UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

Role of Biometric Technology in Aadhaar Authentication

Authentication Accuracy –Report

Date: 27 March 2012

Executive Summary

This report focuses on findings of a series of Proof of Concept (PoC) studies carried out by UIDAI from Jan 2011 to Jan 2012 on Aadhaar biometric authentication. The PoC studies focused on fingerprint biometric and its impact on authentication accuracy in the Indian context.

This report describes the series of proof of concept (PoC) studies conducted, the design framework of these studies, the analysis of the data obtained from the studies, specific techniques, processes and methods that can improve the authentication accuracy and concludes with a set of recommendations for the Aadhaar Authentication system.

Authentication answers the question 'Are you who you say you are?', and it does so using different factors:

- What you know– user id/password, PIN, mother's maiden name, etc.
- What you have – a card, a device such as a dongle, mobile phone, etc.
- What you are – a person's biometric markers such as fingerprint, iris, voice etc.

The 'what you are' biometric modes captured during Aadhaar enrolment are fingerprints, iris scans and face. Of the 3 modes, fingerprint biometric happens to be the most mature biometric modality in terms of usage, extraction/matching algorithms, standardization as well as availability of various types of fingerprint capture devices. This report focuses on fingerprint authentication and looks into improving the Aadhaar Authentication accuracy in the Indian context by various methods.

Location of PoCs: To ensure that residents from both rural and urban areas were covered, the PoCs were carried out at the following locations and they covered more than 50,000 Aadhaar holders:

- PoC1 Karnataka - Apr 15 2011 to May 21
- PoC2 Delhi - June 3 to 15
- PoC3 Delhi - July 9 to 20
- PoC4 Himachal Pradesh - July 23 to Aug 3
- PoC5 Maharashtra - July 28 to Aug end
- PoC6 Jharkhand - Aug 18 to 26
- PoC7 Delhi - Sep 22 to 29
- PoC8 Karnataka - Dec 17 to Jan 31 2012

Factors Studied: The PoCs studied the impact of various factors on fingerprint biometric authentication including:

- Authentication devices and interoperability - different sensor makes & technologies, different minutiae extractors, different form-factors (handheld devices & USB based devices)
- Number of fingers - using single finger once, same finger multiple times, using multiple distinct fingers
- Fingerprint quality
- Feasibility and effect of "best finger" detection (BFD)
- Network (availability, bandwidth, service provider, landline vs. mobile, reliability & latency factors across networks)
- Feasibility of buffered authentication

The PoC was conducted using the principles outlined in [ISO 19795-2, 2007], “Biometric performance testing and reporting—Testing methodologies for technology and scenario evaluation”, an ISO standard.

Proof of Concept (PoC) Study Process: The PoCs consisted of performing authentication over a resident population in a controlled manner using different authentication devices. The collected data was sent to the UIDAI Technology Centre. Further statistical analysis was performed at the Center.

Aadhaar Authentication Accuracy Study: Learning’s from previous study was used to devise an authentication procedure. Traditionally, right index finger and right thumb are used for biometric verification. However, these did not give us the desired accuracies and hence a procedure was devised which depended on the identification of a ‘Best Finger’ for every resident. The ‘Best Finger’ is the finger that gives the best matching result for that resident and it varies from one resident to another. The main goal of this study was to rigorously assess the authentication accuracy from this procedure. The key findings are presented below.

The PoC conducted in the rural setting representing typical demography of the population establishes that it is technically possible to use fingerprint to authenticate a resident in 98.13% of the population. The accuracy of 96.5% can be achieved using one best finger and 99.3% can be achieved using two fingers. Further improvement is possible if the device specifications are tightened to include only the best devices and certain mechanical guide is used to aid proper placement of the finger. It was also be demonstrated through benchmarking that the CIDR infrastructure is able to sustain one million authentication per hour.

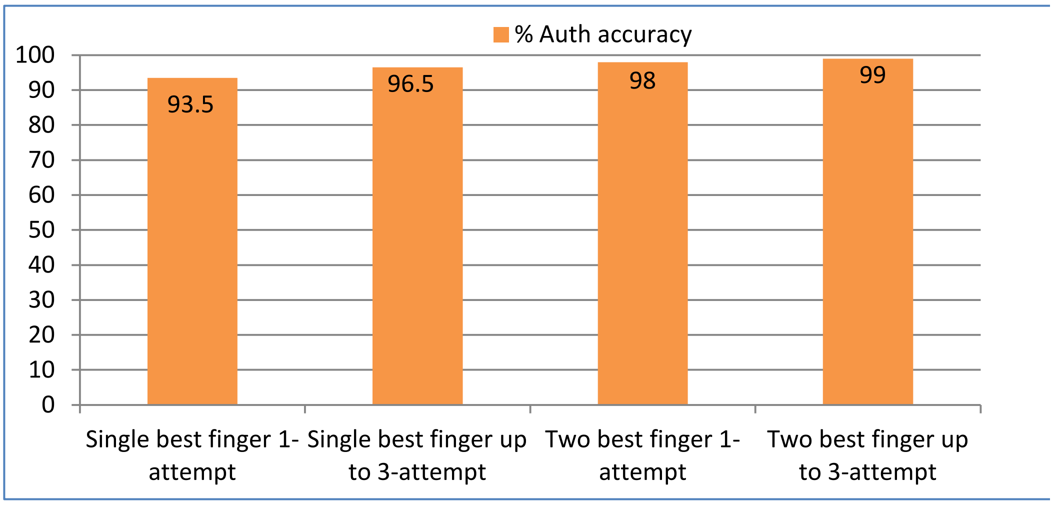
Accuracy could be further improved by using additional factors such as one-time-password (OTP), demographical data or second modality such as iris. It is recommended that a separate study in the line of the current study should be conducted for additional factors.

Fingerprint Biometric Authentication Accuracy – Key Findings

1. *There were differences in performance of different sensor-extractor combinations. This was observed under general conditions as well as across age groups. Study of this enabled identification of device specifications and certification procedure necessary for high authentication accuracy under Indian conditions.* ***[STQC, Certification, 2011]****.*
2. *Determining the 'best finger' of a resident so that they can use their best fingers for authentication improves the authentication accuracy:*
   - *Using the resident's best finger single-attempt gives an accuracy of 93.5% (FRR – 6.5%)*
   - *Using multiple (up to 3) attempts of the same best finger improves the accuracy to 96.5% (FRR – 3.5%)*
3. *Using 2 best fingers improves the accuracy further since more information is available to perform the matching:*
   - *Using 2 best fingers can improve the accuracy to 98% (FRR-2%) with a single attempt and above 99 % (FRR – 1%) with up to 3-attempts.*

FAR – False Accept Rate, FRR – False Reject Rate

**System FAR set to 1 in 10, 000 (i.e. 1 in 10, 000 authentications will have a false accept error)*
**For multiple attempt cases, 3 is the maximum number of attempts, but the average number of captures for single finger is 1.11 and for 2 fingers is 1.13.*



Note*: Unlike the Biometric Enrolment report entitled "Role of Biometric Technology in Aadhaar Enrollment" which used 84 million enrolments on the actual production system to analyze enrolment accuracy; it should be kept in mind that this report relies on data gathered at the Authentication PoCs only as opposed to production data – since the volume of production authentication transitions is still quite limited.*

Aadhaar Authentication Performance: A benchmarking study was undertaken to assess the performance of the Aadhaar Authentication system. Since Aadhaar Authentication is a 1:1 check (Aadhaar number is used to fetch the particular resident's record and matching of say fingerprint is performed only on that one record) it is not a compute intensive challenge like Aadhaar enrolment (where a single resident's biometric is compared to every other in the database, i.e. 1:N), the challenge is for the system to be able to handle a large number of authentication transactions – an estimated 100 million transactions per day. The box below presents the authentication performance results observed by an internal benchmarking test.

Authentication Performance Results

1. *The Authentication system was able to handle 10 million authentications in 10 hours with an average response time of around 200 milliseconds giving a system throughput of about 295 concurrent requests per sec.*
2. *80% Of the above requests were biometric authentications, 10% were demographic authentications and 10% were OTP authentications.*
3. *For biometric matching (which is the most computationally intensive of the 3 types) the system performance averaged 200 milliseconds per transaction, well within the sub-second target that was set.*

**Aadhaar authentication performance test environment consisted of 15 blade servers including database servers, biometric matching servers, messaging server, caching servers, and audit logging servers. Server configuration is being x86 Linux dual CPU 6-core.*

** The above benchmarking and load tests were conducted at UIDAI, since the authentication requests coming from pilot locations were in small numbers.*

Abbreviations

API	Application Programming Interface
ASA	Authentication Service Agency
AUA	Authentication User Agency
EOI	Expression of Interest
CIDR	Central Identity Data Repository
DET	Detection Error Tradeoff
FAP	Fingerprint Acquisition Profile
FAR	False Accept Rate
FRR	False Reject Rate
KYC	Know Your Customer
MINEX	The Minutiae Interoperability Exchange Test
NFIQ	NIST Fingerprint Image Quality
PDS	Public Distribution System
PoC	Proof of Concept
SDK	Software Development Kit
STQC	Standardisation Testing and Quality Certification Directorate
UIDAI	Unique Identification Authority of India

Contents

Figures

1 Introduction to UIDAI Authentication

The Unique Identification Authority of India (UIDAI) has been created with the mandate of providing a Unique Identity (Aadhaar) to all residents of India. Aadhaar enrolment has picked up momentum with over 27,000 enrolment stations conducting 10 Lakh enrolments every day across the country. The CIDR processes these enrolments by de-duplicating them to ensure uniqueness and then issues Aadhaar numbers.

One of the mandates given to UIDAI is to define usages and applicability of Aadhaar for delivery of various services. Towards Aadhaar-enabled delivery of services and applications, UIDAI provides online authentication using the resident's demographic and biometric information. The Aadhaar number, which uniquely identifies a resident, will give individuals the means to clearly establish their identity to public and private agencies across the country for service delivery.

Enrolment Process: Aadhaar enrolment has 2 main parts. The enrolment frontend, which consists of enrolment stations deployed across the country where people enroll for an Aadhaar number. The process of enrolment involves the collection of 4 demographic fields: name, address, date-of-birth and gender and the capture of biometrics – which includes all 10 fingerprints, 2 irises and a photo of the face. This enrolment information is securely encrypted and sent to the CIDR. The Enrolment backend operations are carried out at the CIDR, where the packet is checked and validated for correctness and then de-duplicated against the existing enrolment database. Only when the new enrolment record is found to be unique is an Aadhaar number granted to that particular resident.

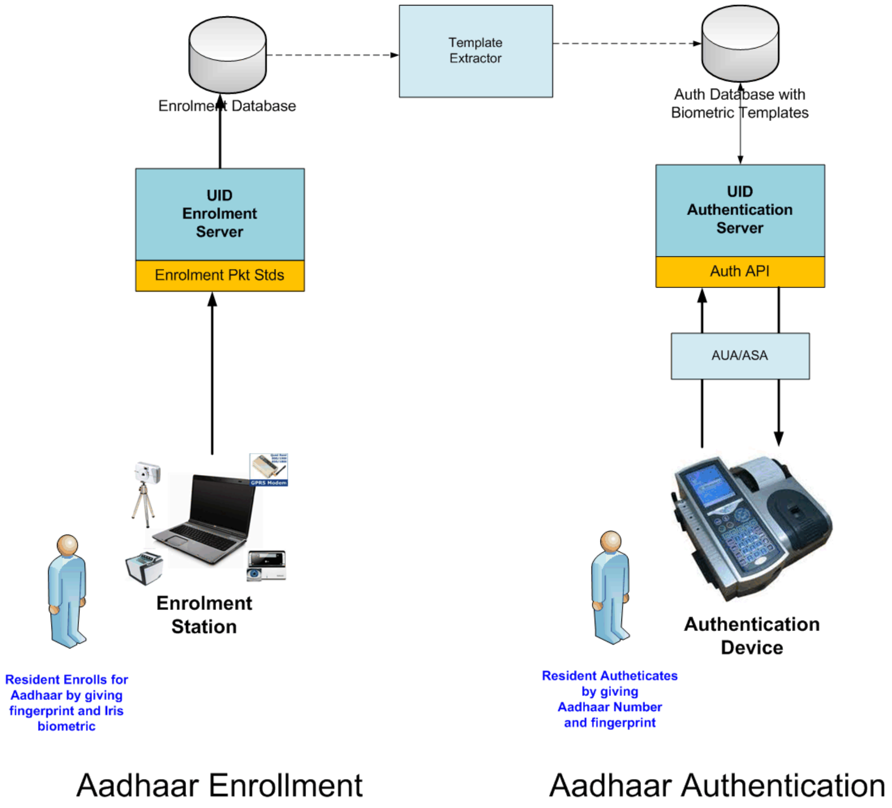

Template Extractor
Enrolment Database
Auth Database with Biometric Templates
UID Enrolment Server
Enrolment Pkt Stds
UID Authentication Server
Auth API
AUA/ASA
Enrolment Station
Authentication Device
Resident Enrolls for Aadhaar by giving fingerprint and Iris biometric
Resident Authenticates by giving Aadhaar Number and fingerprint
Aadhaar Enrollment
Aadhaar Authentication

Figure 1: Aadhaar Enrolment and Authentication

1.1 Aadhaar Authentication

Aadhaar Authentication is the process wherein, Aadhaar number along with the Aadhaar holder's personal identity data is submitted to the CIDR for matching, following which the CIDR verifies the correctness thereof on the basis of the match with the Aadhaar holder's identity information available with it. Since the Aadhaar number is mandatory during an authentication transaction, the appropriate resident's record can be fetched and a simple 1:1 match of the biometric/demographic data can complete the authentication transaction. To protect resident's privacy, Aadhaar Authentication service responds only with a "Yes/No" and no Personal Identity Information (PII) is returned as part of the response.

Aadhaar Authentication enables residents to prove their identity based on the demographic and/or biometric information captured during enrolment, thus making the process of identification convenient and accurate. Aadhaar Authentication can help agencies in delivering services to eligible beneficiaries based on establishing their identity, thus improving efficiency and transparency in service delivery to the common man.

Aadhaar Authentication supports several different types of authentication through a combination of demographic fields, biometric fields as well as other methods such as one-time-password (OTP), but, in all forms of authentication the Aadhaar Number needs to be submitted so that this operation is reduced to a 1:1 match. The service delivery agency can choose any required authentication type based on its application and service needs. The Aadhaar Authentication system consists of partner organizations such as Authentication Service Agency (ASA) and Authentication User Agency (AUA). Details can be found on the UIDAI website **[UIDAI, Authentication Model, 2012].**

The different types of Aadhaar authentication methods are described below.

1.2 Demographic Matching

Demographic matching refers to the usage of Aadhaar Authentication system by AUAs for matching Aadhaar number and the demographic attributes (name, address, date of birth, gender, etc., as per API specifications) of a resident in the CIDR with those submitted by the resident from an authentication device.

Examples of demographic based Aadhaar authentication:

- Banks for automated KYC checking
- Government welfare scheme for eliminating fake and duplicate identities in their databases
- Telecom service providers for address verification
- Private institutions/ banks for date of birth verification

1.3 Biometric Matching

Biometric matching refers to the usage of Aadhaar Authentication for matching Aadhaar number and the biometric attributes of a resident in the CIDR to the biometric data submitted by the resident from an authentication device.

Note: Although currently only fingerprint biometric is being offered – and is the focus of this report, it is likely that in the near future iris biometric authentication will also be supported.

Examples of biometric based Aadhaar authentication:

- Govt. departments delivering services to residents

- Banks for establishing identity of customers before starting a new bank account
- Telecom service providers before issuing a new mobile connection
- Attendance tracking or proof of presence in several scenarios

1.4 Matching using other factors

Besides demographic and biometric authentication, Aadhaar supports certain other authentication factors, such as one-time-password (OTP). In this case, an OTP (a 6 digit number) is sent to the registered mobile phone number of the resident seeking Aadhaar Authentication. The OTP shall have limited time validity (e.g. 15 minutes). The resident shall provide this OTP during authentication and the same shall be matched with the OTP at the CIDR.

For example: OTP based authentication could be used by

- Banks for authenticating customers during internet banking transaction
- E-commerce companies before completing a cash-on-delivery transaction

The service delivery agency (MGNREGA, PDS, Banks, Telecom companies etc.) can mix and match between the demographic, biometric and other factors to construct an appropriate Aadhaar Authentication combination to suit the needs of their application. All the above combinations are available through Authentication APIs (Application Programmatic Interface) that registered AUAs can access.

The next chapter will describe the components of Aadhaar Authentication system in further detail.

2 Components of Aadhaar Authentication System

This section describes components of the Aadhaar Authentication system and the flow of authentication request and response. The high level components are:

1. Authentication frontend
2. Authentication aggregator/partner network
3. Authentication backend at CIDR

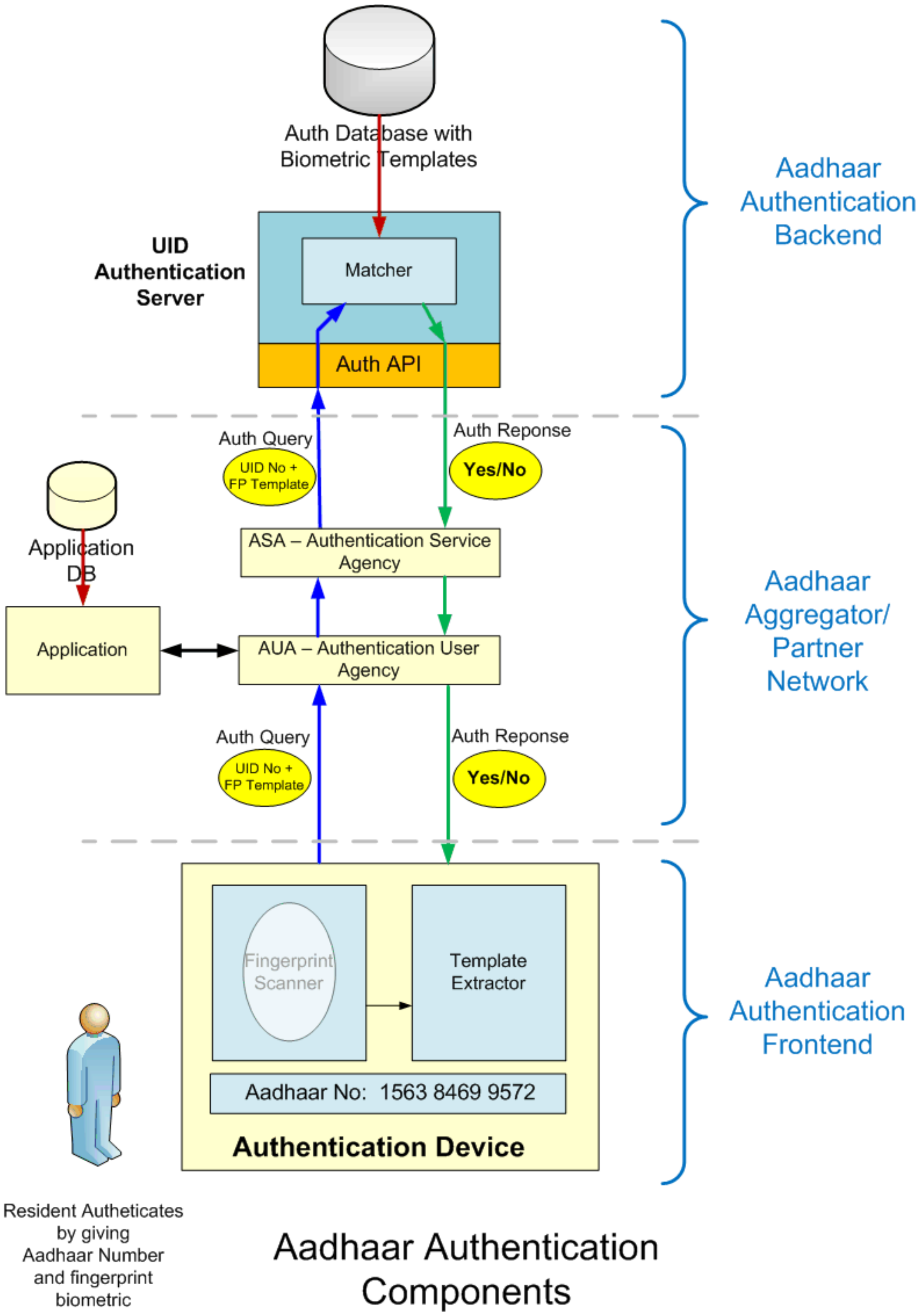

Auth Database with Biometric Templates
UID Authentication Server
Matcher
Auth API
Aadhaar Authentication Backend
Auth Query
UID No + FP Template
Auth Reponse
Yes/No
Application DB
Application
ASA – Authentication Service Agency
AUA – Authentication User Agency
Aadhaar Aggregator/ Partner Network
Auth Query
UID No + FP Template
Auth Reponse
Yes/No
Fingerprint Scanner
Template Extractor
Aadhaar No: 1563 8469 9572
Authentication Device
Aadhaar Authentication Frontend
Resident Autheticates by giving Aadhaar Number and fingerprint biometric
Aadhaar Authentication Components

Figure 2: Components of Aadhaar Authentication

2.1 Aadhaar Authentication Frontend

The Authentication frontend largely consists of the service provider at the point of service, such as a fair price shop using an Aadhaar compliant authentication device to authenticate ration card holders who come to purchase subsidized grains. A biometric authentication device is deployed at the point-of-service; this device could consist of:

- The fingerprint sensor – which captures a single fingerprint image
- Fingerprint extractor – the software in the device that extracts fingerprint minutiae from the captured image, so as to submit small size minutiae instead of a large image
- Number/Text capture device – used to input Aadhaar number, name, address etc.

The Aadhaar number, demographic information and biometric information (such as the fingerprint minutiae) are all packaged into an Authentication packet ***[UIDAI, Authentication, 2012]*** and sent to the Aadhaar CIDR through the network of AUA/ASA partners.

This paper focuses on the biometric sensor, extractor and the actual method of fingerprint authentication (single finger, best finger, two best fingers etc.) and its impact on overall biometric accuracy of the system.

The Authentication frontend components are designed and implemented by service providers (PDS, MGNREGA, Banks, etc.) who sign up as AUAs, in conjunction with application software companies and device manufacturers – all in compliance with UIDAI standards and guidelines.

2.2 ASA/AUA aggregator/partner network

In order to service the large expected demand for online Aadhaar Authentication services, a set of aggregators and network partners have been envisioned in the authentication framework. They include:

Authentication Service Agency (ASA): ASA is an entity that has established secure leased line connectivity with UIDAI data center(s) compliant with UIDAI's standards and specifications. ASAs offer their UIDAI-compliant network connectivity as a service to AUAs and transmit AUAs' authentication requests to CIDR.

Authentication User Agency (AUA): AUA is a government / public / private entity that uses Aadhaar Authentication to enable its services and connects to the CIDR through an ASA. It is also possible that an AUA engages more than one ASA. It is also possible for an AUA to also be an ASA.

The authentication packet created by the Authentication device will be routed through the appropriate AUA and ASA before it reaches the Aadhaar CIDR.

2.3 Aadhaar Authentication Backend

The Aadhaar biometric authentication backend system consists of:

- Authentication Server – which among other things contains a biometric matcher
- Authentication API layer – API used by device/AUA to make an Aadhaar Authentication call
- Authentication Biometric Template Data Base – repository of fingerprint and iris templates of all the enrolled residents

From an authentication backend perspective, this paper focuses on the biometric SDK (Software Development Kit) used at the backend for extraction of template from the enrolment database as well as matching incoming templates with the ones in the database. The various choices of the frontend in combination with backend SDK will determine the accuracy of the overall system. This will be studied in detail in the coming chapters.

3 Proof of Concept Study - Design and Field Implementation

3.1 Introduction to PoC studies

There have been very few studies regarding biometric authentication in the Indian field context and it was important to conduct rigorous PoC studies in order to design and configure the UIDAI authentication system. A number of such PoC studies have been carried out – each building on the learning from the previous ones. This chapter describes the design and setup for this study.

UIDAI undertook a series of studies to understand the impact of various factors on biometric authentication. The goal for these studies was to

> *Characterize & propose optimal authentication setups (server level & device level) for online biometric authentication of residents using single fingerprint device.*

The objectives were to understand the impact of variables at three levels:

- Device – sensor technology & make, extractor algorithms, device ergonomics etc.
- Server – such as matching algorithms, threshold levels, enrolment biometric quality etc.
- Other extraneous factors – resident fingerprint quality, demographic based variation (especially age) etc.

Consequently, the studies included factors such as:

- Device models
  - Different sensor makes
  - Different sensor technologies
  - Different minutiae extractors
- Number of fingers
- Fingerprint quality
- Best finger analysis
- Network (availability, bandwidth, service provider, landline vs. mobile, reliability & latency factors across networks)

International Standards Organization (ISO) has published guidelines for conducting biometric tests under the series ISO 19795. The applicable standard for conducting field tests is specified under ***[ISO 19795-2, 2007]***, which was used to guide the POC.

3.1.1 Population Groups

At each location, the resident population was divided into smaller groups built into the PoC application. These groups were partitioned on the basis of:

- number of fingers to be used for authentication
- whether fingerprint image or fingerprint minutiae was used
- whether transaction was online or buffered (*buffered transactions are those are sent to CIDR for authentication a little while later and not instantly after capturing the request – a solution that may be required for supporting intermittent network unavailability*)

3.1.2 PoC Client Application and Data Collection

As part of the PoC client application, to measure different variables and compare / fine-tune performance of various SDKs, detailed logs were captured for further analysis. At the UIDAI

Technology Centre, all logs were analyzed and authentication requests were replayed on multiple SDKs to understand the impact of various biometric matching algorithmic changes and other backend interventions that could be used to improve the authentication accuracy.

Based on this data, UIDAI had the opportunity to study the impact of single finger, multiple fingers, fingerprint quality at the time of authentication as well as fingerprint quality stored in the enrolment database.

3.1.3 Server Set Up

The authentications during the PoC were done in online mode with SDKs supplied as per contractual requirements by the three Biometric Service Providers (BSPs) of UIDAI. Even the buffered authentication requests were played from the PoC locations itself.

To enable online authentication, fingerprint minutiae need to be first extracted from the enrolment images and authentication templates generated. The minutiae contained in the authentication requests are then matched with the minutiae thus generated through matcher SDK. The SDK used for generating templates was kept same as the matcher SDK.

3.2 PoC 1 - Initial Field Study

The first field study was carried out with hand-held devices at Tumkur district in Karnataka in the months of April and May 2011 in which 14,220 residents were requested to participate.

The residents were divided into the following population groups:

Fingers	Online / Buffered	Percentage
Single	Online	40%
Single	Buffered	10%
Two (2 transactions)	Online	20%
Two	Online	10%
Two	Buffered	10%
Five	Buffered	10%

For this PoC study, UIDAI had published device specifications (based primarily on Micro ATM standards published jointly by Indian Banks' Association & UIDAI) and published an EOI asking for participation by device vendors. The vendors were required to implement standard PoC application software on their devices based on prototype PoC application software given by UIDAI as a reference. The vendor application software was mandated to store the data in a standardized log format, so that UIDAI could later analyze data from various devices in a uniform manner.

This study saw participation from 6 device vendors, who provided devices in the point-of-sale (POS) form factor.

During the fingerprint authentication trials, residents were requested to provide their Aadhaar number. The PoC application software divided them into population group as listed above and then the residents were asked to place their fingers on the sensor. Data gathered during these studies provided an opportunity to study the effect of single and multiple fingers on authentication accuracy.

Analysis and Observations of the above study are all listed in section 3.4.

3.3 PoC 2-7 - Next Round of Field Studies

In order to further sharpen the focus of the study, UIDAI conducted additional rounds of PoCs wherein UIDAI standardized its requirements to not only biometric sensor and extractors but also standardized the underlying device (to be a generic laptop PC). To further standardize the study, UIDAI designed an authentication station, consisting of an authentication PoC client software deployed on laptops, connected to various biometric sensors via USB ports.

Locations

To ensure that residents from both urban and rural areas are covered under the PoC study, the PoC was carried out at the following locations covering more than 35,000 Aadhaar holders:

- Delhi
  - Mongolpuri
  - RK Puram
  - Nanda Nagari
- Jharkhand
  - Ratu Block Office
  - Pooriya Village
  - Parhepat Village
- Maharashtra
  - Thane
  - Naupada
  - Wagle
  - Kalwa
- Himachal Pradesh
  - Mandi town
  - Talhayar Village
  - Biholi Village
  - Baddi Village
  - Gumanu Village
  - Ner Chowk
  - Bhangrotu Village
  - Mahadev Village
  - Bhor Village
  - Kannaid Village
  - Sanyardi Village

3.3.1 Population Groups

The distribution was as follows:

Fingers	Image / Minutiae	Online / Buffered	Percentage
Single	Minutiae	Online	10%
Single	Image	Online	10%
Single	Minutiae	Buffered	10%
Two	Minutiae	Online	50%
Two	Minutiae	Buffered	10%
Five	Minutiae	Buffered	10%

The PoC software application ensured that when multiple fingers were to be used, the resident actually used different fingers. For online authentication, multiple attempts (up to 3) were permitted in cases where a single attempt did not succeed.

3.3.2 Sensor Participation

In this study sensor/extractor vendors were invited to participate, based on an EOI. Following an initial evaluation, a large number of sensor-extractor combinations were selected for the study, as summarized below:

• Participants	14
• OEMs	10
• Sensor Models	15
• Sensor Technologies	5
• Extractors	9
• Sensor- Extractor combinations	23

3.3.3 Field Setup

Authentication PoC centers were designed to resemble expected ground reality. No attempt was made to create an ideal situation. Some key considerations for setting up and managing the authentication stations were as follows:

- Except biometric sensors & extractors provided by EOI participants, UIDAI procured rest of the components and standardized them across all authentication PoC stations – such as laptops.
- Telecom data card used for network connection in order to send authentication requests to CIDR.
- For power supply, the electricity available in the PoC location was used. No UPS/Gen sets were deployed. In case of intermittent power cuts, the activities were carried out on the battery backup of the laptops. No major disruption was observed in the PoC exercise.
- Sensors were deployed across various stations to provide equal opportunity to all participating device technologies / OEMs, constrained by USB port availability.
- The key consideration was to get each resident to authenticate using as many authentication devices as possible.

Some of the deployed devices had challenges relating to scanning fingerprints, causing system crash etc. Considering the larger PoC objectives & crowd management issues, the devices causing problems and significant delays had to be disconnected temporarily. Overall all residents participating in the PoC2-7 authenticated on 6-12 different sensors.

3.4 PoC1-7 Observations

The learnings and observations from these studies are listed below:

1. **Viability of online authentication:** During the PoC, all the authentication transactions were carried out on existing mobile wireless networks. This assures the viability of online authentication using existing mobile networks in the country.
2. **Interoperability across sensors / extractors / matchers**: A variety of sensors were deployed in the PoC along with different extractor algorithms. These were found to work well with the three different matcher algorithms deployed at the backend providing true interoperability.
3. **For each resident, certain fingers provide a higher chance of authentication success:** Certain fingers were observed to provide better authentication accuracy due to good fingerprint ridges and hence better image quality. Every resident seems to have certain fingers that give better authentication results (reduced FRR). Therefore, to consistently achieve a lower FRR, tools and processes may be required to help residents identify these fingers.
4. **Multiple attempts of same finger further improve the chances of successful authentication:** In online authentication situations, providing multiple attempts of the same finger was seen to improve resident's chances of successful authentication. This seems to indicate the resident learns to place fingers appropriately over multiple attempts.
5. **FRR reduces with increased number of distinct fingers used**: The false reject rate decreases substantially when resident provides more fingers during authentication. FRR decreased when number of fingers was increased. Mechanisms may be required for capturing more distinct fingers if a resident is not able to authenticate with a single finger.
6. **Authentication accuracy is based on sensor/extractor combination:** There were differences in performance of different sensor-extractor combinations. This indicates a need to draw up specifications and deploy devices that give higher authentication accuracy.

7. **FRR is lower for high quality images (NFIQ 1 or 2):** The FRR is much lower when high quality (NFIQ scores 1 or 2[1]) fingerprint images are considered. Device and application ecosystem would need to be encouraged to fine-tune sensors/extractors for capturing higher quality fingerprint images.
8. **Effect of resident age on authentication accuracy**: Residents in 15-60 years group showed the best authentication accuracy.
9. **Immediate feedback to resident improves authentication**: The devices which were connected online and hence were able to give a result to the resident instantaneously (allowing the resident to conduct multiple attempts in case of failure) showed an improved accuracy when compared with buffered devices which did not provide any feedback to the resident during authentication.
10. **Buffered authentication is feasible**: Large number of transactions were carried out in the buffered mode as a part of the PoC design. Buffered transactions that had more distinct fingers gave much better accuracy results. Buffered authentication can be used during occasional network outage. Applications provisioning for buffered authentication may need to be designed to capture multiple distinct fingers.
11. **Visual feedback from sensors is important**: Certain sensors, which did not provide adequate feedback to the resident for placing / removing fingers, showed longer time to capture as compared to other sensors which did. Further, this occasionally caused the operator to assume a malfunction and these devices removed from the study.

3.5 PoC8 – Authentication Accuracy Study

Based on the PoCs 1-7 and its learnings, it became clear that a further study was needed to establish if it is possible to help residents identify fingers that have higher probability and then observe the resultant authentication accuracy if the residents used these identified fingers.

Such fingers that have higher probability of authenticating successfully are being referred to as the "best" fingers.

As part of PoC 8 study it was decided to create best finger detection (BFD) tool. It was also decided that the PoC application software needed to support the capture of multiple distinct fingers to study the effect of both multiple capture at frontend as well as fusion algorithm at the backend.

3.5.1 Best Finger Detection (BFD) process

The Best Finger for a resident is the one that, when selected for authentication, provides the highest chance of successful authentication for that resident.

The best finger to be used for authentication depends on the intrinsic qualities of the finger (ex. ridge formation, how worn out they are, cracked, etc.), as well as the quality of images captured during enrolment process and the authentication transaction.

3.5.2 Best Finger API

A separate API (application programming interface) was developed ***[UIDAI, BFD, 2012]*** and deployed on the client authentication device for the detection of the best finger. When BFD feature is implemented on an authentication device, residents can determine their best fingers, prior to authentication.

[1] NFIQ 1 and 2 are generally considered as good quality fingerprint images, NFIQ 3-5 are generally considered lower quality fingerprint images.

A complete set of fingerprint template, each individually labeled, along with their respective NFIQ (quality) scores, is sent to the server. Each fingerprint is then matched with the corresponding fingerprint template of the resident on the enrolment server. The fingers are then sorted on the resulting match scores – and a rank provided (rank1 – best finger, rank2 – second best finger). These results are then sent back to the client for resident to know his/her best fingers.

Further, the fingers are labeled Green, Yellow, or Red – depending on their suitability for single finger authentication. In addition, some residents could be determined to be not suitable for reliable fingerprint authentication.

3.5.3 Field set up

To carry out the study, two types of stations were created – a BFD station and an authentication station.

3.5.3.1 BFD Station

Each Best Finger Detection (BFD) station was setup with the following configuration:

1. One laptop with best finger detection client application developed by UIDAI
2. One barcode reader
3. Internet connection through USB device
4. One externally powered USB hub connected to one biometric sensors
5. An application built by UIDAI was deployed on these stations. This application helps to capture the 10 fingers of the resident and conduct best finger detection based on the BFD API to help residents find their best finger. The BFD process collects all fingerprints with a single finger sensor and attempt to match these with the enrolment data. This process is further refined by allowing the quality of each fingerprint to be improved through recaptures of resident fingerprints and using the image with the best quality - up to 3 attempts or till the NFIQ score for the finger captured is 1 or 2.
6. The response as to best fingers of the resident received from the server is printed and provided to the resident.

3.5.3.2 Authentication PoC Station

Each Authentication PoC station was setup with the following configuration:

1. One laptop with authentication PoC client application developed by UIDAI
2. One barcode reader
3. Internet connection through USB device
4. Two externally powered USB hubs connected to 6 different biometric sensors (6 sensors on each laptop)
5. An application was developed that captures the fingerprints from resident and conduct single and two finger authentication transactions.

3.5.3.3 Sensor Selection

The sensors used in the study were selected through an open process and required to integrate the capture / extractor software with the PoC client. All the sensors which were enlisted during the EOI process earlier were used during the proof of concept studies.

3.5.3.4 Participant Selection

In order to study the accuracy of fingerprints, experimental group consisting of residents who had received Aadhaar letters from villages around Nanjangud Tehsil (Mysore District, Karnataka) were invited to participate in the study. The study was conducted in the months of December 2011 and January 2012 and about 3500 residents participated.

This group was further categorized into 2 sub-groups on the basis of the BFD results.

1. **Best Finger Population** - Population group with one or more good fingers that can be used to study authentication accuracy using various sensor-extractor combinations
2. **Population group without any reported good fingers** - Biometrics of such residents to understand the root cause for this issue

The Rule of 30 ***[Wayman, 2002]*** states that "To be 90% confident that the true error rate is within ±30% of the observed error rate, there must be at least 30 errors". Since we are studying sensor/extractor up to 1% FRR we need to therefore include about 3000 residents in the study.

3.5.4 Field procedure

This section describes the field procedures followed in PoC8 which includes 2 steps:

- Best finger detection
- Authentication using best fingers

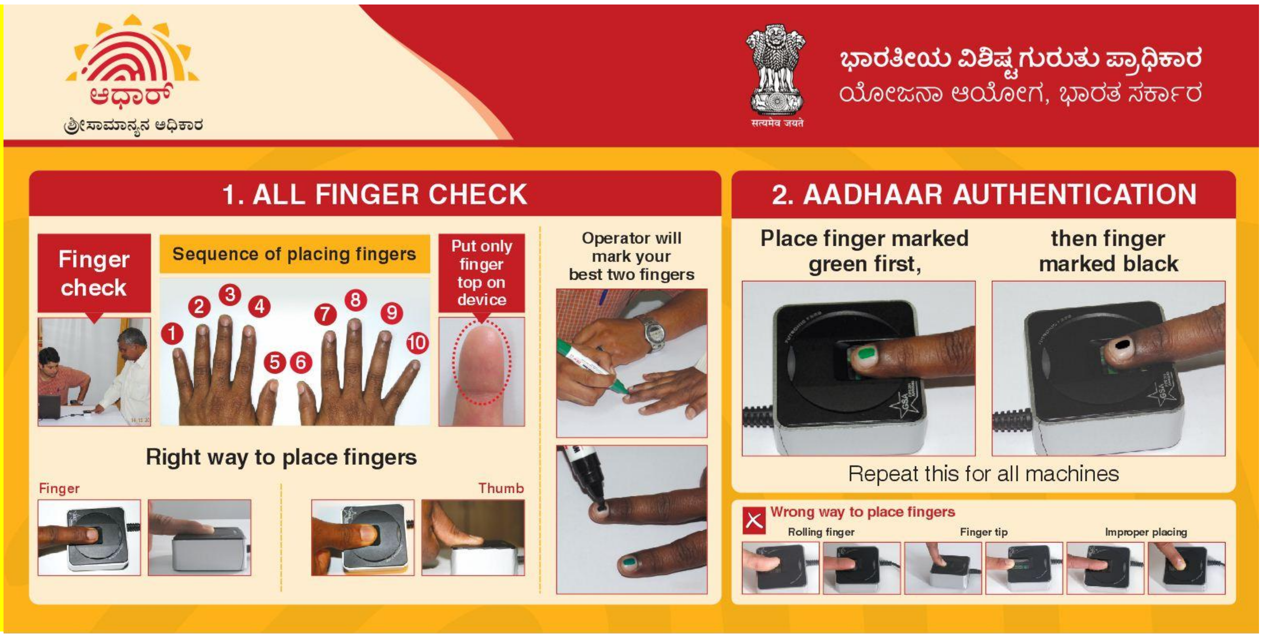

ಆಧಾರ್
ಶ್ರೀಸಾಮಾನ್ಯನ ಅಧಿಕಾರ
सत्यमेव जयते
ಭಾರತೀಯ ವಿಶಿಷ್ಟ ಗುರುತು ಪ್ರಾಧಿಕಾರ
ಯೋಜನಾ ಆಯೋಗ, ಭಾರತ ಸರ್ಕಾರ
1. ALL FINGER CHECK
Finger check
Sequence of placing fingers
1 2 3 4 5 6 7 8 9 10
Put only finger top on device
Operator will mark your best two fingers
Right way to place fingers
Finger
Thumb
2. AADHAAR AUTHENTICATION
Place finger marked green first,
then finger marked black
Repeat this for all machines
Wrong way to place fingers
Rolling finger
Finger tip
Improper placing

Figure 3: Field procedure for BFD and authentication

PoC8 field procedure details comprised of following steps.

1. Resident presents his/her Aadhaar letter (containing Aadhaar number).
2. Aadhaar credentials of the resident are verified by checking the photo on the Aadhaar letter.
3. Resident proceeds to the BFD station and uses the BFD tool. All fingerprints are captured and sent to the CIDR through the BFD API. The response from the BFD API is printed and provided to the resident to know their best fingers.
4. In the event that the resident does not possess even 1 good finger for authentication, they are informed of the same.
5. Residents after completing BFD process, proceed to the Authentication PoC station for the accuracy test. For ease of field management, the best 2 fingers were marked with coloured felt pens (Green for the 1st best finger and Blue for 2nd best finger)

6. Resident's best finger and second best finger are captured in that order on each of the sensors.
    a. When the NFIQ scores are between 3-5, up to three capture attempts were conducted to improve the NFIQ scores to 1-2 if possible.
    b. Similarly, each of the captured fingers is compared with each other to ensure resident is presenting two separate fingers and not the same finger twice.
    c. Minutiae count for the captured fingers are also presented to the operator. In cases where the number of minutiae was found to be very low, operator had option to rescan the finger.
7. After completion of the fingerprint capture process, three authentication transactions were initiated in the following order. Each of the fingerprints was separately sent to CIDR using the Aadhaar Authentication API version 1.5. The result of the transaction (Yes/No) was displayed for further action.
    a. Single finger authentication transaction using the first best finger.
    b. Single finger authentication transaction using the second best finger.
    c. Packed two finger authentication transaction using both first and second fingers.
8. If any one of the two single finger authentications failed, the process of capture and authentication (step 5 and 6) was repeated up to three times.

The above process was repeated for each of the authentication devices deployed during the study.

3.5.5 Detection Error Tradeoff (DET or ROC) curve determination

All biometric algorithms / SDKs used for authentication purpose provide a matching score, which represents the probability of a false match between the provided biometrics and the previously captured biometrics. When this score is higher than a specified threshold, the system responds with a "yes" response.

False Reject Rate

All data collected from the field included an operator set flag for the expected response (the Ground Truth). Based on this, all 'true' authentication transactions were rerun in the lab and the matching scores recorded. This allowed capture of the false reject rate for a particular threshold.

False Accept Rate

Expected false requests were created by pairing biometric data collected from the field with an Aadhaar number other than the original Aadhaar holder. A large number of these requests were rerun and matching scores recorded. This allowed capture of the false accept rate for several thresholds (in between 30-70). As many false requests as necessary were created to provide statistically significant results.

DET Curve

The false accept rate and false reject rate for a particular threshold were paired and the resulting curve plotted. For standardization and easier readability, the FRR is plotted on a linear scale, while the FAR is plotted on a logarithmic scale.

4 Best Finger Detection (BFD) Results

This section summarizes the following results from the BFD study:

- Demographics of the BFD study participants
- Resident authentication readiness feedback from the BFD process
- Finger position analysis of the BFD results

4.1 Demographics of BFD Study Participants

The demographic profile of participants in the BFD study was compared with the profile of residents enrolled in Aadhaar – both nationally as well as within Mysore district to ensure that there is no significant bias in the sample. The comparison was done on the basis of participant age bands, as well as gender.

It was found that children in 5-15 years range were under represented in the sample compared to overall Aadhaar enrolment statistics, while senior residents (60+ years) were slightly over represented. Similarly, it was found that females were over represented in the study as compared to males.

The following charts show the Age and Gender distribution of all Aadhaar holders nationwide, in Mysore district and all participants in the BFD study.

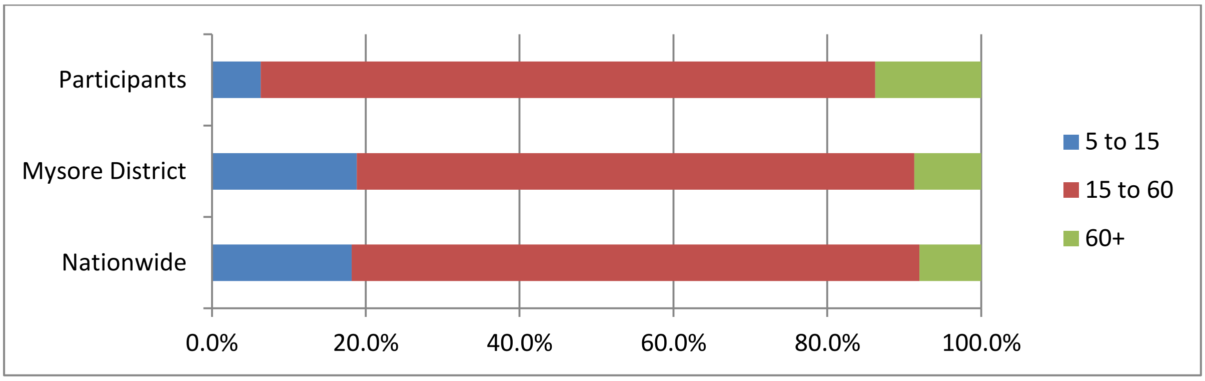


Figure 4: Age distribution of participants in study compared to Aadhaar enrolment

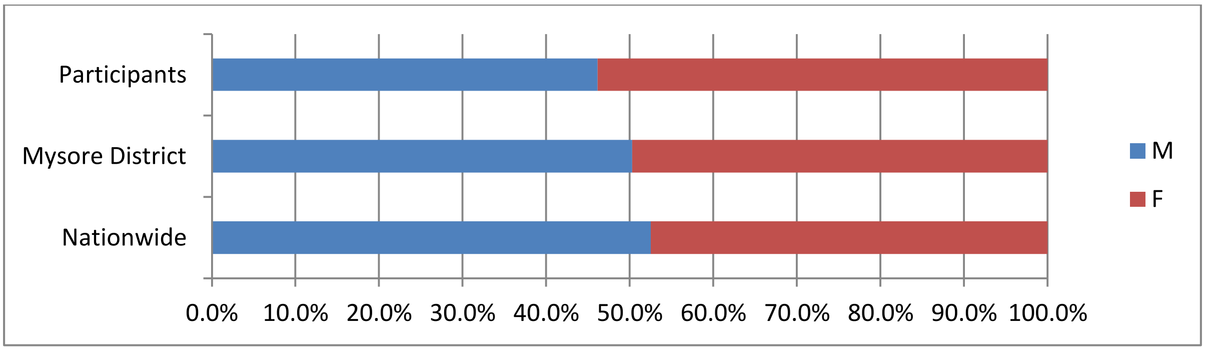


Figure 5: Gender distribution of participants in study compared to Aadhaar enrolment

4.2 Resident Authentication readiness using BFD

Of the residents who participated in BFD, over 93.63% of residents possessed at least one green finger (best finger), i.e., they are likely to authenticate successfully with a single finger. Another

4.50% of residents were found to have two yellow fingers, i.e., they are likely to authenticate successfully using two fingers. Finally 1.87% of residents participating in the study were found to have fingerprint quality not sufficient for fingerprint authentication. They were not included in the further authentication tests.

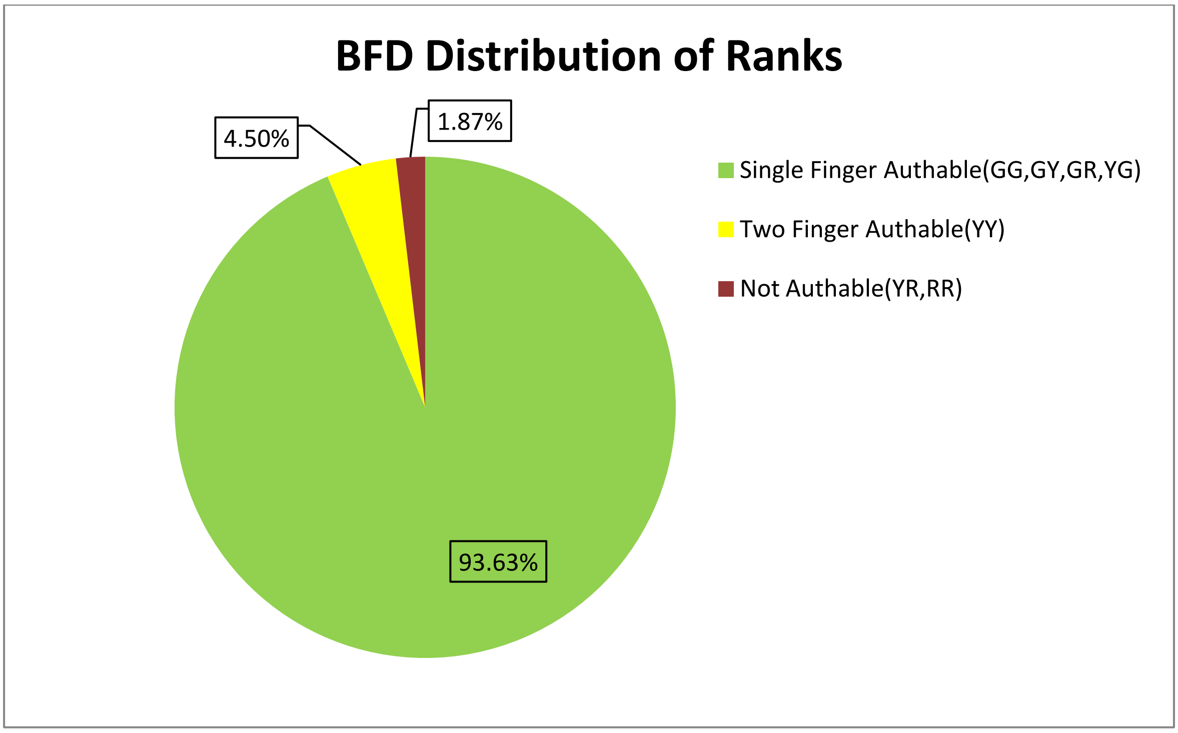


Figure 6: Figure Resident authentication readiness

Out of the 1.87% of the residents, 89.8% (1.68% of all participants) was identified as having intrinsically poor quality fingerprints. For the remaining 10.2% (0.19% of all participants), although they had good quality fingers, the quality of fingerprint captured during enrolment was poor. Hence by updating their biometrics, they can successfully participate in authentication process.

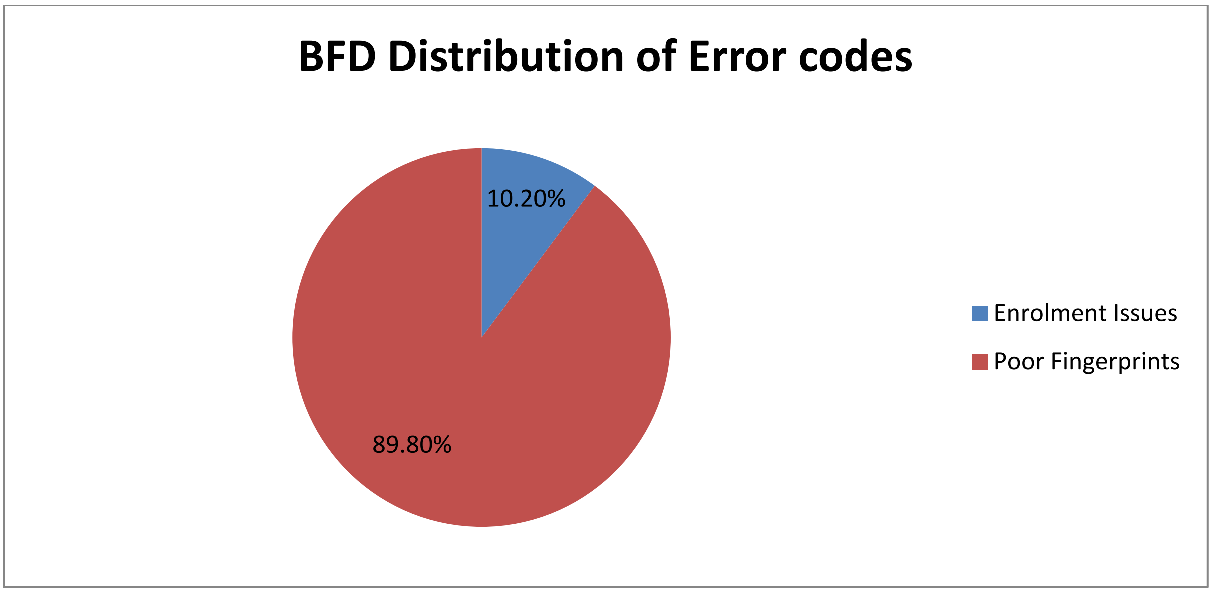


Figure 7: Reasons for BFD failure

4.3 Distribution of BFD fingers by finger position

The finger position of the best finger (Rank 1) and 2nd best finger (Rank 2) obtained by using the BFD process was analysed. As expected, the index fingers and thumbs were identified as the best finger in most of the cases. However, almost 20% of residents had one of the other fingers as their best finger.

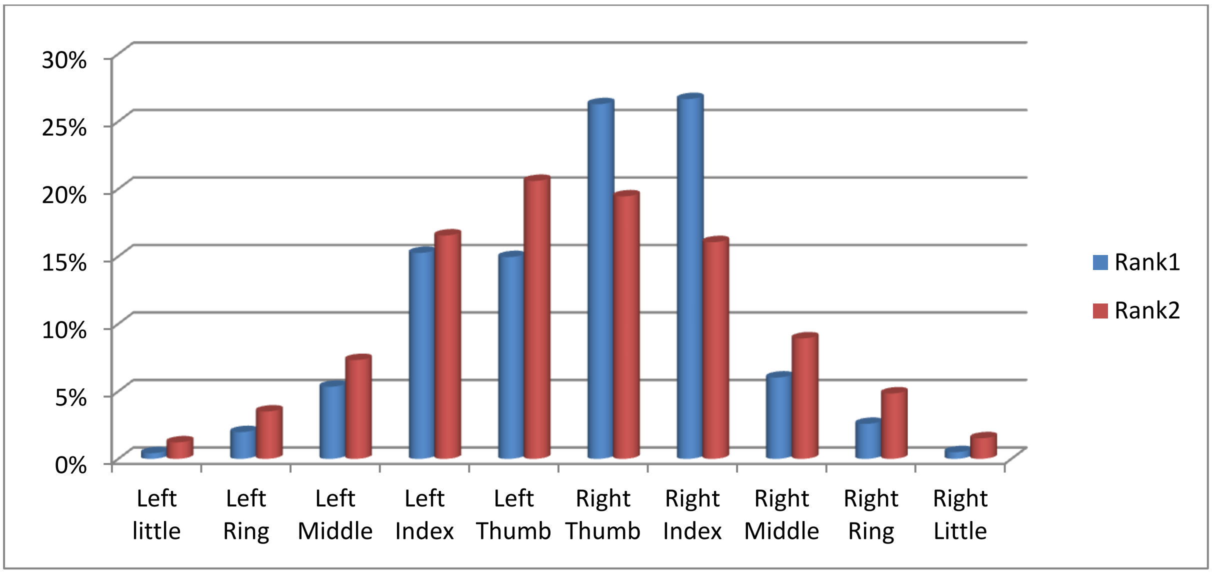


Figure 8: Best finger distribution by position (Rank 1 & Rank 2)

4.4 BFD result stability

Anecdotal evidence shows that there is slight variation of the best finger determined during the BFD process depending upon the sensor used and also over time. However, a formal study of BFD variation by sensor and over time was beyond the scope of the current study.

Best Finger Detection (BFD) - Highlights

- *93.6% of people can reliably authenticate with a single finger*
- *4.6% of people can additionally reliably authenticate with minimum two fingers*
- *1.9% of people cannot reliably authenticate using fingerprints*

5 Fingerprint Authentication Concepts

Prior to presenting authentication accuracy results using the fingers identified in the BFD studies, some concepts are defined for clarity.

5.1 Labeled vs. Unlabeled Matching

Unlabeled matching: The frontend authentication device does not provide the position/label of the finger presented to the authentication server backend and the backend matches it with all the 10 fingers of the given resident. This method is referred to as unlabeled matching or 1:10 matching.

Labeled matching: The frontend authentication device provides the position/label of the finger presented (e.g. Right Index) to the authentication server backend and the backend matches it with exactly that finger of the resident. This method is referred to as labeled matching or 1:1 matching.

Since unlabeled matching involves multiple matching operations, it results in more false matches at the same threshold. Hence, such a system needs to be operated at a higher threshold to maintain the target FAR, which results in a higher FRR as compared to a system based on labeled matching. However, a labeled matching system depends on correct labeling by the operator, which may introduce human error and increase the reject rate as well as require additional operator training.

DET curves have been computed for both the above scenarios and can be used to make policy decisions in this regard. Based on these policies, the thresholds required to achieve the desired operating points can be determined.

5.2 Fusion Algorithms

Fusion algorithms are a method of combining multiple biometrics to improve the accuracy of biometric authentication. In the context of this study, fusion algorithms were used to compute the score for two finger authentication, where 2 distinct fingers were presented. The matching scores were combined. The resultant DET curve is the basis to choose an appropriate threshold for maintaining the required FAR.

5.3 Accuracy results from BFD test

Some accuracy results have been derived directly from the BFD test. Since all ten finger scores were obtained during the BFD test, it is possible to compare various finger positions. However, it is important to note that the BFD test was performed only on a single sensor and the BFD results include ALL residents including those who did not find any finger suitable for authentication.

5.4 Accuracy results from Authentication test

Other accuracy results have been derived from the Authentication test. Only residents who have at least one green or two yellow fingers participated in the Authentication test.

After the best finger (Rank1) and 2nd best (Rank2) finger have been determined using BFD, residents use these fingers to authenticate on 26 of sensor/extractor combinations. Unless stated otherwise the results below have been derived from the combined response of 14 “good” sensor/extractor combinations which had an FRR below the average FRR of all sensors for a single finger authentication at an FAR of 1e-4. This was done to eliminate sensor/extractor combinations which were outliers, while providing results relevant to a heterogeneous, interoperable environment.

5.5 Back End Matcher Tuning

All results have been derived using one of the three backend SDKs available to UIDAI. Potential improvements in accuracy could be achieved by tuning the backend SDKs.

6 PoC8 - Single Finger Authentication

This section seeks to answer the following questions in the context of authenticating with a single finger:

- Is the BFD effective? How does a 'named' (e.g. Right Index) finger compare with the 'Best' finger identified by the BFD process?
- What is the effect of multiple attempts of the best finger?
- What is the effect of labeled matching (1:1)? How does this compare to Unlabeled (1:10) matching?

6.1 BFD effectiveness: "Named Finger" vs. "Best finger"

One of the objectives of the BFD study was to identify if the best finger would provide better accuracy (lower FRR at the same FAR) than a "named" finger. Literature ***[NISTIR 7346]*** shows that the right index and right thumbs are the most common (and effective) fingers used for fingerprint authentication. It must also be noted that 55% of the participants had either of these fingers as their best fingers. Additionally, if BFD worked as expected, the best finger must provide a better accuracy than the 2nd best.

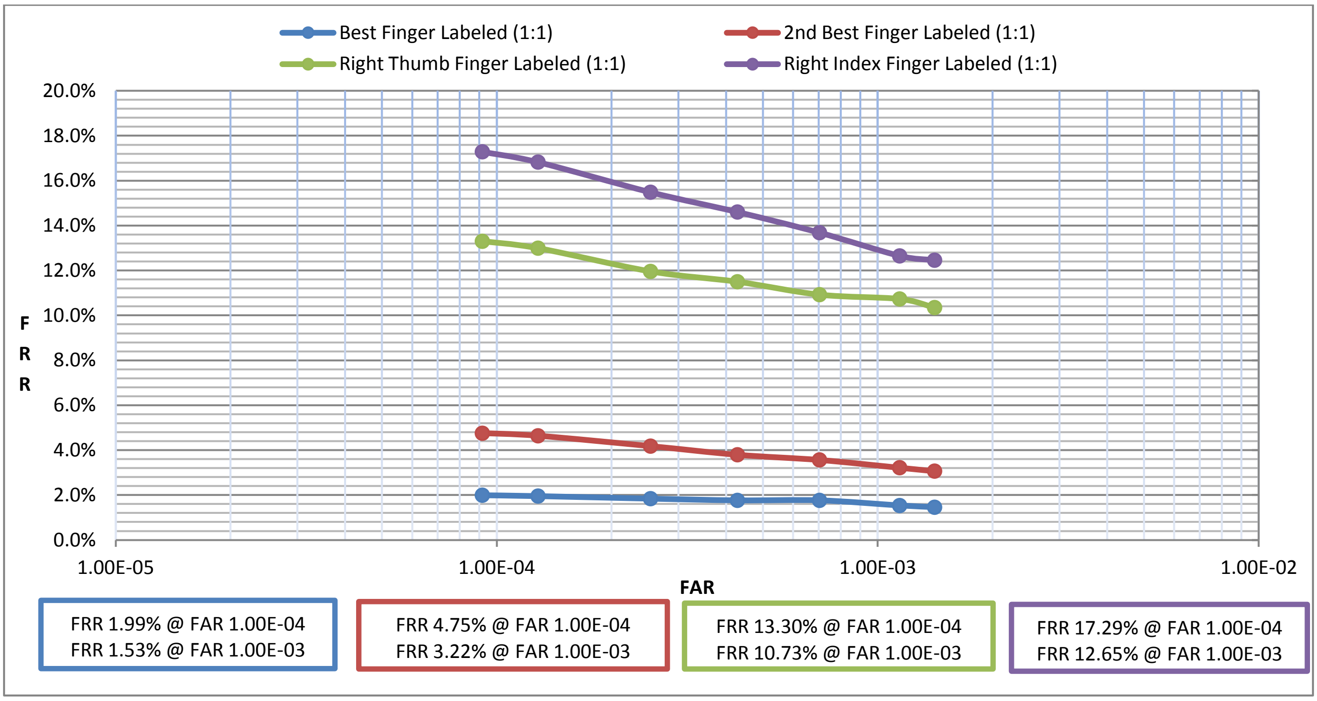


Figure 9: Comparing Authentication accuracy achieved using different fingers.

At an FAR of 1e-4, the following FRRs are observed:

Best Finger	1.99%
2nd Best Finger	4.75%
Right Thumb	13.30%
Right Index	17.29%

This demonstrates that the best finger and the 2nd best finger are indeed better than the named fingers and that the BFD tool / process is effective in identifying the best fingers to use for authentication.

6.2 Single Attempt vs. Multiple Attempts, Labeled vs. Unlabeled

Another objective was to study whether using multiple attempts of the same (best) finger would improve the accuracy of results. Other studies ***[NISTIR 7346], [NIST, 2006]*** have shown that multiple impressions of the same finger results in the improvement of the FRR.

Since the Aadhaar authentication system provides for labeled and unlabeled matching, it was important to understand the implications of these choices on accuracy.

The DET curves below compare the accuracy obtained from the system using the best finger for the 1st attempt only and up to 3 attempts. Further, comparisons are also studied for using labeled and unlabeled matching options using 14 different sensor/extractor combinations.

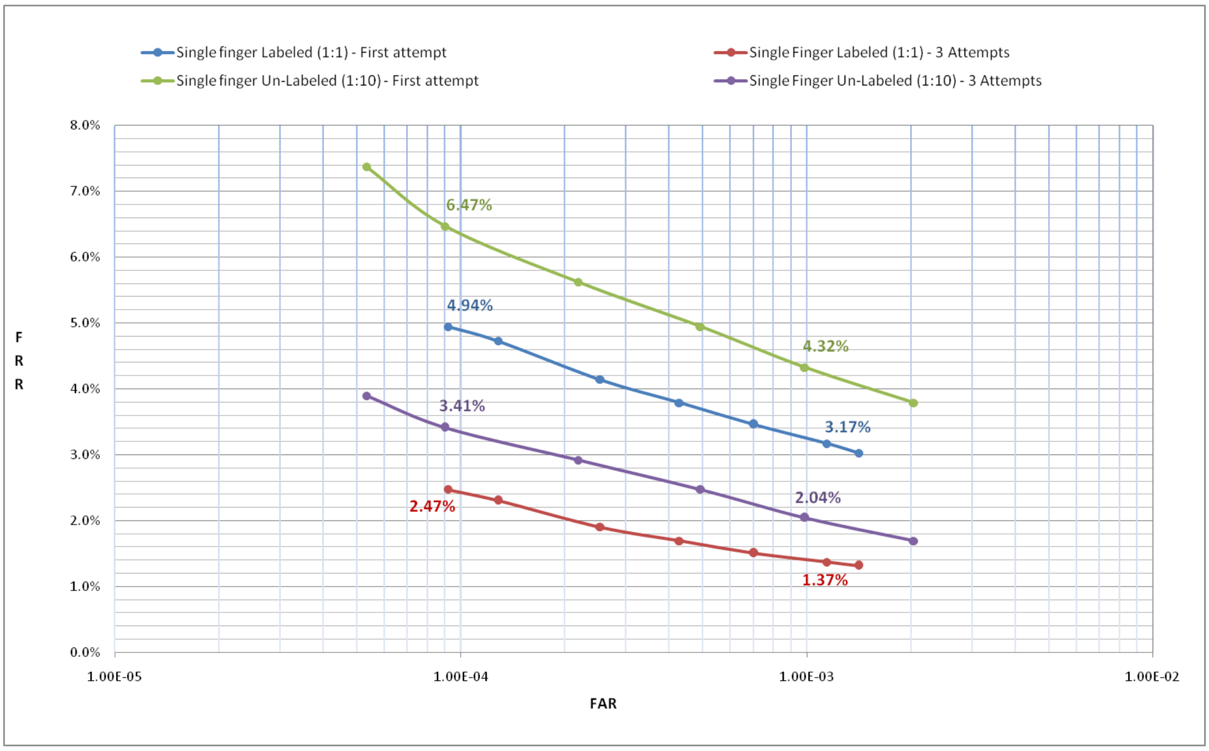


Figure 10: Single finger 1st attempt vs. 3 attempts for labeled & unlabeled matching

At an FAR of 1e-4, the following FRRs are observed:

	Unlabeled	Labeled
1st Attempt	6.47%	4.94%
Up to 3 Attempts	3.41%	2.47%

As expected, 3 attempts result in a large reduction (halving) of the FRR. Similarly, labelling results in an improvement in the FRR.

Single Finger Authentication – Highlights

- *93.5% residents can authenticate in the first attempt using their best finger and 96.5% can authenticate using their best finger in up to 3 attempts*
- *Using Best Finger for authentication, FRR is much lower (up to 6 times) than using any specific finger*
- *Multiple attempts help to improve the accuracy (reduce FRR by up to 2 times) of single finger authentication*

7 PoC8 - Two Finger Authentication

Two best fingers fusion has been proposed as a possible way to improve the "inclusiveness" of authentication, allowing a larger percentage of the population to participate in fingerprint authentication without compromising the security of the system. Many studies ***[[NISTIR 7346], [NIST, 2006], [Jain, 1999]]*** show that the two fingers fusion can significantly improve FRR at the same FAR levels.

7.1 Impact of 2 Finger Fusion

The impact of two fingers fusion on the accuracy of the system has been studied. A simple sum of scores based fusion scheme was used. In biometric literature this is considered to be effective and requires no training compared to more complex fusion schemes.

During field testing in authentication accuracy study, the fusion scheme was implemented as part of the testing in the field, i.e. two fingers were captured and were sent together in a single authentication transaction.

The DET curves compare the accuracy of up to three attempts of the best finger, with up to three attempts of fusion of the best two fingers. The curves have been plotted both for Unlabeled (1:10) and Labeled (1:1) matching.

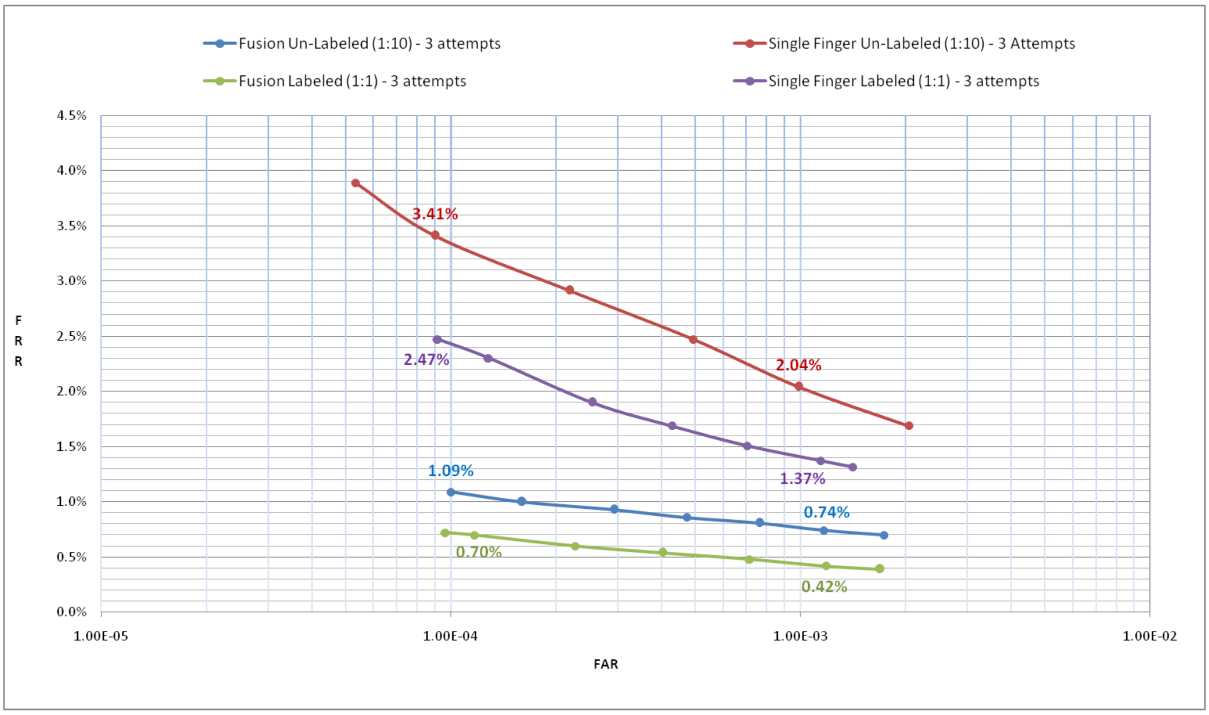


Figure 11: Up to 3 attempts, Single finger vs. two fingers Fusion, unlabeled vs. labeled match

The DET curves show a large reduction in FRR across all FAR values. At an FAR of 1e-4, the following FRRs are observed:

	Unlabeled	Labeled
Single Finger	3.41%	2.47%
Two Finger Fusion	1.09%	0.70%

Clearly, there is a large reduction in the FRR for both labeled and unlabeled matching when a second finger is presented and the scores are fused.

Note that the matching score threshold used for achieving the **same FAR** for single finger and fusion is different.

7.2 Ability of fusion to help people who cannot use single finger

In addition to reducing the overall FRR, 2 finger fusion has the added advantage of including residents who would otherwise not be reliably authenticated with a single finger. To compare the benefits of fusion, DET curves for this set of residents were plotted across 14 sensor/extractor combinations. As expected there is a big improvement in inclusion for such residents using 2 best fingers fusion. For Unlabeled (1:10) matching, an FRR of 28.54% was achieved for the single finger case, while an FRR of 12.55% was achieved for the 2 finger fusion at FAR of 1e-4.

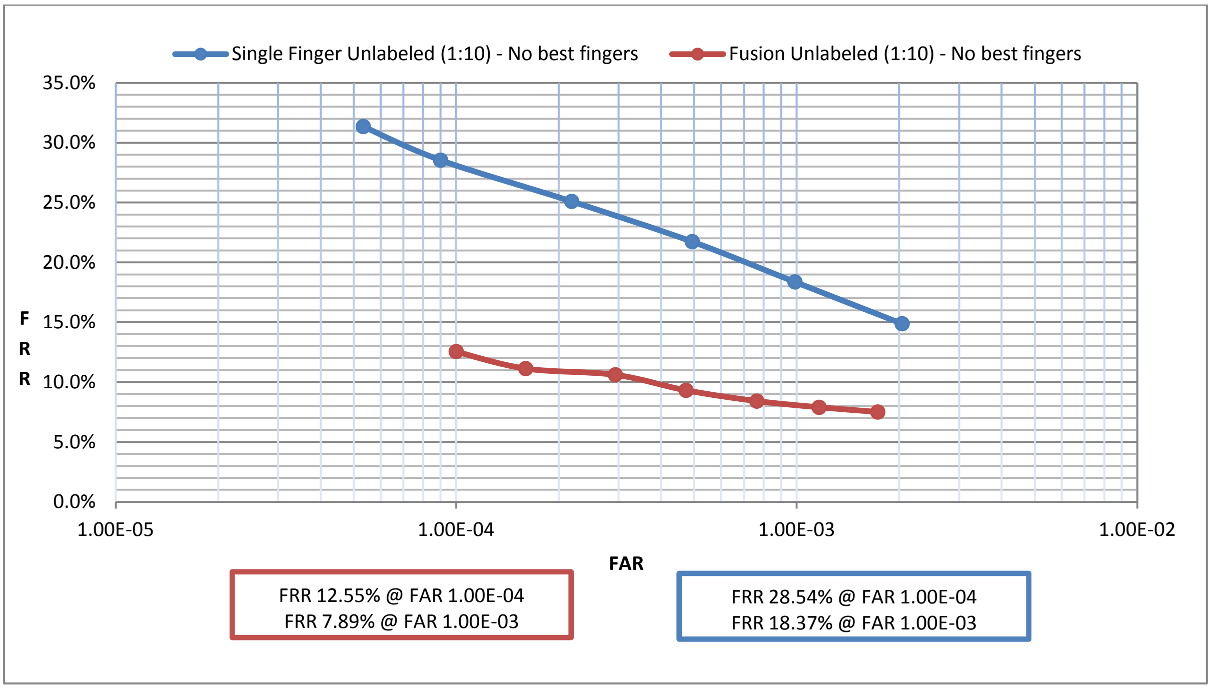


Figure 12: Up to 3 attempts [residents with NO best fingers] unlabeled match [1:10]: single finger vs. 2 finger fusion

Two Finger Authentications – Highlights

- *Two best finger fusion can help to reduce the FRR to 1.09% for Unlabeled (1:10) matching, and 0.7% for Labeled (1:1) matching without impacting the FAR*
- *As expected, two best finger fusion shows large reduction in FRR for residents who cannot reliably authenticate using one finger*

8 PoC8 – Impact of Sensor Extractor combination

Previous PoC studies have highlighted the impact of devices (sensor / extractor combination) on the accuracy. In this section, the impact of the various devices has been examined.

8.1 Device Performance

The following table captures the performance variation for the various devices.

Device	**Area** (pixel)	**Area** (mm)	**FAP** Classification	**MINEX** Compliance	FRR **Single Finger** 3 Attempts Unlabeled(1:10)		FRR **Fusion** 3 Attempts Unlabeled(1:10)	
					@FAR of 1e-3	@FAR of 1e-4	@FAR of 1e-3	@FAR of 1e-4
1	320 X 480	16 x 24	FAP 20	Yes	1.05%	1.84%	0.39%	0.63%
2	320 X 480	16 x 24	FAP 20	No	1.45%	2.14%	0.82%	1.03%
3	320 X 480	16 x 24	FAP 20	Yes	1.14%	2.23%	0.46%	0.70%
4	416 X 416	23 x 23	FAP 20	Yes	1.33%	2.46%	0.55%	0.68%
5	352 X 544	18 x 28	FAP 20	Yes	1.33%	2.49%	0.28%	0.56%
6	352 X 544	18 x 28	FAP 20	Yes	1.37%	2.52%	0.34%	0.42%
7	320 X 480	16 x 24	FAP 20	Yes	1.89%	3.43%	0.84%	1.09%
8	320 X 480	16 x 24	FAP 20	Yes	2.20%	3.48%	0.68%	1.06%
9	352 X 544	18 x 28	FAP 20	Yes	2.04%	4.01%	0.36%	0.57%
10	256 X 400	14 x 22	FAP 10	Yes	2.45%	4.57%	0.83%	1.24%
11	320 X 480	19 X 27	FAP 20	Yes	2.88%	5.18%	1.15%	1.75%
12	256 X 360	13 X 18	FAP 10	Yes	3.30%	5.46%	1.25%	1.81%
13	256 X 360	13 X 18	FAP 10	Yes	3.33%	5.58%	1.04%	1.71%
14	260 X 340	16 x 19	FAP 10	Yes	4.42%	6.17%	1.17%	1.78%
15	258 X 336	16 x 18	FAP 10	Yes	3.07%	6.50%	1.11%	2.22%
16	258 X 336	16 x 18	FAP 10	Yes	4.58%	6.51%	1.09%	2.28%
17	256 X 360	13 X 18	FAP 10	Yes	4.40%	6.61%	2.01%	3.08%
18	256 X 360	13 X 18	FAP 10	Yes	5.17%	7.57%	2.35%	3.17%
19	256 X 324	13 X 16	FAP 10	No	5.41%	7.84%	2.46%	3.38%
20	288 X 320	16 x 18	FAP 10	Yes	6.39%	8.55%	3.27%	4.41%
21	288 x 352	15 x 18	FAP 10	Yes	5.99%	8.76%	5.58%	6.66%
22	320 X 480	19 X 27	FAP 20	No	6.92%	9.59%	3.98%	5.38%
23	288 X 320	16 x 18	FAP 10	Yes	9.17%	12.77%	3.52%	4.87%
24	280 X 352	14 x 17	FAP 10	Yes	9.80%	12.97%	3.26%	5.29%
25	280 X 352	14 x 17	FAP 10	Yes	12.14%	18.97%	5.46%	9.65%
26	280 X 352	14 x 17	FAP 10	Yes	16.25%	22.81%	6.08%	8.97%

Figure 13: Single finger - 3 attempts accuracy by device

There is a large variation in performance by device. Among the 26 devices studies, the single finger unlabeled FRR for up to 3 attempts varied from 2% to 23%! The best set of devices did much better than the good set of devices, which did much better than the rest of devices.

Using the 2 finger fusion score, the scenario is still similar, the overall FRR varies from 0.4% to 9.7%:

	No. of Devices	**FRR Range (%)**	**Average FRR (%)**
Best	9	0.4 – 1.1	0.75
Average	5	1.2 – 1.8	1.66
Rest	12	2.2 – 9.7	4.95

8.2 Impact of Sensor Size

There appears to be a correlation between sensor size (as classified by FAP) and the performance. The smaller sensors have capture area of 13 X 16 mm. The larger sensors have capture area of 15 X 20 mm. It was observed that smaller capture area combined with incorrect placement produced insufficient common area between the enrolment image and authentication image. This can be visually seen below.

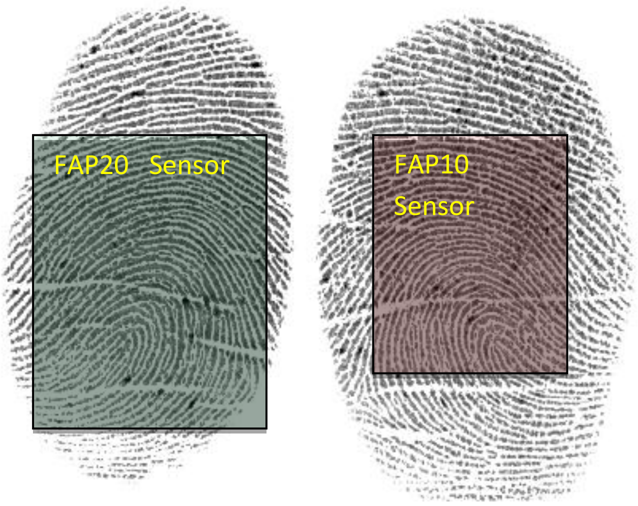


Figure 14: Two rectangles show the size of sensors and resulting area that is missed

Using fingerprint sensors with larger capture area provides better accuracy. This can be demonstrated by comparing the DET curves for devices which are FAP20 / FAP10 classified. To separate the effect of the extractor, only MINEX certified extractors are used for this chart.

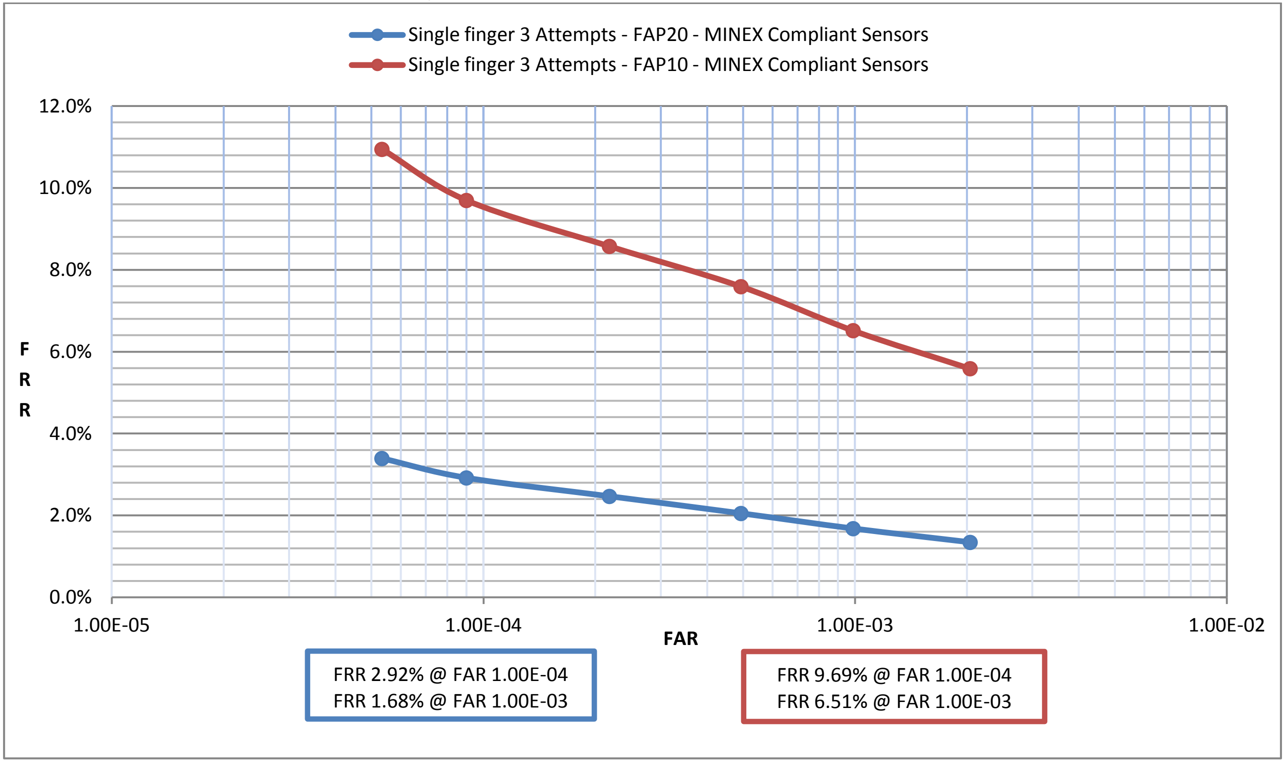


Figure 15: FAP20 and FAP10 sensors using MINEX compliant extractors - single finger (3 attempts)

Similarly, with fusion 3 attempts, FAP20 sensors using MINEX compliant extractors demonstrated 0.84% FRR whereas FAP10 sensors that used MINEX compliant extractor demonstrated 3.95% FRR at FAR of 1e-4.

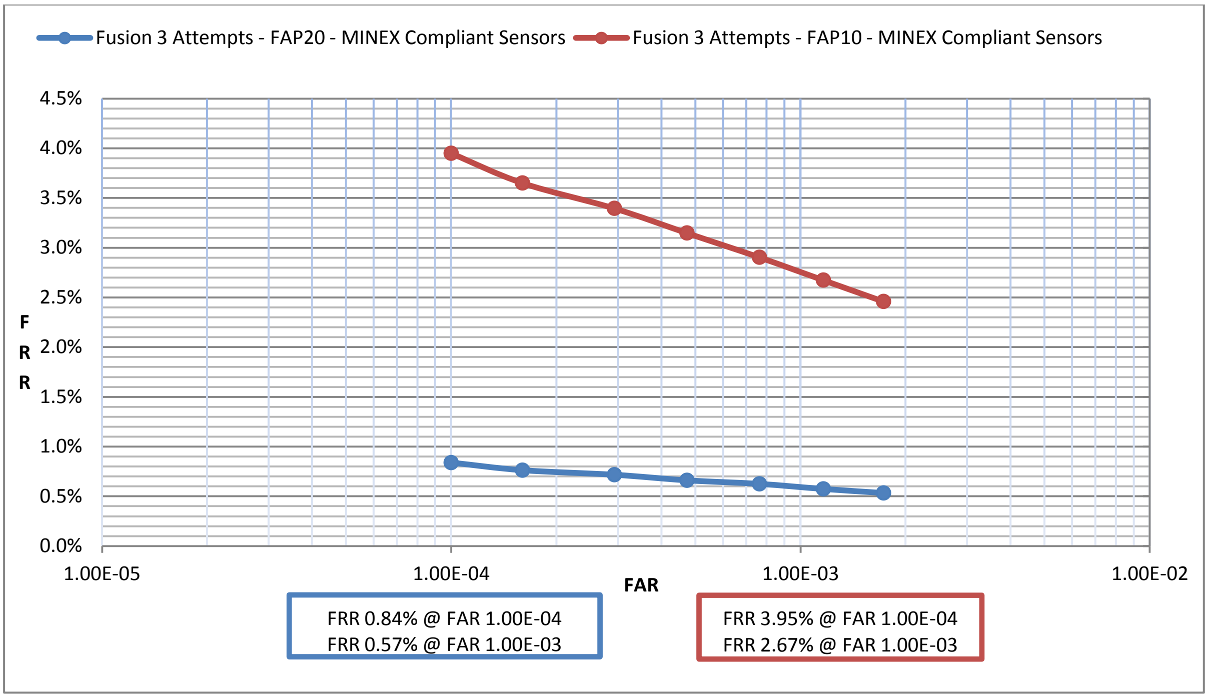


Figure 16: FAP20 and FAP10 sensors using MINEX compliant extractors – Fusion (3 Attempts)

Device Impact – Highlights

- *Larger sensors (FAP20 compliant) provided better accuracy than smaller sensors (FAP10 compliant)*

9 PoC8 - Other findings

9.1 Image vs. Template Comparison

Aadhaar authentication provides the option to send a fingerprint image from the field instead of the extracted templates. While the templates extracted on the field are from different extractors (bundled with the device), the matching done on the server uses the same SDK that was used to extract the enrolment templates. While the image is certainly much larger in size than the template, it is expected to provide better accuracies.

Since it is important to understand this tradeoff, a study was conducted using the images and templates stored by the device in the field. These were replayed against the server and the resulting DET curves generated.

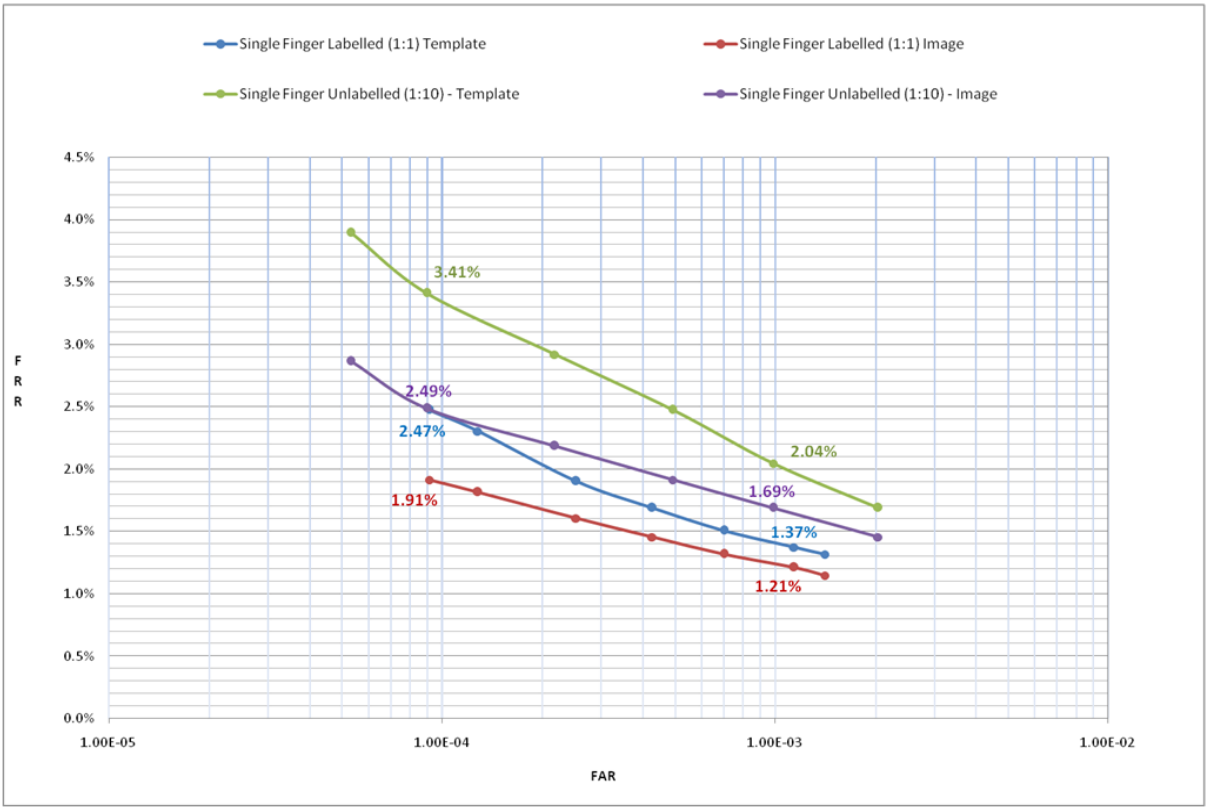


Figure 17: Up to 3 attempts single finger labeled vs. unlabeled, Image vs. Template

The DET curves show an improvement in FRR across all FAR values for both labeled and unlabeled matching. At an FAR of 1e-4, the following FRRs are observed:

	Unlabeled	Labeled
Template	3.41%	2.47%
Image	2.49%	1.91%

9.2 Impact of Resident Age

The impact of age on authentication accuracy was studied. The computed DET curves compare the accuracy of matching for people in the age group 5-15, 15-60 and 60+ years. As expected the FRR rates are the lowest for a given FRR in the 15-60 years age groups and is 0.79% for an FAR of 1e-4 when using 2 best finger fusion and an unlabeled (1:10) matching strategy.

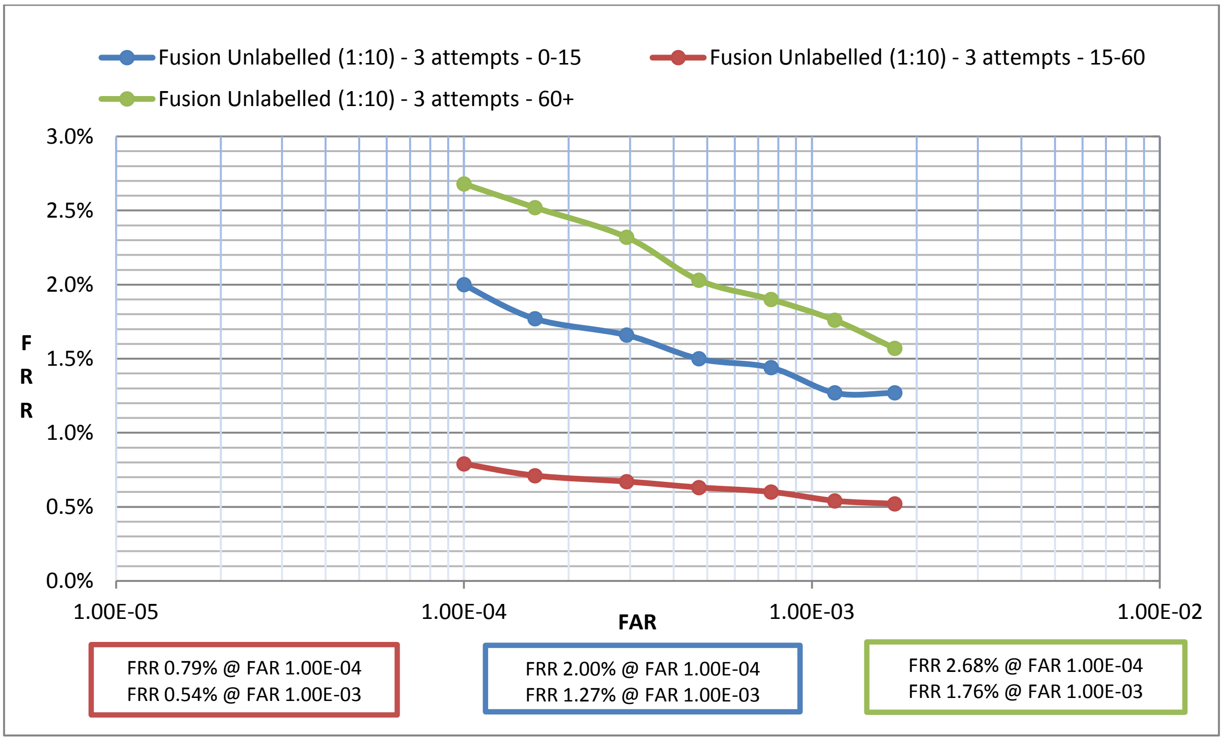


Figure 18: Up to 3 attempts fusion Unlabeled (1:10) compared for different age groups

9.3 Adaptive Thresholds

As described in section 5.1, unlabeled matching involves multiple matching operations and results in more false matches at a given matching score threshold. Hence, such a system must be operated at a higher matching score threshold to maintain the target FAR, which results in a higher FRR as compared to a system based on labeled matching. This is demonstrated explicitly in section 6.2 where the labeled finger matching scheme is seen achieving lower FRR at a given FAR compared an unlabeled scheme.

However, a labeled matching scheme depends on correct labeling of the finger by an operator. This may introduce human error and increase the rejection rate due to incorrect labeling in the field. In addition, operator may need training in order to correctly label the finger.An adaptive threshold scheme is being proposed which combines the accuracy advantage of a labeled matching scheme while retaining the convenience of an unlabeled matching scheme. In this scheme, a label hint is required during the matching operation. Matching is conducted using two different thresholds, a lower threshold while matching against finger with label hint and a higher threshold while matching against the remaining nine fingers.

Label hint of the finger used during the authentication transaction can be determined using two methods:

1. It can be provided explicitly by the resident or operator during authentication.
2. It can also be derived from the backend by assuming that the resident uses the best finger during the authentication. This approach assumes that resident has gone through the BFD process.

During the matching process:

- A lower matching score threshold is applied for matching the finger with label hint
    - This enables the minimization of FRR, if the label hint is correct.
- A higher threshold is applied for matching other nine fingers
    - The enables the resident to match at a higher threshold even if the label hint is incorrect. The usage of a higher threshold prevents any increase in FAR.

Assuming the label hint is correct most of the time, the adaptive threshold scheme can achieve lower FRR without compromising either FAR or the convenience of an "unlabeled" system.

The following charts show that the adaptive scheme provides an accuracy that is almost as good as the labeled scheme. We see that the adaptive threshold scheme without labeling can achieve an FRR of 2.75% while the labeled scheme has an FRR of 2.47% and the unlabeled scheme has an FRR of 3.41% at an FAR of 1e-4.

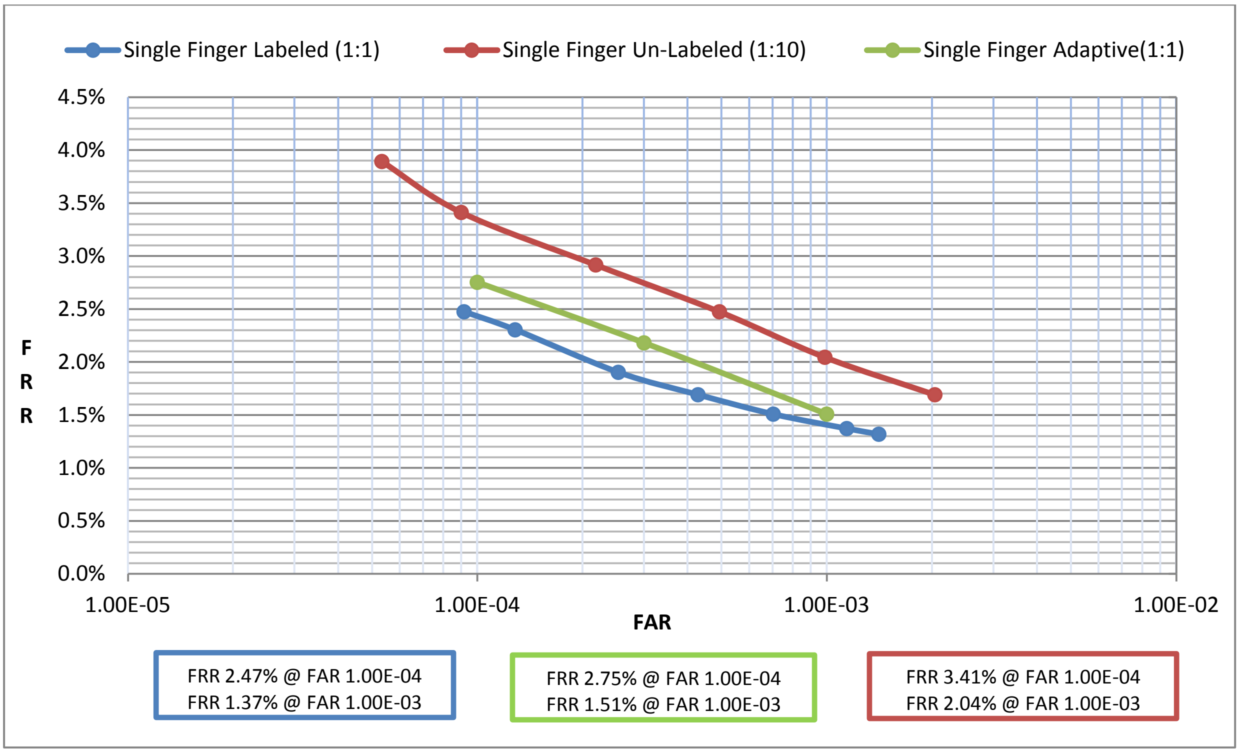
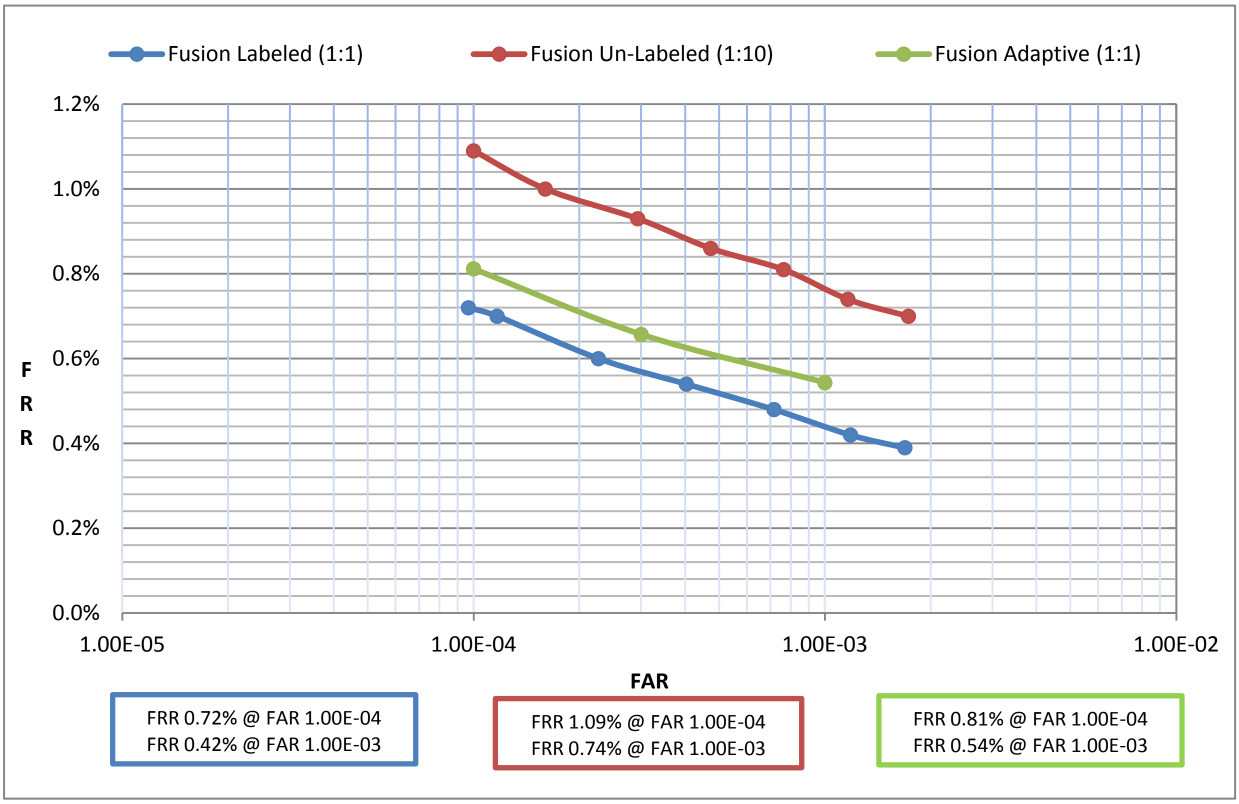


Figure 19: Single finger authentication labeled (1:1), Unlabeled (1:10) and adaptive - 3 attempts

Similarly, for two finger fusion, from the DET curves we see that the adaptive threshold scheme without labeling can achieve an FRR of 0.81% while the labeled scheme has an FRR of 0.72% and the unlabeled scheme has an FRR of 1.09% at an FAR of 1e-4.



FRR 0.72% @ FAR 1.00E-04
FRR 0.42% @ FAR 1.00E-03

FRR 1.09% @ FAR 1.00E-04
FRR 0.74% @ FAR 1.00E-03

FRR 0.81% @ FAR 1.00E-04
FRR 0.54% @ FAR 1.00E-03

Figure 20: Two finger fusion authentication with Labeled (1:1), Unlabeled (1:10) and Adaptive - 3 attempts

Other Findings – Highlights

- *Using images instead of templates for authentication showed some improvement in accuracy especially at lower FAR values*
- *Residents in 15-60 years age group showed the best authentication accuracy. Senior residents (60+) had the highest rejection rates.*
- *Using adaptive thresholds, further reduction in FRR is possible while maintaining the required FAR and reducing operator efforts required for labeling.*
- *Enrolment NFIQ is poor indicator to determine the best finger.*

10 Authentication System Performance

UIDAI conducted internal performance tests for authentication within the UIDAI benchmark environment. Goal of this test was to ensure sub-second response time is achievable even under the load and these servers can continue to perform over a long period of time without degradation. Linear scalability of the entire authentication system was studied in detail.

Performance test covered all key aspects of authentication and covered the following:

- Pure demographic matching scenarios
- Biometric and demographic matching scenarios
- OTP usage scenarios

This section covers the details on this performance test and provides the conclusions and readiness in terms of scaling up Aadhaar Authentication service.

Aadhaar Authentication performance test environment had a total of 15 blade servers (each server being x86 Linux dual CPU 6-core servers) including database servers, biometric matching servers, messaging server, caching servers and audit logging servers. Actual matching servers (application servers) were just 4 out of this 15, remaining 11 being a onetime infrastructure and not affecting the scalability in linear fashion.

By using 4 matching (application) servers, authentication system handled 10 million Aadhaar authentications in 10 hours with an average response time around 200 milliseconds giving a system throughput of about concurrent 295 requests/sec. 80% of these authentication requests were for biometric authentication and 10% for pure demographic authentication and remaining 10% for OTP authentication. Biometric matching being the most computationally heavy compared to demographic and OTP, system performance of averaging to 200 milliseconds is well below the promised 1 second response.

Performance Test Details

Authentication system is built on open source technologies and is deployed on a commodity computing environment using standard off-the-shelf blade servers. Authentication API is built as a stateless service having the ability to seamlessly load-balance within and across the data centers. Data caching and asynchronous event logging are enabled for maximum performance.

Authentication service is deployed behind an SSL accelerator and an HTTP load balancer. High level deployment diagram is shown below:

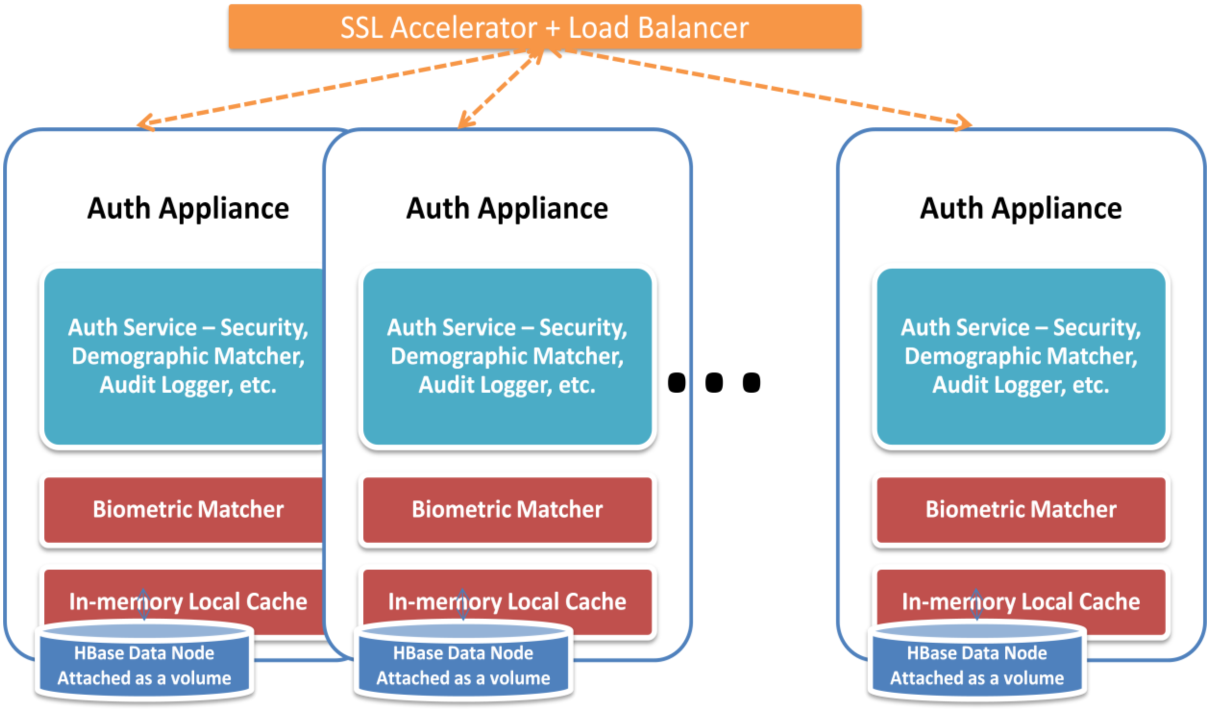

SSL Accelerator + Load Balancer
Auth Appliance
Auth Service – Security, Demographic Matcher, Audit Logger, etc.
Biometric Matcher
In-memory Local Cache
HBase Data Node Attached as a volume
Auth Appliance
Auth Service – Security, Demographic Matcher, Audit Logger, etc.
Biometric Matcher
In-memory Local Cache
HBase Data Node Attached as a volume
Auth Appliance
Auth Service – Security, Demographic Matcher, Audit Logger, etc.
Biometric Matcher
In-memory Local Cache
HBase Data Node Attached as a volume

Figure 21: Authentication server, high level deployment diagram

A work load of 10 million authentication requests were carried out for 10 hours to monitor and measure the system performance. Total work load was split into:

- Pure demographic authentication – 10%
- Pure fingerprint authentication – 60%
- Combined fingerprint and demographic authentication – 20%
- OTP authentication – 10%

Following graph shows average response time per authentication across the 10 hours. Topmost line in the graph below indicates the total authentication time. Other lines below that provide the split of time for various functions to complete an authentication request such as data decryption, data fetch, demographic matching, biometric matching, response creation, auditing, digital signature etc.

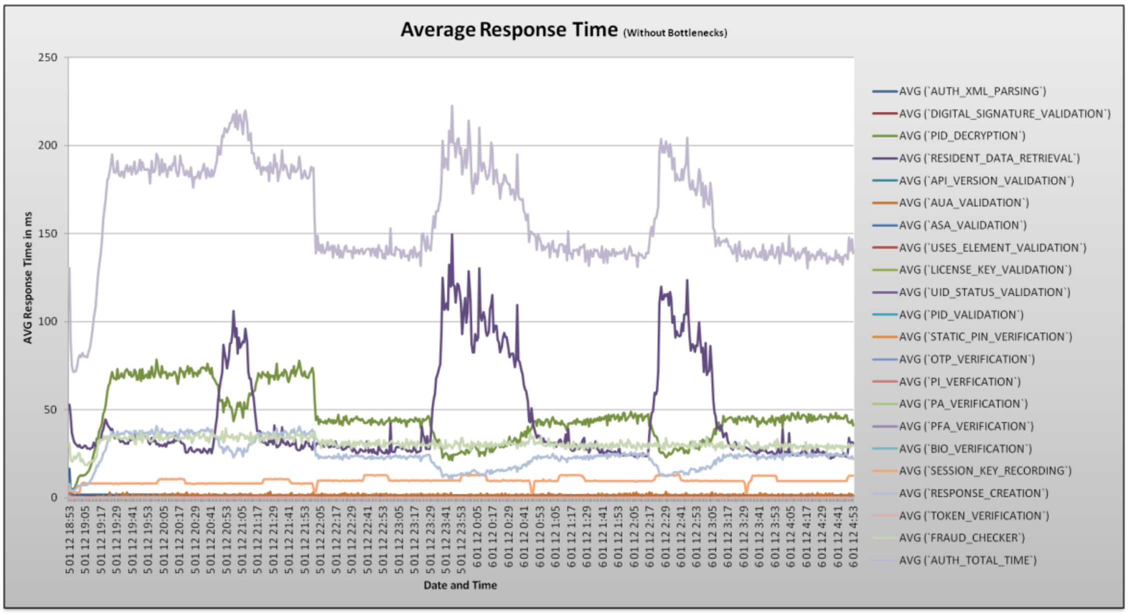


Figure 22: Average response time per authentication over 10hours

It was observed that over the 10 hours, for a total of 10554031 requests (10.5 million), 98.5% of the requests resulted in sub-second response whereas only 0.003% of requests resulted in greater than 3 seconds.

Although 15 servers were used for entire test environment, during the 10 hour test, it was observed that the average CPU utilization was well below 15% showing enough room to further grow the volume even with the same number of servers.

Endurance test carried out during this time also concluded that the fully load balanced authentication servers were able to handle these high volume of requests without any severe degradation of performance and still perform within the expected response time. Average CPU utilization remained under 20% and offered further opportunity to scale. Linear scalability was observed across application and database servers.

The UIDAI authentication system is built to scale to large volumes and can be deployed across one or more data centers within India allowing linear scalability for handling millions of authentications a day. The UIDAI production system across both data centers is currently sized to handle 100 million authentication requests a day.

11 Observations & Recommendations

In conclusion, a set of observations derived from the analysis of the PoC results and subsequently a list of recommendations that flow from the observations are presented.

11.1 Observations from Proof of Concept Studies

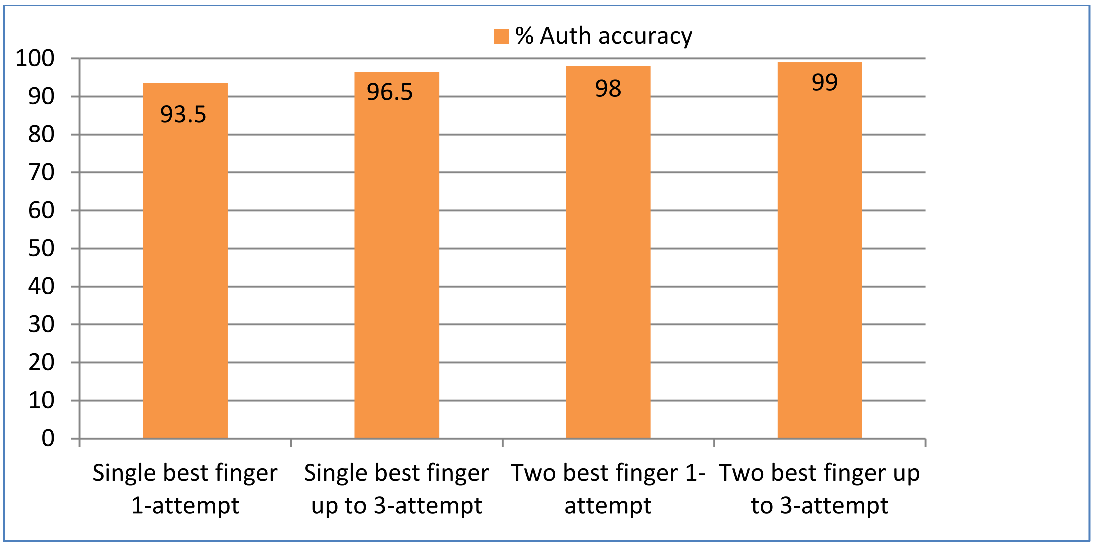


Figure 23: Improving Aadhaar Authentication accuracy

1. **High Accuracy Authentication:** It is possible to attain a high degree of authentication accuracy of- 99% and beyond based on careful design choices. We can keep FRR levels to 1% at a fairly stringent FAR of 1e-4. The above graph shows how high accuracy authentication may be achieved using various strategies.

2. **There is a variation in authentication accuracy based on sensor/extractor combination.** In the study, it was observed that certain combinations of sensor and extractor performed much better than other combinations. The variation in two finger fusion performance ranged from 0.4% to 10%. It is critical that UIDAI encourages the use of good sensors in the field through certification and testing.

3. **For each resident, certain fingers provide a higher chance of authentication success:** Certain fingers were observed to provide better authentication accuracy due to good fingerprint ridges and hence better image quality. Every resident seems to have certain fingers that give better authentication results (reduced FRR). Therefore, to consistently achieve a lower FRR, we need tools and processes to help residents identify these fingers.

4. **Multiple attempts of same finger further improve the chances of successful authentication:** In online authentication situations, providing multiple attempts of the same finger was seen to improve resident's chances of successful authentication. This seems to indicate the resident learns to place fingers appropriately over multiple attempts.

5. **FRR reduces further with increased number of distinct fingers used**: The false reject rate decreases substantially when resident provides more fingers during authentication. FRR decreased when number of fingers was increased.

6. **FRR is lower for high quality images (NFIQ 1 or 2):** The false reject rates are much lower when high quality (NFIQ scores 1 or 2) fingerprint images were considered. *NFIQ 1 and 2 are generally*

considered as good quality fingerprint images, NFIQ 3-5 are generally considered lower quality fingerprint images

7. **Immediate feedback to resident improves authentication**: The devices which were connected online and hence were able to give a result to the resident instantaneously (allowing the resident to conduct multiple attempts in case of failure) showed an improved accuracy when compared with buffered devices(*buffered authentication - the authentication transactions were grouped and submitted as-and-when the network connection was available)* which did not provide any feedback to the resident during authentication.

8. **FRR depends on Age**: Adults (15 to 60) achieved better authentication accuracy as compared to children in the 5-15 age group as well as seniors above 60yr. This indicates the need to tune extractor and matcher algorithms specifically to accommodate children's smaller fingerprints and for seniors to accommodate for drier and worn-out fingerprint.

9. **Visual feedback from authentication device is important**: Certain sensors, which did not provide adequate feedback to the resident for placing / removing fingers, showed longer time to capture as compared to other sensors which did. Further, this occasionally caused the operator to assume a malfunction and these devices removed from the study.

10. **Deploying mechanism for "Best finger detection" helps in following:**
    a. Provide **consistent** higher authentication accuracy
    b. Identify resident who are likely to need two fingers for authentication
    c. Identify residents who may need to update their biometrics
    d. Identify residents who may need to use alternate authentication mechanisms due to inherent poor finger quality

11. **BFD Results – Observations:**
    - 93.6% of people can reliably authenticate with a single finger
    - 4.5% of people can reliably authenticate with more than one finger
    - 1.9% of people cannot reliably authenticate using fingerprints

12. **Single finger authentication – Observations:**
    - Using Best Finger for authentication FRR is much lower (up to 6 times) than using any specific finger
    - Multiple attempts help to improve the accuracy (reduce FRR by 50-75%) of single finger authentication
    - Labeled Matching (1:1) achieves much lower FRR as compared to Unlabeled matching (1:10)

13. **Two finger authentication – Observations:**
    - Two best finger fusion can help to reduce the FRR to 1.0% for Unlabeled (1:10) matching and 0.7% for Labeled (1:1) matching without impacting the FAR
    - As expected, two best finger fusion shows large reduction in FRR for resident who cannot reliably authenticate using one finger

14. **Fingerprint image vs. template**: Using images instead of templates for authentication showed some improvement in accuracy especially at lower FAR values

15. **Effect of resident age on authentication accuracy**: Residents in 15-60 years group showed the best authentication accuracy.

11.2 Recommendations based on the above observations

1. Stringent authentication device testing and certification is recommended to ensure high quality authentication devices are deployed for Aadhaar authentication.
2. It is recommended that residents undergo a 'Best Finger Detection' (BFD) step in order to increase the authentication accuracy.
3. Since both multiple attempts of the same finger as well as multiple attempts with different fingers improve authentication accuracy, it is recommended that support for both techniques be built into the authentication frontend and backend systems.
4. Two best finger fusion shows large reduction in FRR for resident who cannot reliably authenticate using one finger. It is recommended that resident use single finger for authentication first and in case the transaction fails due to biometric mismatch, the resident provides second best finger and two finger authentication be carried out. This method can be used multiple times to reduce FRR.
5. When "buffered" authentication is used, multiple fingerprints should be captured as part of authentication transaction.
6. Since the study demonstrates an age wise variation in authentication accuracy, it is recommended that the extractor & matcher algorithms be tuned for the age bands below 15, 15-60 and above 60 years to give the best age specific matching results.
7. To improve assurance level and make service offerings more inclusive, biometric authentication coupled with OTP is recommended.
8. Multi-modal authentication is expected to not only improve accuracy but also ensure inclusion and hence recommended. Iris authentication helps provide an alternative biometric authentication mechanism for those residents who cannot be authenticated using fingerprints. Further studies need to be undertaken in this regard.
9. Applications using biometric authentication will be diverse in nature, each requiring different level of assurance and conducted in different environment. Fingerprint based authentication as tested is one of the several authentications methods. Further studies in the following three broad areas may be considered:
    a. **Improve fingerprint based authentication**: Further studies are required to investigate, characterize, understand and improve fingerprint based authentication, such as:
        i. Variations in best finger detection based on sensor used and their impact on authentication performance.
        ii. More detailed studies on resident demographics (including age, gender) and its implications on authentication accuracy
        iii. Labeled fingers provide better performance than unlabeled fingers. However, given the possibility of human error, it is recommended that further studies be done to identify the appropriate environments, where this can be used effectively.

    b. **Multi-modal authentication**: Low cost iris capture devices are becoming available in the market. A combination of fingerprint and iris is expected to improve accuracy by a factor of 10 to 100, while reducing failure to enroll (red fingers) rate by a factor of 10. A detailed study such as this one needs to be taken up for Iris authentication in order to characterize the front end and back end set up.

    c. **Multi-factor authentication**: Biometric coupled with PIN or OTP will also prove useful in many financial services and security applications. A smaller study coupled with the current study would provide data and optimized process for creating multi-factor authentication.

12 References

[ISO 19795-2, 2007]: Biometric performance testing and reporting—Testing methodologies for technology and scenario evaluation. By International Standards Organization.

[Jain, 1999]: Jain, Prabhakar and Ross, 1999 http://www.csee.wvu.edu/~ross/pubs/RossFingMatch_MSUTR99-14.pdf

[NISTIR 7346]: NISTIR 7346, Studies of Biometric Fusion, Brad Ulery, Austin Hicklin, Mitretek Systems, Craig Watson Image Group, Information Access Division Information Technology Laboratory, William Fellner, Mitretek Systems, Peter Hallinan, Mitretek Systems Consultant

[NIST, 2006]: MINEX Performance and Interoperability of the INCITS 378 Fingerprint Template, Supplement No. 1 Native Matching, Patrick Grother, Michael McCabe, Craig Watson, Mike Indovina, Wayne Salamon, Patricia Flanagan, Elham Tabassi, Elaine Newton, Charles Wilson, National Institute of Standards and Technology March 21, 2006

[STQC, Authentication, 2011]: STQC: UIDAI Biometric Authentication Device specification http://stqc.gov.in/sites/upload_files/stqc/files/STQC UIDAI BDCS-03-08 UIDAI Biometric Device Specifications _ Authentication_1.pdf

[STQC, Certification, 2011]: STQC Biometric Devices Testing and Certification http://www.stqc.gov.in/content/bio-metric-devices-testing-and-certification

[UIDAI, Authentication, 2012]: AADHAAR Authentication API Specification - Version 1.5 http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_5_rev1_1.pdf

[UIDAI, Authentication Model, 2012]: AADHAAR Authentication Operating Model http://www.uidai.gov.in/images/authDoc/d3_1_operating_model_v1.pdf

[UIDAI, BFD, 2012]: AADHAAR BEST FINGER DETECTION API Specification - Version 1.0 http://uidai.gov.in/images/FrontPageUpdates/aadhaar_bestfingerdetection_api_1.0_draft.pdf

[Wayman, 2002]: Best practices in testing and reporting performance of biometric devices, Version 2.01 By A. J. Mansfield, National Physical Laboratory and J. L. Wayman, San Jose State University. Middlesex: NPL Report CMSC 14/02.