IITB Summer Internship 2013

Software Design Description

Attachment for Aadhar Authentication on Aakash

Principal Investigator
Prof. D. B. Phatak

Project In-charge
Mr. Nagesh Karmali

Project Mentors
Miss. Birundha M.
Miss. Firuza Aibara (PMO)
Mr. Jugal Mehta

Project Team Members
Miss. Archana Iyer
Mr. Hitesh Yadav
Miss. Pooja Deo
Mr. Prashant Main
Mr. Prateek Somani
Mr. Prathamesh Paleyekar
Miss. Sonu Philip
Mr. Sudhanshu Verma

TABLE OF CONTENTS:

1. Scope

The scope of the project is to develop an optical assembly which will make use of the camera of the Aakash tablet itself, to replace the existent external fingerprint scanner. This scanner makes the in-built camera of the tablet redundant. So, this project envisages making use of this camera for the authentication process. The project also includes enhancing the captured image, in order to provide an optimized result. More specifically the system is designed in order to reduce the cost and use the camera on Aakash tablet for the purpose of fingerprint scanning.

This document provides an overview on the techniques that have been used for fingerprint capture and algorithms that have been implemented in order to enhance the image. It also provides a description of the workflow of the system implemented by the team members.

2. References

1. "1998 IEEE Recommended Practice for Software Requirements Specifications. IEEE Computer Society, 1998. - IEEE Std 830"

2. Chirag Dadlani, Arun Kumar Passi, Herman Sahota, Mitin Krishan Kumar, Under Prof. Ajay Kumar Pathak, IIT Delhi- "Fingerprint Recognition Using Minutiae-Based Features"

3. Javier Ortega-Garcia,Josef Bigun, Douglas Reynolds and Joaquin Gonzalez- Rodriguez – "Authentication gets personal with biometrics."

4. Dario Maio, Anil K. Jain –"Handbook of fingerprint recognition."

5. Raman Maini and Dr. Himanshu Agarwal –"Study and Comparison of various Image edge detection techniques."

6. Z.Guo , RW Hall-"Full parallel thinning with tolerance to boundary noise."

7. TY Zhang, CY Suen- "Thinning Methodologies : a comprehensive survey."

8. P. Kumar, D. Bhatnagar, and P.S. Umapathi Rao –" Pseudo one pass Thinning Algorithm. Pattern Recognition Letters, 12:543--555, 1991"

9. http://developer.uidai.gov.in/site/auth_basics

10. "Aadhar Authentication: API Specification- Version 1.5"

11. http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf

12. http://uidai.gov.in/UID_PDF

13. http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf

14. Robert K. Rowe, Kristin Adair Nixon, and Paul W. Butler

-"Multispectral Fingerprint Image Acquisition"

15. http://www.it.iitb.ac.in/arndg/brain2013/sites/default/files/SEIR_0.pdf

16. Richard Wilde -Iris Recognition: "An Emerging Biometric Technology"

17. Daugman –"How iris recognition works"

3. Definitions:

(a) Authentication User Agency (AUA):

An organization or an entity using Aadhaar authentication as part of its applications to provide services to residents. Examples include Government Departments, Banks, and other public or private organizations. All AUAs (Authentication User Agencies) must be registered within Aadhaar authentication server to perform secure authentication.

(b) Sub-AUA (SA):

An organization or a department or an entity having a business relationship with AUA offering specific services in a particular domain. All authentication requests emerging from an AUA contains the information on the specific SA. For example, a specific bank providing Aadhaar enabled payment transaction through NPCI as the AUA becomes the SA. Similarly, a state government being an AUA can have the health department under them as the SA using Aadhaar authentication while providing healthcare benefits.

(c) Authentication Service Agency (ASA):

An organization or an entity providing secure leased line connectivity to UIDAI's data centres for transmitting authentication requests from various AUAs. All connections to production authentication servers must come through private and secure connection through ASAs. Those AUAs who wish to provide their connectivity can become their own ASA where as

smaller AUAs who do not wish to create direct leased line connection to UIDAI's data centres can use an ASA.

(d) Terminal Devices:

Terminal devices are devices employed by SAs/AUAs (both government and non-government) to provide services to the residents. Examples include MicroATM devices, PoS devices, PDS terminals, and MGNREGA terminals, and Access Security devices. These devices will host the applications of the SA/AUA andsupport biometric capture mechanism to capture biometrics of residents for authentication purposes. Any additional features of these terminal devices would depend on specific needs of services offered by SAs/AUAs. These devices must comply with specifications issues by UIDAI to protect all the biometric and demographic information provided by the residents.

(e) Authentication Factors:

Aadhaar authentication will support authentication using multiple factors. These factors include demographic data, biometric data, PIN, OTP, possession of mobile, or combinations thereof. Adding multiple factors may increase the strength of authentication depending on the factors. Applications using Aadhaar authentication need to choose appropriate authentication factors based on the application needs. Currently, not all factors are supported.

(f) Matching Strategy:

Various demographic and biometric matchers use fuzzy matching and work on match thresholds and not on absolute digital (0 or 1) outputs, the interpretation of match scores to a MATCH or NON-MATCH needs to be tuneable using matching strategy. For demographic data matching, currently "Exact" and "Partial" matching strategies are supported in English and fuzzy matching of Indian language data is also supported.

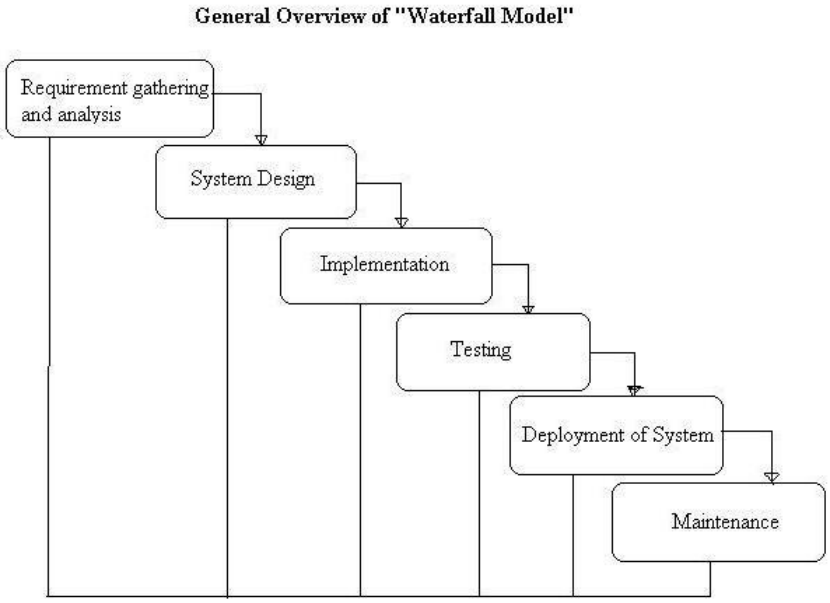
(g) Registered and Public Devices:

Term "Registered Devices" refers to devices which are registered with Aadhaar system for encryption key management. Aadhaar authentication server can individually identify and validate these terminals and manage encryption keys on each registered device. Term "Public Devices" refers to devices which are not registered with Aadhaar system and uses its own encryption key generation scheme. Aadhaar authentication server does not individually identify public devices and uses an alternate encryption strategy for them.

4. Considerations for producing an SDD

4.1 Software life cycle

Attachment for Aadhar authentication system has used the waterfall lifecycle model. The **waterfall model** is a sequential design process, often used in software development processes, in which progress is seen as flowing steadily downwards (like a waterfall) through the phases of Analysis, Design, Construction, Testing and Maintenance. Each phase must be completed fully before the next phase can begin. At the end of each phase, a review takes place to determine if the project is on the right path and whether or not to continue or discard the project.



4.2 SDD within the life cycle

The system goes through a number of stages of the waterfall model one of them being the Design stage. It is necessary that we ensure that the design and implementation used for a software system satisfy the requirements driving that system. The SDD is written in the Design stage of the software lifecycle. It records the result of the design processes that are carried out during the design phase.

4.3 Purpose of an SDD

In the fingerprint authentication for Aadhar system project, the SDD helps ensure that all the requirements that have been stated can be traced to entities. A software design document details how the software requirements should be implemented as well as giving the programmers a blueprint to follow. It helps in coordination of a large team.

5. Design description information content:

This section provides the precise design information needed for planning, analysis, and implementation of the software system. It represents a partitioning of the system into design entities and describes the important properties and relationships among those entities.

5.1. Introduction:

The entire software can be divided into three main sub divisions:

1. Image Capture.

2. Image Enhancement.

3. Application Code.

The image gets captured by an optical assembly developed on the basis of the FTIR principle. The in-built camera of the tablet itself is used to capture the image. This image passes through the application written for enhancing the image which further passes on the image to the main application code, which passes on the encoded finger print, along with other demographic details, onto the ASA server.

5.2.Image Capture:

This sub division has the following properties:

5.2.1.Identification

The identification of the first sub division with which the application execution begins is Image Capture.

5.2.2. Type

The Image Capture part of the application can be classified as a module on the basis of its nature.

5.2.3.Purpose

This module has been included in this application to obtain an image of the finger print of the user for future authentication.

5.2.4.Function

To capture the finger print image of the user.

5.2.5.Subordinate

An optical assembly has been developed to perform the operation of image capture. It consists of 3 parts:

1.Clamp :

The main function of the clamp is to fix the assembly to the tablet over the camera and to hold the spacer. It is made of black acrylic (opaque). It fits directly onto the camera of the Aakash tablet. It is capable of holding the spacer.

2.Spacer :

To get better focusing of the image, there should be a certain distance between the finger and the camera. Empirically, the optimal distance was found to be 30 mm. This value was determined by making cardboard prototypes of different heights of the spacer. The spacer is mounted on the clamp.

3.Optical Assembly

Illumination needs to be provided while fingerprint image is being taken. This assembly implements the FTIR (frustrated total internal

reflection) principle for fingerprint recognition. It consists of two parts-

i) PCB

The LEDs are mounted on the PCB , next to the acrylic plate on which finger has to be kept. When the fingerprint has to be captured, the LEDs glow and due to FTIR principle, the fingerprint image obtained, has differentiation between the ridges and valleys of the finger. The LEDs used were of 3 mm length. The power source of the LEDs is 5V DC source and the resistors connected to the LEDs are of 220 ohms. LEDs illuminate the transparent acrylic of 3 mm width.

ii) Lid

The lid is needed to cover the PCB so that light from outside does not affect the fingerprint image.

The Acrylic used in the whole assembly is 3 mm thick.

5.2.6. Dependencies

It passes on the image to the image enhancement module for further processing. This module is useful for camera with low resolution. It can only be useful for front facing camera with proper lighting conditions.

5.2.7 Resources

- Black acrylic (3 mm thick)
- Transparent acrylic (3 mm thick, 32.5mm x 35 mm)
- PCB
- LEDs (4 quantity, 3 mm thick)
- Resistors (4 quantity, 220 ohms)
- Wires
- Driller
- Soldering gun

- Soldering wire
- Hack saw
- File
- Polishing paper

5.3 Image enhancement

This part of the application has the following properties:

5.3.1 Identification

The identification of the next sub division with which the application execution continues is Image Enhancement.

5.3.2 Type

The Image Enhancement part of the application can be classified as a module on the basis of its nature.

5.3.3. Purpose

This module has been prepared to enhance the fingerprint image which has been received.

5.3.4. Function

This module undertakes the functionality of enhancing the fingerprint image received by passing it through a number of image processing techniques.

5.3.5. Subordinate

1.Rescaling
This is the process of resizing of the image.

2. Conversion of RGB to Gray scale

It involves changing of RGB values by taking average of the RGB value and then assigning the average value to the R, G, and B separately.

3. Resizing

This step involves converting the image to one having a size of 300 x 200 pixels and it separates out the unwanted parts of the image.

4. Adaptive Histogram equalization of Grey scale

Adaptive histogram equalization (AHE) is a computer image processing technique used to improve contrast in images. It differs from ordinary histogram equalization in the respect that the adaptive method computes several histograms, each corresponding to a distinct section of the image, and uses them to redistribute the lightness values of the image. It is therefore suitable for improving the local contrast of an image and bringing out more detail

5. Sharpening

Sharpening an image means to make the differences between the neighboring pixels more noticeable. Sharpening brings out the details of an image. Sharpening is done by kernel based convolutions. It brings out the details of an image, it makes the picture smudge free and it emphasizes on the texture of the image. The method adopted is Laplacian based convolution since the kernel is usually much smaller than the image, this method usually requires far fewer arithmetic operations

6. Thresholding

In Fingerprint image processing, thresholding is used to split an image into smaller segments, or junks, using at least one color or gray scale value to define their boundary. A possible threshold might be 40% gray in a gray scale image: all pixels being darker than 40% gray belong to one segment, and all others to the second segment. It's often the initial step in a sequence of image processing operations. These segments are not necessarily convex since image content is arbitrary. In that sense segments should represent objects in the image. Unfortunately, such objects vary with respect to colors, intensity, illumination, lens aberrations and

noise which makes choosing the right threshold not an easy task. Multiple thresholds might be needed in connection with more sophisticated algorithms. In case the object in the foreground has quite different gray levels than the surrounding background, image thresholding is an effective tool for this separation. Otsu thresholdig has been implemented.

7. Thinning

Thinning is a morphological operation that is used to remove selected foreground pixels from binary images, somewhat like erosion or opening. It can be used for several applications, but is particularly useful for skeletonization. In this mode it is commonly used to tidy up the output of edge detectors by reducing all lines to single pixel thickness. Thinning is normally only applied to binary images, and produces another binary image as output. In thinning algorithms, the best algorithm is Zhang Suen algorithm as it considers end to end points and also takes care of the minutiae's and the bifurcations in an efficient way.

5.3.6. Dependencies

It receives the image from the image capture model and after carrying out all the enhancement steps on it, passes the enhanced image on to the final application, Its conditions are that Only available for Android 4.0 Ice cream-Sandwich Operating System.

5.4. Application Code

This part of the application has the following properties:

5.4.1. Identification

The identification of the last sub division with which the application execution ends is Application Code.

5.4.2. Type

On the basis of its nature it can be identified as a procedure in unexecuted state and a program in executed state.

5.4.3. Purpose

This procedure has been developed to start the scanning process and forward the result to the ASA server.

5.4.4. Function

The Application undertakes the following functionality:

- Starts the device, which the captures the finger print image.
- Closes the device.
- Converts the image into a byte stream.
- Takes in other demographic details from the user and generates a request.xml file.
- Encodes the finger print image.

5.4.5. Subordinate

The Software Source is divided into 3 parts. Each part performs certain specific operations.

- **com:**

  This is the part responsible for scanning of fingerprint it has code which contains the code for scanning the Image and doing some processing for the Aadhar

- **in**

  This is the part developed for passing of information by the device to the Aadhar Authentication Server. It has a small code which takes care of only passing the Attributes. The only file in this code is AUAData.java.

  All typical functions are like:

```
public String getTerminalId()

{

    return terminalId;

    }
```

- **Bouncy castle:**

The conversion of data(image) into encrypted form is done by Bouncy Castle. It takes an image and encodes it and sends it over to the server. At the server side, this image is decoded and used by the server for the process of authentication.

5.4.6. Dependencies

The image enhancement module passes on the enhanced image to this procedure. The procedure then encodes it and passes it on to the ASA server.

5.4.7. Resources

The files included in the Com section of this procedure are:

- Aadhaar.java
- DataUtil.java
- FingerHeaderGenerator.java
- FtrScanDemoActivity.java
- ImageDetail.java
- MyBitmapFile.java
- Scanner.java
- BioConstants.java
- DecoderProperties.java
- FPScan.java
- Home.java

- ImageSize.java
- NDKTest_22Activity.java

Following is a brief description of what each file does:

- **Aadhar.java:**

This file takes the given image and encodes it using the bouncy castle files.

- **DataUtil.java:**

It uses the big integer functionality to convert a byte array and pass it back.

- **FingerHeaderGenerator.java:**

It generates a header for the image being sent in order to be recognized and used by the back-end server each file(image) has different headers. The method wraps an image with ISO 19794-4 headers. It takes an image as byte[] (any format jpeg, jp2, gif, etc).

- **FtrScanDemoActivity.java:**

This part of the code takes care of all the options marked by the user and provides results based on the selected options. The file calls for the scanning of image and then checks and displays the quality of image in the meantime it also stores the image as "fp.bmp" in the directory "sdcard/Android/fp.bmp".

A function named "ShowBitmap()" is also present in the code which displays the image of the fingerprint on the tablet. It also creates an FTP template (i.e. a template of the scanned image).

- **ImageDetail.java:**

This file sets the height and the width of the image and also sets the image to a particular defined size.

- **MyBitmapFile.java:**

  This part of the code receives an image with the parameters such as its height and width once received this image is converted into a corresponding bitmap file using an byte[](array) and also the colors of the image are modified to be in a range of 0-256(RGB). This part also sets the DPI of the newly formed image to 500 by default.

- **Scanner.java:**

  This part of the code checks the input for some incorrect format or fingerprint with variables like:

  • FTR_ERROR_EMPTY_FRAME – for empty frame

  • FTR_ERROR_NO_FRAME – fake finger detected

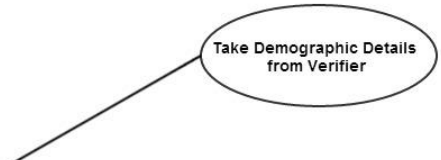
  • TR_ERROR_INVALID_AUTHORIZATION

It also has the codes to open the device and close the device. All these functions are native functions.

6. Design description organization

6.1. Design views

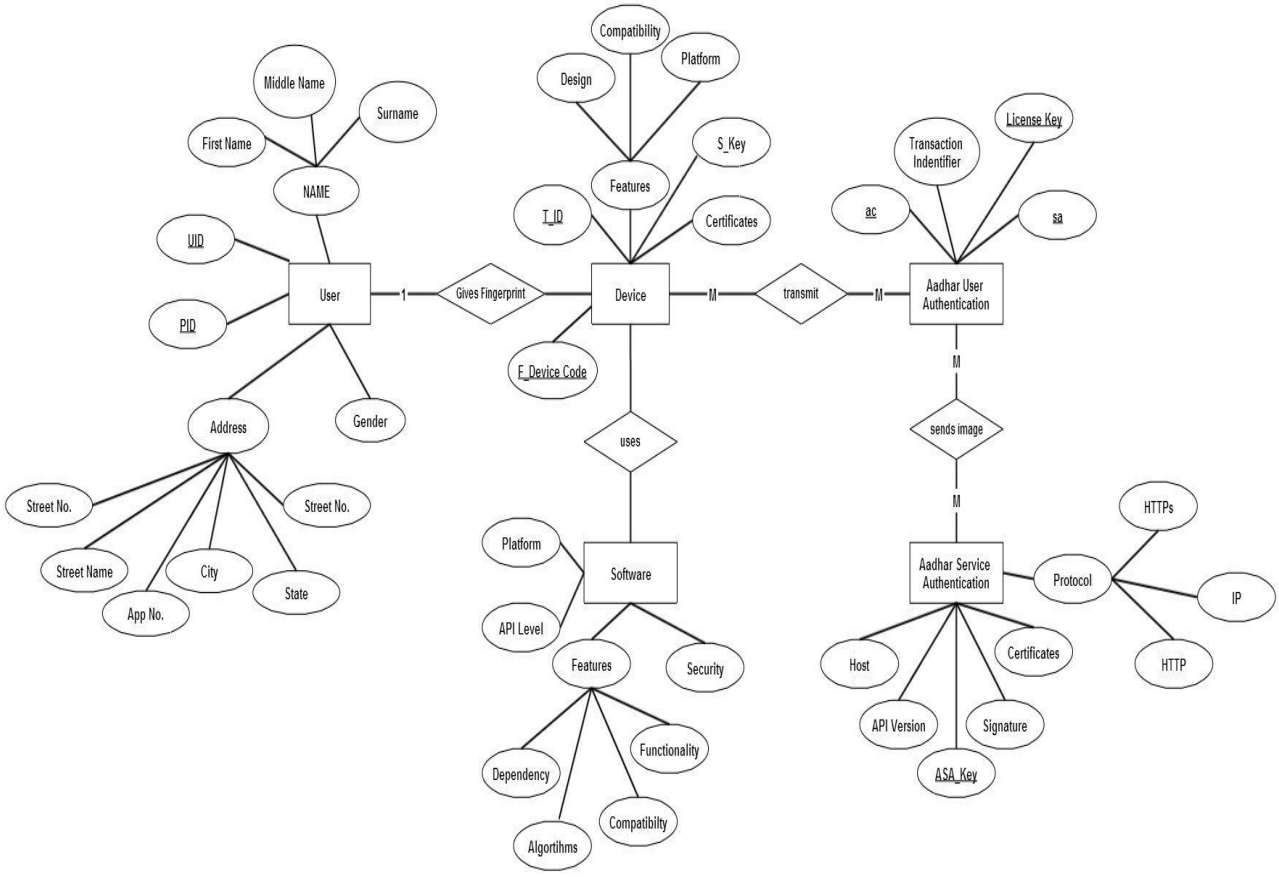
Use Case Diagram:



Tabular Description:

Actors	Operator, Aadhar Authentication
Descriptions	The data consisting of Demographic details and the fingerprint images of the verifier is sent to server.
Data	Verifier's Demographic Details and fingerprint images.
Stimulus	Send Command by the operator
Response	The data related to verifier is sent to the server.

ER DIAGRAM



6.1.1. Decomposition description

The product functions are:

1. Optic assembly on Camera:

Gets the fingerprint image of the verifier.

2. Enhancement of image:

Enhances the image received from the scanner.

3. Send:

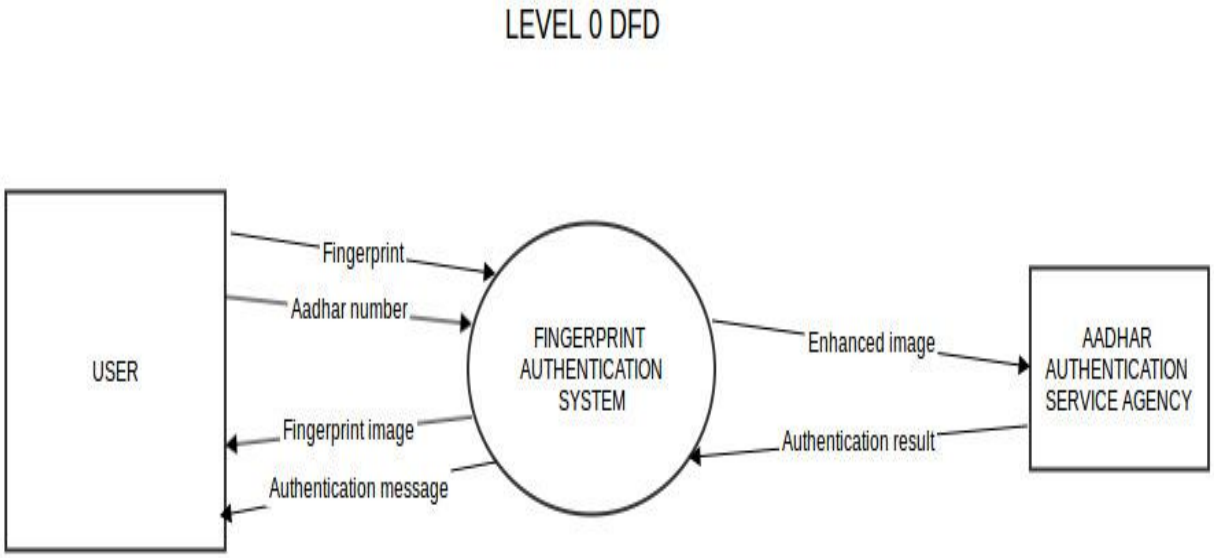
Sending of image and other demographic information to the ASAs.

4. Get results:

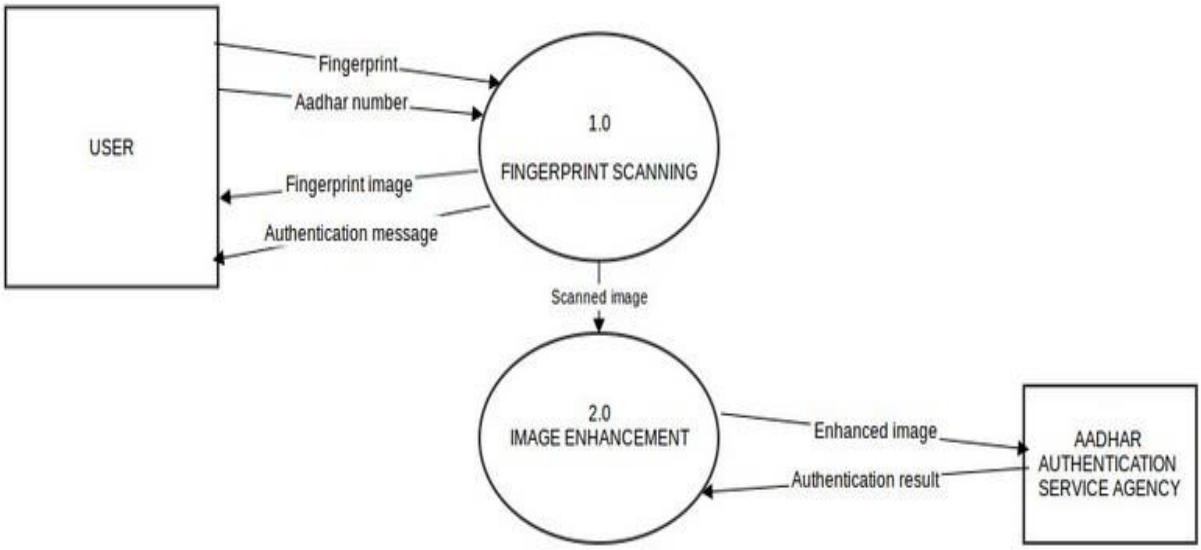
Receiving the response from the ASA.

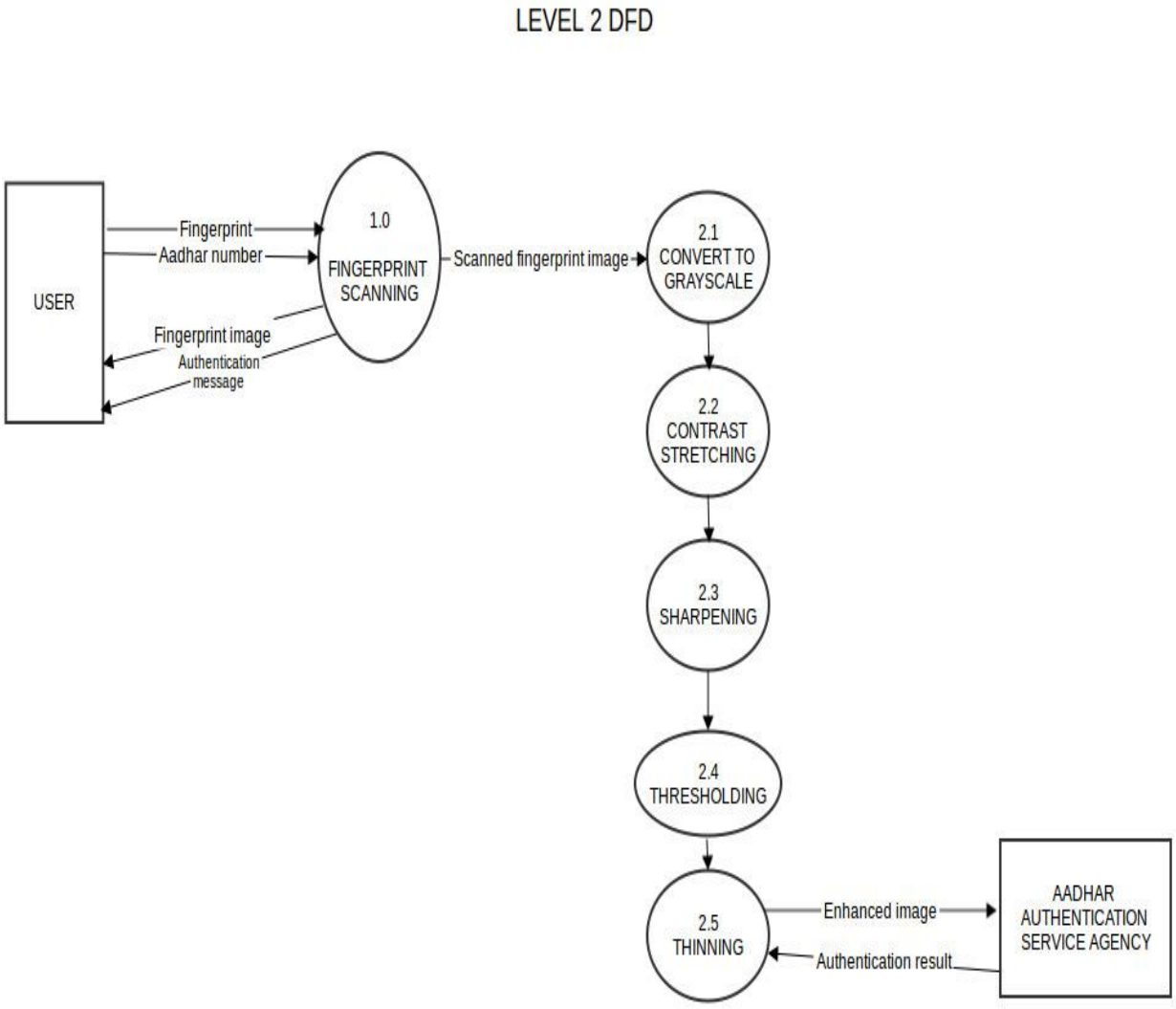
6.1.2 Dependency Description

This is the representation of he system using data flow diagrams. Level 0, Level 1 and Level 2 DFDs are shown below.

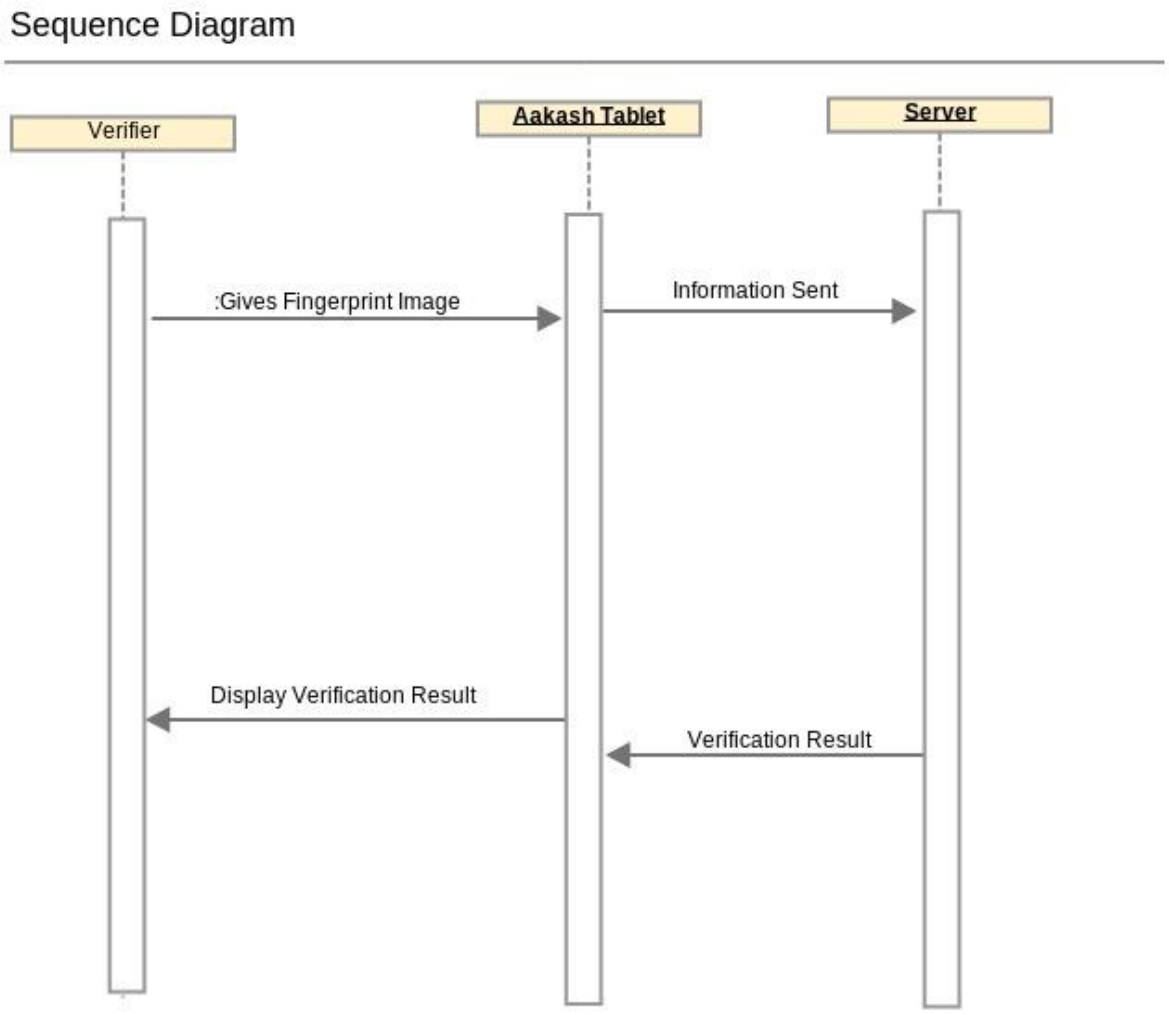


LEVEL 1 DFD


USER
Fingerprint
Aadhar number
Fingerprint image
Authentication message
1.0
FINGERPRINT SCANNING
Scanned image
2.0
IMAGE ENHANCEMENT
Enhanced image
Authentication result
AADHAR
AUTHENTICATION
SERVICE AGENCY



This is the system representation using a sequence diagram.



6.1.3 Interface Description:

It provides everything designers, programmers, and testers need to know to correctly use the functions provided by an entity.

6.3.1: Hardware Interface:

The optic assembly built on the camera takes care of getting the fingerprint image of the verifier. The image taken is send to the application on the Aakash tablet and then is sent to the Aakash authentication server by the operator.

6.3.2: Software Interface:

The interface is on Android operating system.

6.3.4: Communication Interface:

The connection between the ASAs and AUAs uses HTTP protocols.