolment Agency transfers residents’ data to the Central Identities Data Repository (CIDR)

STAGE 3
De-duplication and generation of an Aadhaar number by the UIDAI

STAGE 4
Individual receives Aadhaar number and letter from the UIDAI

The UIDAI’s technical reports and publications provide a high level of detail on the regulations and protocol for each step in the Aadhaar enrolment process. However, we lack rigorous evidence on the execution quality of each step. Systematic analysis of the design and implementation of the various enrolment steps may be an area for future research.
Enrolment Data Quality and Security

The UIDAI has put in place certain measures to strengthen data quality and security at various steps of the enrolment process. Independent assessment of these measures, and research to further strengthen data quality and security, are important areas of future inquiry. These are discussed in the last section of this Chapter.

Data quality

The quality of the Aadhaar database can be assessed by analysing the accuracy of individual data contained within it, as well as the completeness of the database with respect to the target population (which, in the case of Aadhaar, is all Indian residents). Accuracy and completeness can be competing concerns. For example, tightening eligibility criteria for enrolment (such as by requiring pre-existing identity proofs) may increase the accuracy of enrollee data, at the cost of excluding entitled individuals.

The UIDAI constituted two committees in 2009 to review the nature and procedure of the biometric and demographic information to be captured during Aadhaar enrolment. Based on these committees’ recommendations, the UIDAI adopted measures to improve the accuracy and completeness of the Aadhaar database. These measures, and any associated evidence, are discussed below.

Accuracy

The accuracy of the Aadhaar database relates to two features: whether all individuals in the database are real and unique persons, and whether the personal information of such individuals is accurate.

Biometric de-duplication (the process of eliminating duplicates using individuals’ biometric data) is the main lever for achieving the first measure of accuracy. The UIDAI released performance data for the Aadhaar de-duplication process in 2012, when 84 million individuals had been enrolled. According to this data, the biometric false acceptance rate—the probability that the system erroneously accepts an individual as unique when in fact she or he is a duplicate—was pegged at 0.035 percent. This implies that about 99.97 percent of duplicates submitted to the biometric de-duplication system are correctly identified by the system.

Further, the UIDAI pegged the rate of duplicate submissions at 0.5 percent of all submissions. According to the UIDAI, the false acceptance rate (0.035 percent) combined with the rate of duplicate submissions (0.5 percent) implies that only a small number of duplicates would be falsely accepted at scale. The UIDAI further states that the false acceptance rate remains steady and does not increase with the size of the database.

While the 2012 data released by the UIDAI provides an important indication of the accuracy of the Aadhaar database, these figures would benefit from both updating and regular independent assessments.

A number of UIDAI regulations aim at achieving the second aspect of data accuracy: whether individuals’ personal information recorded in the database is accurate. Some measures are detailed below:

1. The UIDAI has outlined uniform provisions to be followed at every Enrolment Centre, to ensure data is collected consistently. These provisions include standardisation of enrolment devices, data formats, and software.

2. Quality control checks for biometric and demographic data, and consistency of biometric capture, are built into the Aadhaar enrolment software.

3. Enrolment Agencies receive feedback on data quality. According to the UIDAI, consistent feedback to Enrolment Agencies leads them to improve their training and enrolment processes. Enrolment Agencies are incentivised based on the number of successful Aadhaar numbers generated—and not the number of enrolments conducted—to encourage collection of high-quality data.

4. As noted above, individuals have to supply proofs-of-identity and address to verify their demographic information at the time of enrolment.
5. A provision exists for individuals to update their demographic and biometric information after enrolment. In addition, the UIDAI may require individuals to do so periodically. See Figure 2.4 for a discussion on updating resident information in the CIDR.

More empirical research on whether, and to what degree, these measures lead to increased accuracy of personal information in the Aadhaar database, compared with other identity databases, would be valuable. Such research might include assessment of how well these provisions are enforced. This can strengthen existing procedures for the UIDAI and guide other national governments looking to build digital identity systems.

Completeness
In addition to accuracy, another measure of data quality is the completeness of the database with respect to India’s population. While 85 percent of India’s population is enrolled, it is useful to examine variation by gender, age, and geography.

Gender: Just over half (52 percent) of total Aadhaar holders are male, which is in line with the country’s gender ratio.48

Age: The UIDAI data estimates that the adult population is almost fully enrolled and 72 percent of children aged 5 to 18 are enrolled. Less than one-third (31 percent) of children below five are enrolled.49

Geography: Twenty-four (of thirty-six) Indian states and Union Territories have 90 percent or more of their populations enrolled in Aadhaar. The three states with the lowest enrolment are Assam (7 percent), Meghalaya (9 percent), and Nagaland (55 percent), all situated in India’s north-east region.50 In Figure 2.5 below, we show Aadhaar enrolment by state and Union Territory.
The UIDAI has taken certain measures to reduce entry barriers to Aadhaar:51,52

1. All Indian residents are entitled to an Aadhaar number free of cost.

2. Aadhaar employs a decentralised enrolment system that makes use of multiple Enrolment Centres and outreach efforts.

3. The proofs-of-identity and address required from an Aadhaar enrollee may be one of a large number of accepted supporting documents. Eighteen proofs-of-identity and thirty-six proofs-of-address are considered valid for the purposes of enrolment.53 For individuals lacking such documentation, alternate means of enrolment have been specified (discussed in Appendix 2.1).

4. Individuals who have incomplete biometrics (for example, because of disability or age) are eligible to enrol. As a matter of policy, no individual can be denied Aadhaar even if she or he does not possess usable biometrics.54 Individuals lacking functional biometrics are meant to be de-duplicated using demographic information and manual adjudication. According to the UIDAI’s data, about 99.9 percent of the population possesses biometrics that are sufficient according to Aadhaar requirements.55 This issue is discussed further in Appendix 2.1.

Independent research on whether, and what, barriers to Aadhaar enrolment remain for individuals who wish to enrol would be useful. This research is of particular importance as difficult-to-access populations such as the homeless, or other marginalised groups, may face higher barriers, and it is pivotal to understand how these can be mitigated. Since Aadhaar increasingly links to a wide range of government benefits for the poor (see Chapters 3, Legal and Governance Framework, and 5, Social Protection, for details), reducing or eliminating exclusion because of the lack of an Aadhaar number is critical.

An important metric to assess the completeness of the Aadhaar database is the biometric false rejection rate. This refers to the percentage of individuals who will be falsely rejected by the Aadhaar biometric de-
duplication system, despite being eligible (that is, unique) candidates. According to the UIDAI, the biometric false rejection rate as measured in 2012 (with 84 million enrolees) was 0.057 percent. All entries identified as duplicates by the biometric system must go through a manual adjudication process, where these errors may be corrected. (In addition, there will be genuine duplicates that will also require manual adjudication). Unlike the false acceptance rate, the false rejection rate is expected to grow linearly as the Aadhaar database expands.56

Two counteracting forces must be taken into account when estimating contemporary false rejection rates. Per-day enrolment in the Aadhaar database has fallen from a peak of one million enrolees per day, to an average of about 360,000 enrolments per day in May 2017.57 This would imply fewer manual adjudications required each day, if false rejection rates were held constant. However, since the last enrolment quality studies were done in 2012, the Aadhaar database has grown from 84 million to 1.14 billion residents. Given that the false rejection rate is expected to grow linearly as the Aadhaar database expands, we can expect an increase in the rate of false rejections. Estimating this rate at current enrolment, and comparing it with those of other large biometric databases or international benchmarks, is an important area for future inquiry. In addition, assessing the UIDAI’s capacity to resolve false rejections through manual adjudication is a key area of research to determine the extent of potential exclusion from Aadhaar. These topics are summarised in the final section of this Chapter.

Data security

In addition to the quality of the Aadhaar database, a key consideration is the security of Aadhaar holders’ personal information. Below are certain provisions the UIDAI has embedded in the enrolment process to increase data security:58,59

1. All enrolment operators and supervisors must have an Aadhaar number to be uniquely identified and for their performance to be analysed.

2. Enrolment data sent from the Enrolment Agency is encrypted and is only decrypted once at the CIDR.
3. Upon reaching the CIDR, enrolment data is decrypted for de-duplication, but decrypted data is not held in storage.

4. The data sent to the ABIS is anonymised; that is, none of the ABIS systems have access to a resident’s demographic information.

5. ABIS providers do not store biometric source data; they can only store templates for the purpose of de-duplication.

6. All data is stored in UIDAI storage and cannot leave its premises.

7. The original biometric images of fingerprints, irises, and face are archived and stored offline and are not accessible through an online network.

A 2011 Parliamentary Standing Committee raised concerns regarding the involvement of private sector entities in the data capture and de-duplication stages of the enrolment process. The UIDAI has consistently maintained that it employs best-in-class technologies and rigorous security protocols throughout the enrolment process to ensure data security. Independent assessment of these mechanisms may be an area for future research.

Aadhaar Authentication

The Aadhaar database allows government and private sector entities to authenticate individuals against their Aadhaar records. In this Chapter, we discuss the processes through which Aadhaar authentication functions. In Chapters 4 to 6 (Financial Inclusion, Social Protection, and Emerging Uses), we cover a range of authentication applications.

The UIDAI provides two types of Aadhaar authentication services to the public and private sectors. First, there is a “yes/no” authentication facility. Second, there is an electronic Know Your Customer (e-KYC) facility. Both are discussed in the following sections.

Yes/No authentication

Yes/No authentication refers to the process by which an individual’s Aadhaar number, along with demographic or biometric information, is submitted to the CIDR for verification. The CIDR checks the correctness, or lack thereof, of the data. The purpose of Aadhaar Yes/No authentication is to provide a digital, online identity platform to validate the identity of Aadhaar holders “instantly, anytime, and anywhere.” Both government and private service providers can use this authentication service to verify an individual’s identity for the provision of a service. For example, the Food and Civil Supplies Department of a state may require beneficiaries to authenticate themselves using their biometrics and Aadhaar numbers to receive grain under the Public Distribution System (a food subsidy programme).

Aadhaar Yes/No authentication can be performed in three ways:

1. **Demographic authentication** wherein the Aadhaar number and demographic data of the Aadhaar holder is matched with the holder’s demographic attributes stored in the CIDR. A “yes” or “no” response is returned, along with other information related to the transaction.

2. **Biometric authentication** wherein the Aadhaar number and biometric data submitted are matched with the biometric attributes of the Aadhaar holder stored in the CIDR. Biometric authentication may be carried out through fingerprint authentication or iris scans. The CIDR returns a “yes” or “no” response, along with other information related to the transaction.

3. **One-time Pin authentication** is when a One-Time Pin (OTP) is sent to the mobile number of the Aadhaar holder as specified in the UIDAI’s records. The Aadhaar holder shall provide this OTP along with her or his Aadhaar number during authentication and the same shall be matched with the OTP sent by the UIDAI. As before, a “yes” or “no” response is provided together with any other information related to the authentication transaction.
Multi-factor authentication is a combination of two or three approaches highlighted above. The UIDAI offers five types of authentication services, based on a combination of the three authentication types discussed above. These are detailed in Appendix 2.2. No personal information can ever be returned by the Yes/No authentication process. The process serves only to verify the identity of an Aadhaar holder to a requesting entity.

According to the Aadhaar Act 2016, all authenticating agencies (described in the next section) shall obtain the consent of an individual before collecting her or his identity information, in a manner specified by UIDAI regulations. They are also required to ensure that the identity information of an individual is used only for submission to the CIDR. See Chapter 3, Legal and Governance Framework for more information.

Data available from April 2016 to March 2017 demonstrates that the number of Yes/No authentications has increased rapidly during this period. The number of individual Aadhaar numbers authenticated has been increasing as well, albeit less rapidly. This is visualised in Figure 2.6.

Yes/No authentication ecosystem

Several stakeholders comprise the Yes/No authentication ecosystem. Information flow in the authentication process, and the role of each stakeholder, is discussed below.

UIDAI: The UIDAI functions as the regulator and overseer of the authentication ecosystem. It owns and manages the CIDR, which contains Aadhaar holders’ personal information.

Authentication User Agency (AUA): AUAs are organisations that use Aadhaar authentication to enable their services. To gain access to the Aadhaar authentication facility, AUAs must enter into a formal agreement with the UIDAI. AUAs may also submit authentication requests from other entities that are “sub-AUAs.” For example, a state government (such as the Government of Himachal Pradesh) may act as an AUA, with several state-level departments and ministries functioning as sub-AUAs. In the private sector, a large bank may establish itself as an AUA, and several small banks may access authentication as sub-AUAs. AUAs and sub-AUAs are commonly referred to as “requesting entities.” As of April 2017, there were 352 AUAs in India. The number of sub-AUAs is not publicly available.

Authentication Service Agency (ASA): ASAs establish connectivity to the CIDR and transmit authentication requests from AUAs to the CIDR. In turn, they transmit the CIDR’s responses to authentication requests back to AUAs. ASAs build and maintain their connectivity to the CIDR on the basis of specifications and standards laid down by the UIDAI. As an example, a state government’s

Figure 2.6: Monthly Aadhaar authentications, Apr 2016 to Mar 2017

Data source: UIDAI Authentication Portal
Information Technology department (for example, Directorate of Information Technology, Government of Maharashtra) could function as an ASA through which several state ministries or departments (AUAs or sub-AUAs) may channel their authentication requests. Similarly, a telecommunications carrier could establish connectivity to the CIDR and act as an ASA for private AUAs. An ASA may serve more than one AUA, and one AUA may choose to access Aadhaar authentication through multiple ASAs. An AUA could also choose to become its own ASA. As of April 2017, there were 27 operating ASAs in India.

**Authentication devices:** These devices collect personal information from Aadhaar holders, encrypt and transmit this data, and receive authentication results. They include personal computers, handheld devices, and kiosks. These are used and managed by AUAs or sub-AUAs.

**Aadhaar holders:** Aadhaar holders are individuals whose identity may be authenticated for service delivery.

Figure 2.7 below visualises the flow of information during the Yes/No authentication process.

**e-Know Your Customer (e-KYC)**

The second type of authentication service provided by the UIDAI is Aadhaar-enabled e-KYC. This service authenticates an individual’s identity and provides additional demographic details. Certain service providers—such as those in the banking industry—require individuals to provide proofs-of-identity, address, and other demographic information before they can receive services. For these, Aadhaar-enabled e-KYC provides an instant, electronic, and undeniable proof-of-identity, address, date of birth, and gender. In addition, it provides the resident’s mobile number and email address to the requesting agency. KYC data can only be provided upon authorisation by an Aadhaar holder, through biometric or OTP-based Aadhaar authentication.

**e-KYC ecosystem**

Analogous to AUAs, KYC User Agencies (KUAs) are organisations that have access to the e-KYC service. KUAs gain access to e-KYC services through KYC Service Agencies or KSAs (analogous to ASAs). The flow of information for e-KYC is the same as that for Aadhaar authentication. As of April 2017, there were 274 registered KUAs in India.
Between December 2012-2015, more than 35 million Aadhaar holders used the UIDAI’s e-KYC authentication service.  

**Authentication Quality and Security**

The quality of Aadhaar authentication mechanisms is a critical factor determining individuals’ access to services that require authentication—increasingly, a large number of government programmes. The UIDAI has also put in place technical safeguards to increase the security of authentication transactions. Both authentication quality and security would benefit from policy-oriented research, discussed below and in the last section of this Chapter.

**Authentication quality**

Of the three (biometric, demographic, and OTP-based) mechanisms of authentication, data on biometric authentication is most widely reported.

The UIDAI conducted a series of studies in five Indian states in 2011-2012 to determine the technological systems and processes that would enable the highest possible quality of biometric authentication. They found that identifying a finger that produces the best matching result for every resident (known as “best finger”) would ensure greater authentication accuracy than standardising one finger (for example, the right index finger) for all residents to use.

Further, the UIDAI determined that employing a system of identifying two “best fingers” for each resident, and allowing up to three authentication attempts, would ensure that only about 1 percent of individuals would be falsely rejected during authentication despite having valid biometrics.

Available data from government social protection programmes in Andhra Pradesh and Telangana (two southern Indian states) reveals that on average about one in seven individuals faced authentication failures in 2016-17 after multiple attempts. The transaction failure statistics may point to genuine beneficiaries being falsely rejected (for reasons such as poor capture of biometrics at the time of enrolment, change in biometrics over time, or infrastructure-related problems such as connectivity) or fraudulent authentication attempts. Individuals who face transaction failures may still receive services as paper-based authentication systems can be used to manually override the digital transaction. A more detailed discussion of this data is presented in Chapter 5, Social Protection.

Detailed inquiry into authentication accuracy, rates of failure (including false rejections), and systems for handling authentication failures for genuine beneficiaries are critical areas of research. Since millions of beneficiaries of government programmes interact with these systems regularly, administrators would benefit from understanding how to reduce these failure rates, or fall back on more appropriate alternatives. These issues are discussed further in the closing section of this Chapter.

**Authentication security**

In addition to the quality of Aadhaar authentication, the security of Aadhaar holders’ information transmitted through the authentication process is an important consideration. The UIDAI lists technical regulations to increase the security of (biometric and non-biometric) authentication transactions.

1. All requesting entities must use certified biometric devices and software, conforming to regulations laid down by the UIDAI.

2. All identifying information received from individuals (including Aadhaar number, biometric or demographic information) must be encrypted after collection, and before transmission to the requesting entity’s server.

3. All authentication requests must be digitally signed by the AUA or ASA.

4. The UIDAI allows Aadhaar holders to “lock” their biometrics. All authentication attempted using biometrics that have been locked by an Aadhaar holder receive a “No” response. A user may
unlock her or his biometrics temporarily when attempting authentication. This measure is designed to prevent anyone other than an Aadhaar holder from being able to fraudulently conduct authentication on the holder’s behalf.

Independent and recurring studies of whether and to what degree technical safeguards for data security are upheld in the authentication process may be an area of future research.

**Payment systems**

In addition to its authentication feature, Aadhaar enables two types of payment systems. These are discussed below.

**Aadhaar Enabled Payment System (AEPS)**

AEPS employs the UIDAI’s authentication services to allow residents to conduct banking transactions using only their Aadhaar number and biometrics. Business correspondents, or agents employed by banks, conduct door-to-door banking through the use of microATMs (handheld devices that can execute banking transactions). Aadhaar holders can provide their Aadhaar number, identify their bank, and provide their fingerprint to obtain access to Aadhaar-enabled banking services such as balance enquiry, cash withdrawal and deposit, and fund transfer between Aadhaar holders. The Aadhaar holder’s biometric information is sent to the CIDR for authentication. The CIDR responds with a “yes” or “no” response. If the authentication response is “yes,” the bank carries out the required transaction.

An Aadhaar holder’s bank account must be linked to her or his Aadhaar number to gain access to Aadhaar-enabled banking services. For a more detailed discussion on AEPS, see Chapter 4, *Financial Inclusion*.

**Aadhaar Payment Bridge System (APBS)**

APBS is used for the disbursement of government benefits using Aadhaar numbers. Various government departments that provide subsidies and monetary entitlements to Indian residents make use of APBS to channel beneficiary payments. Similar to AEPS, APBS requires beneficiaries’ Aadhaar number to be linked to a bank account. APBS is discussed in further detail in Chapter 4, *Financial Inclusion*.

---

**Areas for Future Research**

As discussed in later Chapters, Aadhaar’s applications are growing. Understanding and strengthening Aadhaar’s technical architecture is an important step towards improving how Aadhaar functions for individual users, private sector players, and government stakeholders. The strengths and risks of Aadhaar’s architecture could also provide useful lessons for countries across the world building digital identity systems of their own.

Research on Aadhaar’s architecture would be valuable for policymakers at the UIDAI, as well as users of Aadhaar-based services such as authentication and e-KYC. Technological and operational research focused on strengthening Aadhaar’s systems and processes could a) improve Aadhaar’s coverage and prevent inadvertent exclusion, b) strengthen Aadhaar authentication, and c) augment the accuracy and security of the Aadhaar database.

Four research themes encapsulate these objectives:

- **Research on preventing inadvertent exclusion through Aadhaar’s enrolment processes; assessing barriers (if any) to enrolment, exclusion due to insufficient demographic or biometric information, and false rejection from the Aadhaar database**

- **Assessment of Aadhaar authentication quality, including authentication devices, operating processes guiding information flow, and user experience and outcomes, to streamline authentication-based service delivery**

- **Research on the accuracy of Aadhaar’s database; updated measurement of the false acceptance rate and the rate of duplicates enrolling, and mechanisms to improve the accuracy of enrolled individuals’ personal data**

- **Assessment of the data security provisions in Aadhaar enrolment and authentication to protect Aadhaar holders’ personal information**
In addition to the research agenda above, regular release of data by the UIDAI on Aadhaar’s performance relating to each theme above will provide valuable information on how to continually improve Aadhaar’s architecture.

To maximise the impact of practitioner-oriented research, we recommend:

| • Framing research questions in collaboration with practitioners |
| • Being responsive to decision-making schedules and other practitioner constraints |
| • Presenting insights in succinct documents and in-person meetings |
| • Providing follow-up support to translate research to action on-the-ground |
APPENDIX 2.1: Aadhaar Enrolment Process

To enrol for an Aadhaar number, individuals are required to provide certain demographic and biometric information (detailed in Figure 2.2, reproduced below).

In case an individual does not possess valid forms of proof-of-identity and proof-of-address documents, she or he may provide a Certificate of Identity or a Certificate of Address issued by a government-approved authority. Since a large number of Indian residents do not possess a valid proof-of-date-of-birth, the UIDAI allows three types of records. A “verified” date of birth is recorded based on valid documentary evidence. A “declared” date of birth is one wherein the enrollee is aware of her or his date of birth but does not have supporting evidence. Finally, an “approximate” date of birth is recorded when the two procedures above are inapplicable. This date of birth is meant to be estimated and ascertained by trained enrolment operators.

There are also two alternative methods for cases where individuals cannot furnish valid documents, and a separate procedure for children under the age of five. First, an individual may be enrolled using the Head of Family (HoF)-based system. In this method, the head of a family can vouch for the identity and address of her or his family members. The Head of Family must be enrolled in Aadhaar, with valid proof-of-identity and address documents. The enrollee also needs to provide a document serving as a proof of her or his relationship with the Head of Family.

Second, an individual may also be enrolled through the introducer system. An introducer is appointed by the Registrar and is entrusted to vouch for the identity and address of an enrollee in her or his locality. An introducer must possess a valid Aadhaar number, which is submitted during enrolment to ensure traceability.

In the case of children below the age of five, one of either the parent’s or guardian’s names and Aadhaar numbers (or enrolment numbers) must be recorded. A child cannot be enrolled until her or his parent or guardian has been enrolled. Children below the age of five do not have to supply biometrics at the time of enrolment. Upon reaching the age of five, they are required to re-enrol, and provide biometric data. If accepted into the Aadhaar database after the

<table>
<thead>
<tr>
<th>INFORMATION</th>
<th>REQUIREMENT</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEMOGRAPHIC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Mandatory</td>
<td>Proof-of-identity document</td>
</tr>
<tr>
<td>Gender</td>
<td>Mandatory</td>
<td>Proof-of-identity document</td>
</tr>
<tr>
<td>Date of birth</td>
<td>Mandatory</td>
<td>Proof-of-date-of-birth document</td>
</tr>
<tr>
<td>Residential address</td>
<td>Mandatory</td>
<td>Proof-of-address document</td>
</tr>
<tr>
<td>Mobile number</td>
<td>Optional</td>
<td>Self-declared</td>
</tr>
<tr>
<td>Email ID</td>
<td>Optional</td>
<td>Self-declared</td>
</tr>
<tr>
<td>BIOMETRIC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photograph of face</td>
<td>Mandatory</td>
<td>Captured during enrolment</td>
</tr>
<tr>
<td>Fingerprints (all 10 fingers)</td>
<td>Mandatory</td>
<td>Captured during enrolment</td>
</tr>
<tr>
<td>Iris captures of both eyes</td>
<td>Mandatory</td>
<td>Captured during enrolment</td>
</tr>
</tbody>
</table>

Source: This table is based on the UIDAI’s Strategy Overview document.
de-duplication procedure, the child retains the same Aadhaar number.\textsuperscript{84}  

A procedure is specified for cases in which an individual is not able to supply biometric information (for example, because of physical disability). A note is made of any mandatory biometric information that cannot be collected and a photograph is taken with a complete view of the missing biometrics, as evidence.\textsuperscript{85} An inability to supply biometric information cannot be grounds to deny enrolment.

Operators at Enrolment Centres are required to record residents’ consent for sharing their personal data, as well as for enrolling in Aadhaar. In addition, they are required to show enrollees the demographic data being recorded in the database for them to validate it. Copies of all documents received from an enrollee during the enrolment process, along with her or his enrolment form, are stored at the Enrolment Centre. These copies are then sent for permanent storage to the Registrar.\textsuperscript{86} At the end of the process, enrollees receive a 14-digit enrolment number, which serves as proof of enrolment and can be used to check the status of application.
APPENDIX 2.2: Forms of Aadhaar Authentication

The UIDAI allows Aadhaar authentication to be performed in three ways: demographic, biometric, and One-Time Pin authentications. Combinations of these three authentication methods form five distinct authentication services.

1. Type 1 Authentication: This consists of purely demographic authentication. An individual’s Aadhaar number and demographic data are matched with her or his demographic attributes stored in the CIDR.

2. Type 2 Authentication: This consists solely of One-Time Pin (OTP) authentication. A One-Time Pin is sent to the registered mobile number of an Aadhaar holder, and is matched with the OTP sent by the UIDAI. This form of authentication may be used in locations where deployment of biometric authentication is not feasible.

3. Type 3 Authentication: This refers to single-factor biometric authentication. That is, either the fingerprint or iris scan of an Aadhaar holder is collected and matched with her or his biometric attributes stored in the CIDR.

4. Type 4 Authentication: This is a combination of types 2 and 3, wherein residents are authenticated based on single-factor biometric authentication as well as OTP-based authentication. The combination of biometric and OTP (two-factor) authentication is intended to provide a higher degree of authentication assurance.

5. Type 5 Authentication: This refers to three-factor authentication, wherein an Aadhaar holder is authenticated using fingerprint, iris scan, and OTP authentications. This form provides the greatest degree of authentication assurance.
ENDNOTES


2. For more information, see the World Bank’s “Brief on Digital Identity”: Digital ID connects people to electoral participation, educational opportunities, health and social welfare, banking, and economic development. It gives people a chance to better communicate and be recognised by their government, while also giving governments the opportunity to listen and improve the lives of their citizens.”


8. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 defines a resident as any individual resident in India for 182 days or more in the year before application for Aadhaar enrolment.


10. Other forms of digital identity have not reached the same scale as Aadhaar. The total number of Permanent Account Number (PAN) cards (identification issued by India’s Income Tax Department) generated is about 52 million, the number of driver’s licenses is about 170 million, and the number of beneficiaries possessing a ration cards (necessary for receiving a food subsidy under the Public Distribution System) is about 667 million. The Voter ID scheme further covers about 450 million individuals.


   PDS: Figure calculated using data from different State Portals.


11. Ration cards are required for obtaining access to food and fuel subsidies under the Public Distribution System.


13. Non-Aadhaar biometric identities have been used in health and employment programmes such as the Rashtriya Swasthya Bima Yojana (RSBY), the Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS), and for issuing passports in India, among other uses. However, the scale of these is smaller than Aadhaar and the biometric information is not used for eliminating duplicates.

14. An identity system cannot guarantee complete uniqueness; instead, it can only lower the probability of duplication to a certain threshold. In the case of Aadhaar, as discussed later in the Chapter, the probability of duplicates is low. For the rest of this Chapter and report, when referring to Aadhaar’s uniqueness, we will assume such “statistical uniqueness,” but will not
use this phrase each time.

15. The UIDAI carried out a de-duplication exercise in August 2015 and identified 3.94 percent duplicates in food subsidy (Public Distribution System), 0.75 percent duplicates in cooking gas (Liquefied Petroleum Gas) subsidy, and 1.08 percent duplicates in an employment guarantee programme (Mahatma Gandhi National Rural Employment Guarantee Scheme).


17. Ibid.


19. Ibid.


22. Ibid.

23. Later, in September 2015, the government revised the Allocation of Business Rules to attach the UIDAI to the Department of Electronics and Information Technology (DeitY).

24. The United Nations estimates India’s population in 2017 at 1,342,513,000 people.


28. Ibid.


31. Individuals who cannot provide a proof-of-date-of-birth can register their date of birth through other means detailed in Appendix 2.1.

32. The Right to Information Act provides the framework for citizens to request information pertaining to or kept by public authorities in an attempt to create greater accountability and transparency. Parliament of India. The Right to Information Act, 2005 (2005).


34. As of April 2015, the total Aadhaar numbers generated based on the introducer system were 219,296. Based on available UIDAI estimates, the number of Aadhaar holders in 2015 were about 930 million.
   Aadhaar numbers generated based on the introducer system: Ibid.


37. Ibid.


41. UIDAI established two committees in 2009, the Biometric Standards Committee and the Demographic Data Standards and Verification Committee.


43. Ibid.


47. Exceptions to this rule are discussed in Appendix 2.1.


49. UIDAI’s population estimates are based on projected 2015 figures.


50. Ibid.


55. Ibid.

56. Ibid.


63. Ibid.

64. Ibid.


71. These were Delhi, Karnataka, Jharkhand, Himachal Pradesh, and Maharashtra.

72. Ibid.

73. A detailed discussion of this data is presented in Chapter 5, Social Protection.


79. This service can be, and is, provided without the use of Aadhaar as well.


81. Ibid.

82. Ibid.


84. Ibid.


