IITB Summer Internship 2013

Software Requirement Specification

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

List of Figures:

1.0 Introduction:

1.1 Purpose:

The purpose of this document is to present a detailed description of the Aadhar Authentication using Aakash tablet. It will explain the purpose and features of the system, the interfaces of the system, what the system will do, the constraints under which it must operate and how the system will react to external stimuli. This document is intended for both the stakeholders and the developers of the system.

1.2 Scope of Project:

The Scope the Project would be to make an optical assembly for Aakash Tablet so that it can be used in place of current fingerprint scanning device and to get a clear image of fingerprint which in turn used for the authentication of Aadhar ID Card .Also an Image Enhancement Software is developed which will optimize the provided image.

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. Once Completed we will try for its application on other tablets and phones as well.

1.3 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. John Daugman "**How iris recognition works"**

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

7. Z.Guo , RW Hall **"Full parallel thinning with tolerance to boundary noise"**

8. TY Zhang, CY Suen **"Thinning Methodologies – a comprehensive survey"**

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

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

11. K. Rowe, Kristin Adair Nixon, and Paul W. Butler Robert **"Multispectral Fingerprint Image Acquisition"**

12. Richard Wilde **"Iris Recognition: An Emerging Biometric Technology**"

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

14. http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf

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

16. http://www.it.iitb.ac.in/arndg/brain2013/sites/default/files/SEIR_0.pdf 16

17. http://www.cambridgeincolour.com/tutorials/image-sharpening.htm

18. http://dpbestflow.org/image-editing/sharpening

19. http://en.wikipedia.org/wiki/Software_requirements_specification

20. http://techwhirl.com/writing-software-requirements-specifications/

21. **http://developer.uidai.gov.in/site/auth_basics/**

1.4 Terminology:

Frustrated Total Internal Reflection (FTIR): It is basic principle for fingerprint image scanner.

Authentication User Agency (AUA): An organization using Aadhar Authentication as part its application 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.

Sub-AUA (SA): An organization having 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.

Authentication Services Agency (ASA): An organization provides secure leased line connectivity to UIDAI's data centers 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 centers can use an ASA.

Terminal Devices: Terminal devices are devices employed by SAs/AUAs to provide services to the residents. Examples: MicroATM devices, PoS Devices,PDS terminals, and MGNREGA terminals, and Access Security devices. These devices will host the applications of the SA/AUA and support 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.

Authentication Factors: Aadhar Authentication will support authentication using multiple factors which includes demographic data, biometric data, PIN, OTP, possession of mobile.
Adding multiple factors may increase strength of authentication depending on the factors.

Matching Strategy: Various demographic and biometric matchers uses fuzzy matching and work on match threshold and not on absolute digital output, the interpretation of matches' scores to a MATCH or NOT MATCH.

Registered and Public Devices: Term “Registered Devices” refers to devices which are registered with Aadhar system for encryption key management. Aadhar 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 Aadhar system and uses its own encryption key generation scheme. Aadhar authentication server does not individually identify public devices and uses an alternate encryption strategy for them.

2.0. Overall Description:

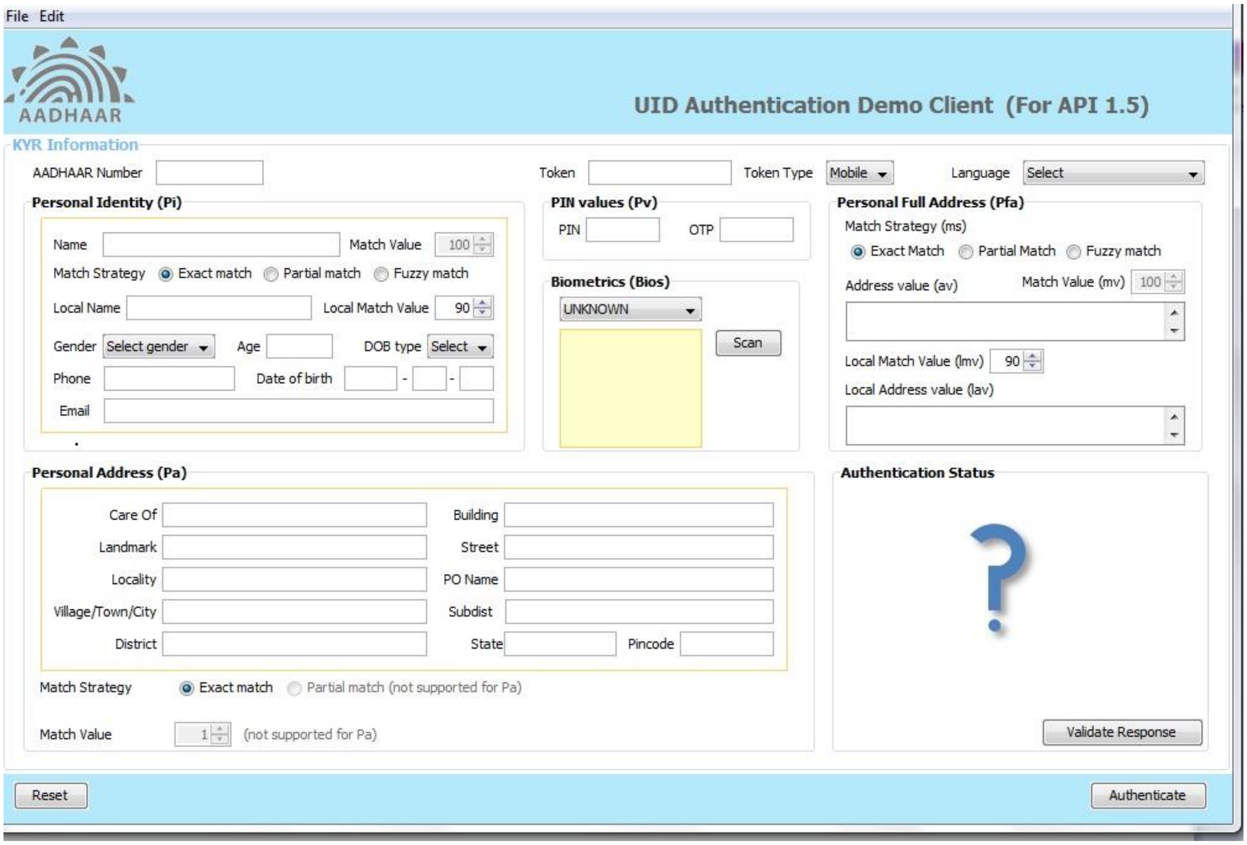
2.1 External Interface Requirements:

There are four different types of External Requirements which are listed below:

2.1.1 User Interface:

The purpose of the product is to provide a best fitted device to take the fingerprint image with the use of the camera on the Aakash Tablet and also to do enhancement of the image got from the fingerprint capture device.

After this the fingerprint image with other personal information related to the user is sent to the Aadhar Authentication server for verification. The server returns the result whether the information provided was correct or false.



Token Type: Mobile
Language: Select
Match Value: 100
Match Strategy: ● Exact match ○ Partial match ○ Fuzzy match
Local Match Value: 90
Gender: Select gender
DOB type: Select
Biometrics: UNKNOWN
Match Strategy (ms): ● Exact Match ○ Partial Match ○ Fuzzy match
Match Value (mv): 100
Local Match Value (lmv): 90
Match Strategy: ● Exact match ○ Partial match (not supported for Pa)
Match Value: 1 (not supported for Pa)

Fig- 1 UI of Aadhar Authentication

2.1.2 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 to authentication server by operator for verification.

2.1.3 Software Interface:

This interface is built for Android 4.0 Ice-cream Sandwich version only.

2.1.4 Communication Interface:

The connection is established between Authentication User Agency (AUA) and Authentication Service Agency using HTTPs protocol. Once connection is established, then processing solely depends upon server processing speed.

2.2 Product Functions:

The major product functions are:

- Optic Assembly on Camera- Gets the fingerprint image of the verifier.
- Enhancement of Image- Enhances the image received from scanner.
- Send- Sending of Image and other demographic information to ASAs.
- Get Results- Receiving the response from ASAs.

2.3 User Characteristics:

2.3.1 Physical Actors:

A) Verifier:

The Verifier is the one who uses the fingerprint biometric for recognition. He needs to provide with personal details and his fingerprint images.

B) Operator:

The operator is one who enters the demographic details of the verifier into the Aakash Tablet.

2.3.2 System Actors:

A) Client:

The Client is the system which sends the personal information related to a particular person to the Aadhar Authentication.

B) Server

The Server (ASAs) is the system which accepts personal information related to a particular person from client and returns the verification result to the client after the comparison of the details provided.

2.4 Constraints:

2.4.1 Software Constraints:

1. Only available for Android 4.0 Ice cream-Sandwich Operating System
2. Can process only fingerprint images taken from low resolution.

2.4.2 Hardware Constraints:

1. Only applicable for capturing fingerprint images.
2. Useful for camera with low resolution.
3. Can only be useful for front facing camera.
4. Device should be enabled with Internet facilities like Wi-Fi.

2.5 Assumptions and Dependencies:

A) Assumptions:

If in case scanned image of fingerprint distorted, user can again scan their fingerprint.

B) Dependencies:

1. Image Processing Speed at Aadhar Authentication Server end.
2. Image Capturing Capacity of Camera.

3. Specific Requirements:

3.1 Performance Requirements:

1. The data sent to the server should not be more than 7.5 MB for a particular user.
2. The fingerprint image should be of 300-500 dpi.

3.2 Design Constraints:

1. Works only on camera with low resolution.
2. The GUI designed only for Android 4.0 Ice-cream Sandwich Operating System.

3.3 Functional Requirements:

Functional Requirements basically includes requirements related to Hardware, Software and Optical Assembly for Aadhar Authentication on Aakash Tablet. The following block diagram shows the procedure of optical assembly.

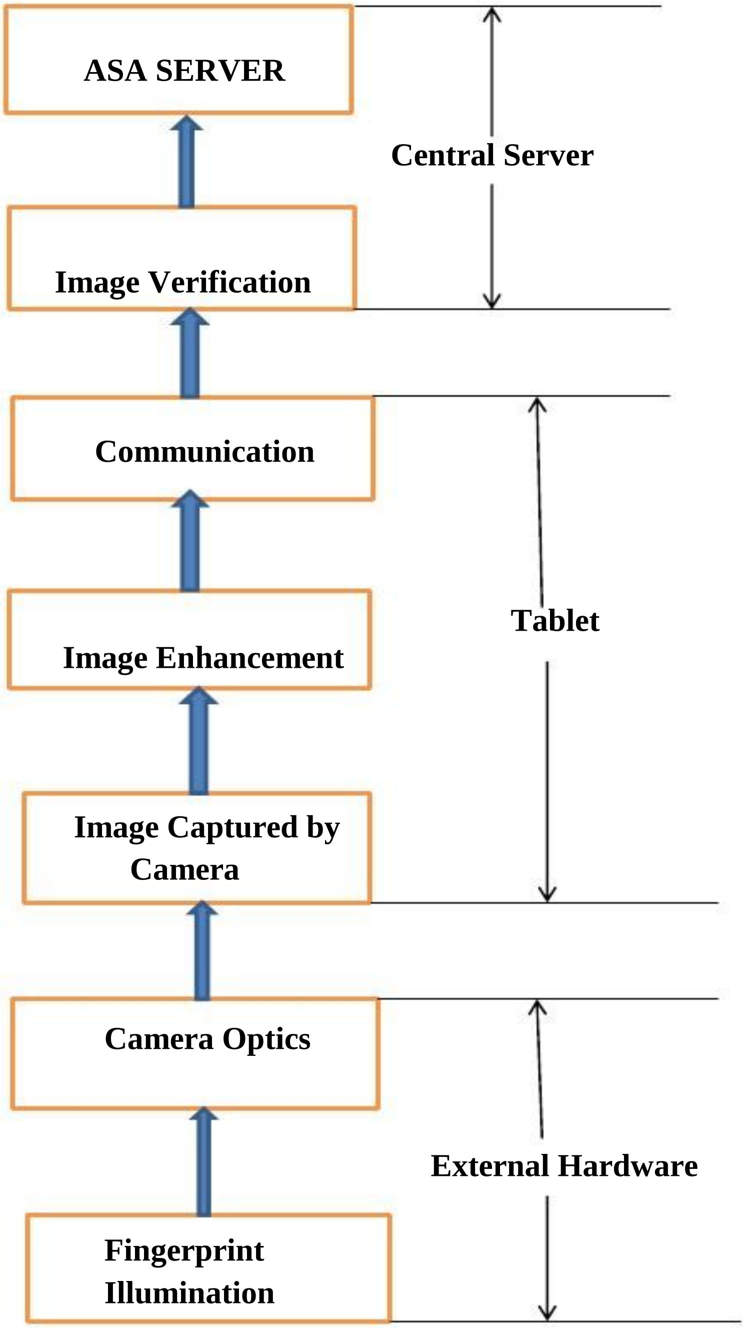


Fig-2 Block Diagram of Aadhar Authentication

A) Optic Assembly:

Normally Optical Fingerprint methods use principle of Frustrated Total Internal Reflection (FTIR) and the absorption of light. To produce fingerprint image, a light source drops light on finger placed at the surface, which is scattered from the surface forming fingerprint image. The behavior of light after it hits fingerprint ridges makes it possible to distinguish the contrast between ridges and valley in the image. Under Total Internal Reflection, when the lights hits valley of fingerprint, the light totally reflects and therefore valley appears as bright spot in image. The following figure shows principle of FTIR.

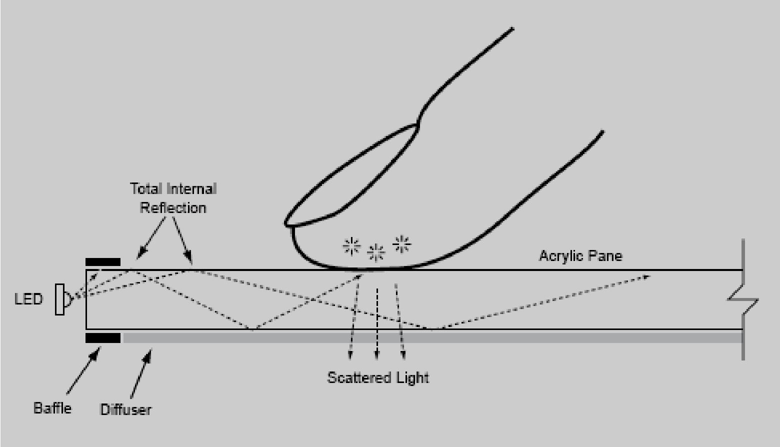


Fig-3 Principle of FTIR

For implementing fingerprint authentication on Aakash Tablet, hardware is built using principle of optics i.e. Frustrated Total Internal Reflection. Optic Assembly is built using material which includes PCB(Printed Control Board for mounting LEDs), Transparent Acrylic, Black Acrylic, LEDs, Clamps to attach optic assembly on Aakash Tablet, Spacer of 30mm where built optic assembly will be kept. This when built, takes much clearer image for proper processing. The figure on page number 15 shows the construction of Additional Optical Assembly (Multi-Spectral Fingerprint Scanner) built for capturing fingerprint images. An optical assembly has been developed to perform the operation of image capture. It consists of 3 parts:

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.

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.

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:

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.

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.

3.3.1 Resources:

The proposed design was made for building optical assembly which is shown in upcoming page, also to build this optical assembly, listed components are used:

- 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)
- Power Source (4.5 V, 3AAA*1.5V) cells in series.
- Switch

Optical assembly

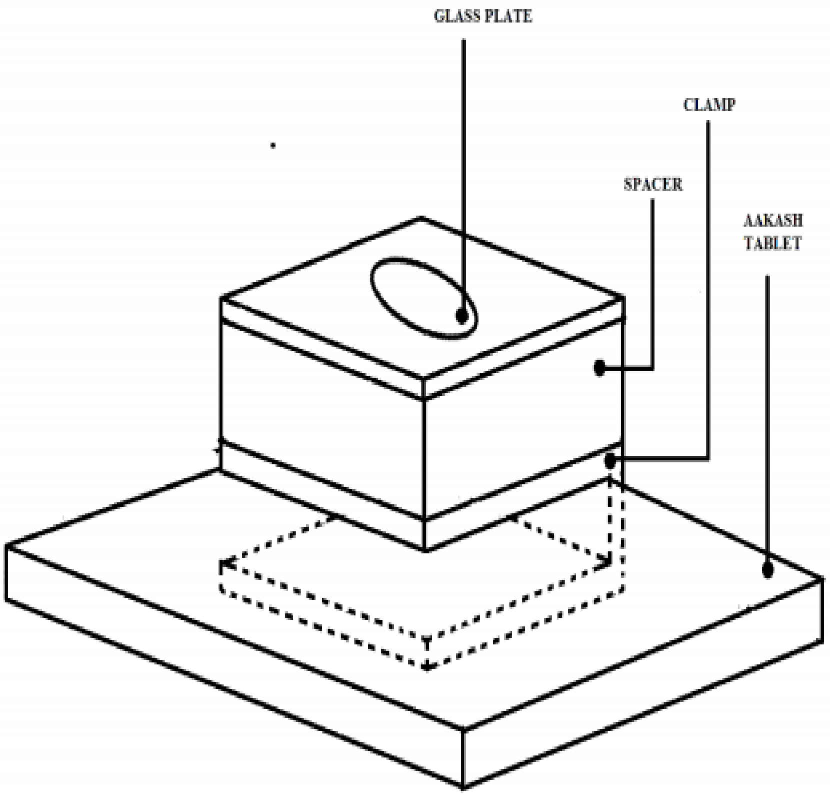


Fig -4 Design of Optical Assembly

The next figure shows the ideal design of fingerprint acquisition device. This is Multi Spectral Fingerprint scanner which uses concept of FTIR.

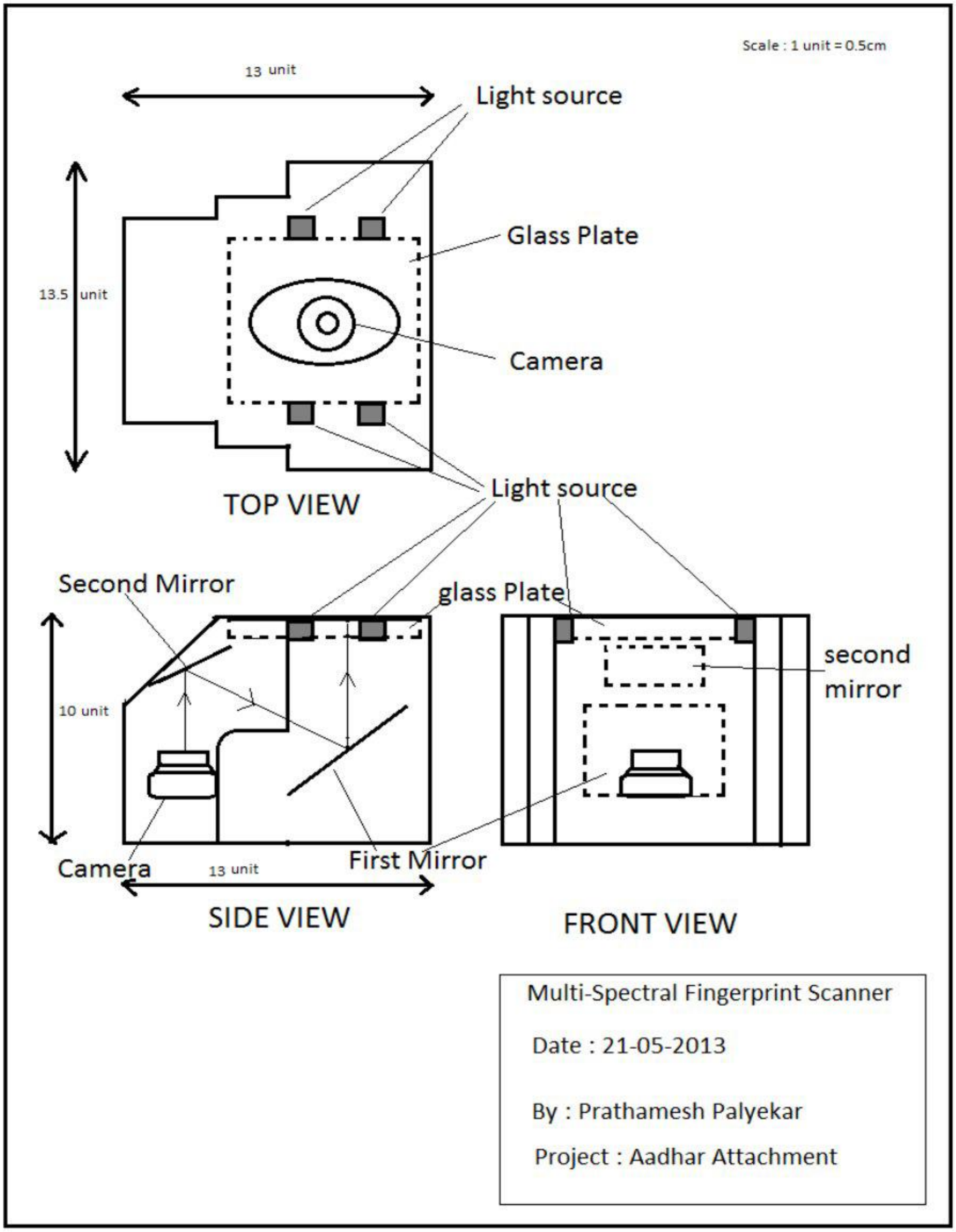


Fig- 4 Line diagram of Multi-Spectral Fingerprint Scanner

In order to capture information-rich data about the surface and subsurface features of the skin of the finger, the Assembly collects multiple images of the finger under a variety of optical conditions. The raw images are captured using different wavelengths of illumination light, different polarization conditions, and different illumination orientations. In this manner, each of the raw images contains somewhat different and complementary information about the finger. The different wavelengths penetrate the skin to different depths and are absorbed and scattered differently by various chemical components and structures in the skin. The different polarization conditions change the degree of contribution of surface and subsurface features to the raw image. Finally, different illumination orientations change the location and degree to which surface features are accentuated.

Illumination for each of the multiple raw images is generated by one of the light emitting diodes (LEDs). The figure illustrates the case of polarized, direct illumination being used to collect a raw image which is captured by Camera of Aakash Tablet and stored in internal memory of Tablet itself. The light from the LED passes through a linear polarizer before illuminating the finger as it rests on the sensor platen. Light interacts with the finger and a portion of the light is directed toward the imager through the imaging polarizer. The imaging polarizer is oriented with its optical axis to be orthogonal to the axis of the illumination polarizer, such that light with the same polarization as the illumination light is substantially attenuated by the polarizer. This severely reduces the influence of light reflected from the surface of the skin and emphasizes light that has undergone multiple optical scattering events after penetrating the skin. After capturing image, its enhancement is done by applying different algorithm. These algorithms are implemented by another software application. In this software, the listed algorithm are integrated and applied to target image for enhancing its quality. The Algorithm are:

- Rescaling
- Gray scaling
- Normalizing
- Sharpening
- Thresholding
- Thinning

B) Software Model (Image Processing Model):

Role of Software model is still important as it first of all initiates the front camera of given tablet and initialize the procedure which is used for processing images which has been taken using camera of Aakash tablet. As this software should support Android 4.0 i.e. Ice-Cream Sandwich version, it is necessary to build the software on JAVA platform which is supported by Android.
Also this software uses different platform to integrate the entire different algorithm. It is necessary to understand that the DPI of image taken using Tablet's camera is only approx 72dpi and the requirement is around 300dpi at least .To resolve this problem it is necessary to implement different algorithm, and by doing this we can obtain desired image. But it is also important at the same time that the images which are taken should be fingerprint of humans, it should not be any other object. For these there is a method called Live Finger Detection (LFD) principle which helps to know that the provided fingerprint is authentic. So for successful fingerprint authentication, it is necessary to understand the concept of Live Finger Detection.

Theory:

Live Finger Detection (LFD) is a patent pending technology developed by Futronic to stop the access to secured data and location by using fake fingers made from silicone, rubber, play-doh, etc.

Skin characteristic:

There are 600 sweat glands per square inch of skin and sweat (dilute sodium chloride solution) diffuses through pores. Distance between these pores does not change over time.

Perspiration over time:

In live fingers perspiration starts from the pores. The sweat then diffuses along the ridges during the time, making the semi-dry portion between the ridges moister and darker in the image. The perspiration phenomenon doesn't occur in cadaver finger or artificial fingerprints.

There are two ways to use perspiration phenomenon

1. Static approach
- Perspiration starts from the pores
- Detection of pores and checking whether distance between them doesn't change

2. Dynamic approach
- Perspiration changes darkness of image over time.

The most positive idea behind this concept is to ensure that the fingerprint provided is genuine, also there is no additional hardware or software changes to be made.

The following code of segment tells about software. Software model does role of image enhancement by integrating different algorithm and follows many algorithmic proceedings which are:

Rescaling:

This is the process of resizing of the image. When original image is provided, it might be in such a size on which application of other algorithm becomes difficult. Therefore, it is necessary to apply rescaling algorithm.

Gray scale:

Gray scale is a range of shades of gray without apparent color. The darkest possible shade is black that means no reflected light. The lightest possible shade is white, which means total reflection of light at all visible wavelength Intermediate shades of gray are represented by equal brightness levels of the three primary colors red, green and blue for transmitted light, or equal amounts of the three primary pigments cyan, magenta and yellow for reflected light.

In practice, gray scale imaging is sometimes called "black and white," but technically this is a misnomer. In true black and white, also known as halftone, the only possible shades are pure black and pure white. The illusion of gray shading in a halftone image is obtained by rendering the image as a grid of black dots on a white background, with the sizes of the individual dots determining the apparent lightness of the gray in their vicinity. The half tone technique is commonly used for printing images.

The basic idea of our method is to follow the ridge lines (in fingerprint) on the gray scale image, by "sailing" according to the fingerprint directional image. A set of starting points is determined by superimposing a square-meshed grid on the gray scale image. For each starting point, the algorithm keeps following the ridge lines until they terminate or intersect other ridge lines. A labeling strategy is adopted to examine each ridge line only once and locate the intersections between ridge lines

Contrasting:

In image processing, normalization is a process that changes the range of pixel intensity values. Applications include photographs with poor contrast due to glare, for example. Normalization is sometimes called contrast stretching or histogram stretching. Contrast modification (Normalization) in image is a point process that involves application (addition, subtraction, multiplication or division) of an identical constant value to every pixel in the image. This procedure is also known as Adaptive histogram equalization (AHE) which is not ordinary histogram equalization.

Sharpening:

Sharpening an image means to make the differences between the neighboring Pixels more noticeable. Sharpening brings out the details of an image. Sharpening can be done by kernel based convolutions. In image processing a Kernel, is a small matrix which is useful for blurring, sharpening, embossing, Edge-detection and more. 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. A kernel is basically a 2D matrix of numbers that can be used as coefficients for numerical operations on pixels. Sharpening involves the following steps:

1. Read the original image.
2. Choose the image processing technique-sharpening.
3. Choose the corresponding kernel to do the sharpening.
4. Apply the above kernel to the image matrix using convolution.
5. Display the sharpened image.

Threshold:

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 make 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.

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 effective way.

After applying all the algorithms, the software application does the following functions:

a) Closes the device.
b) Converts the image into a byte stream.
c) Takes demographic details of user and generates a new request .xml file.
d) Encodes the finger print image.

The following figure shows the procedure. This whole procedure is on front end side. The software is built in such a way that it just sends enhanced image to ASAs.

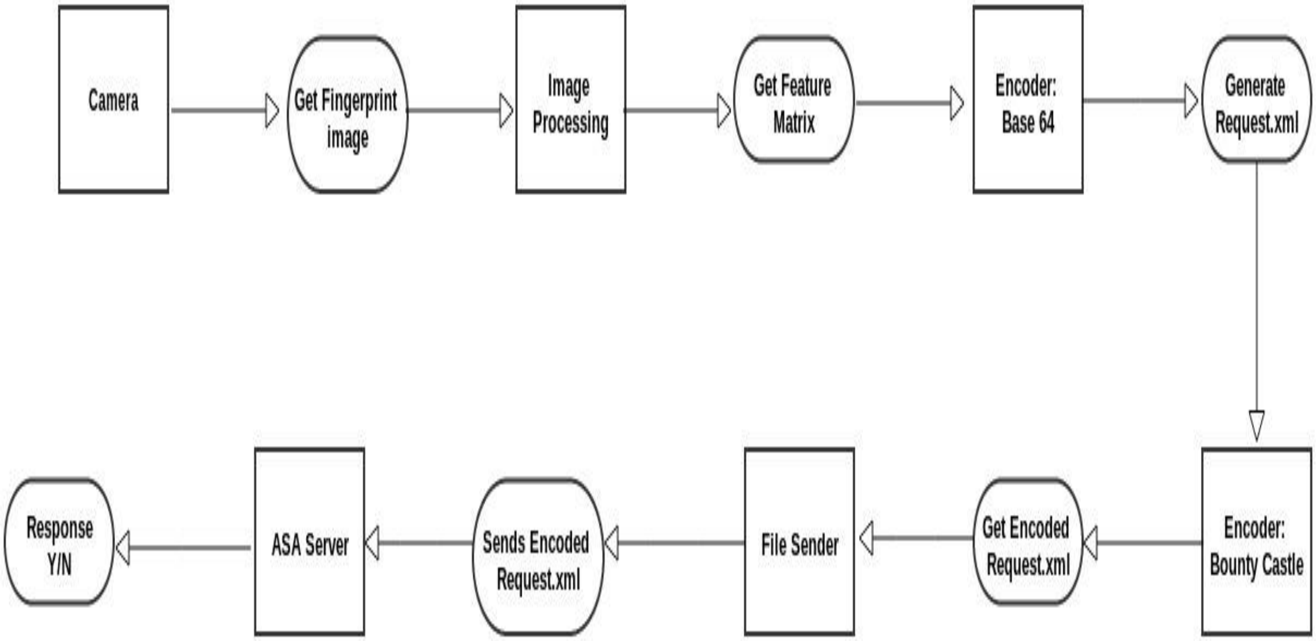


Fig-5 Flowchart of software Process

The whole software functionality and coding is divided into three codes of section:

1) 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.

2) 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.

3) 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 16 to the server. At the server side, this image is decoded and used by the server for the process of authentication.

The next Section of functional requirements deals with different diagrams, using them the requirements can be understood.

A) Use Case Diagrams:

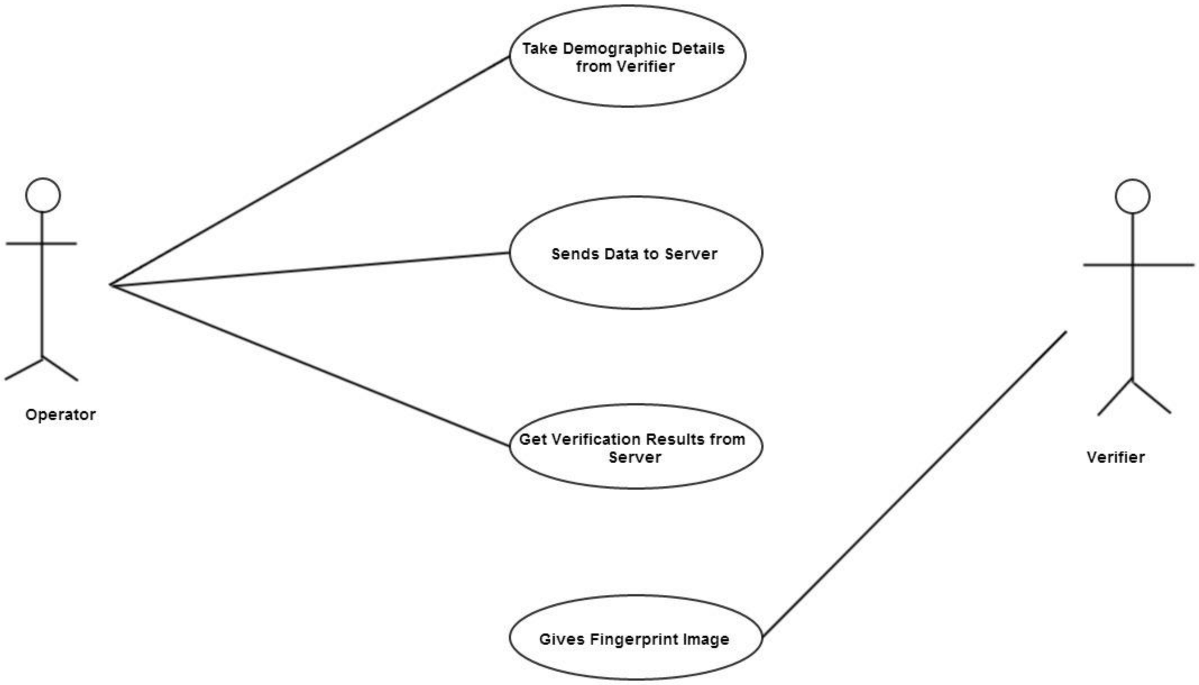

Take Demographic Details from Verifier
Sends Data to Server
Get Verification Results from Server
Gives Fingerprint Image
Operator
Verifier

Fig-6 Use Case Diagram

Table-1 Explain Use Case Components

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.

B) ER Diagram:

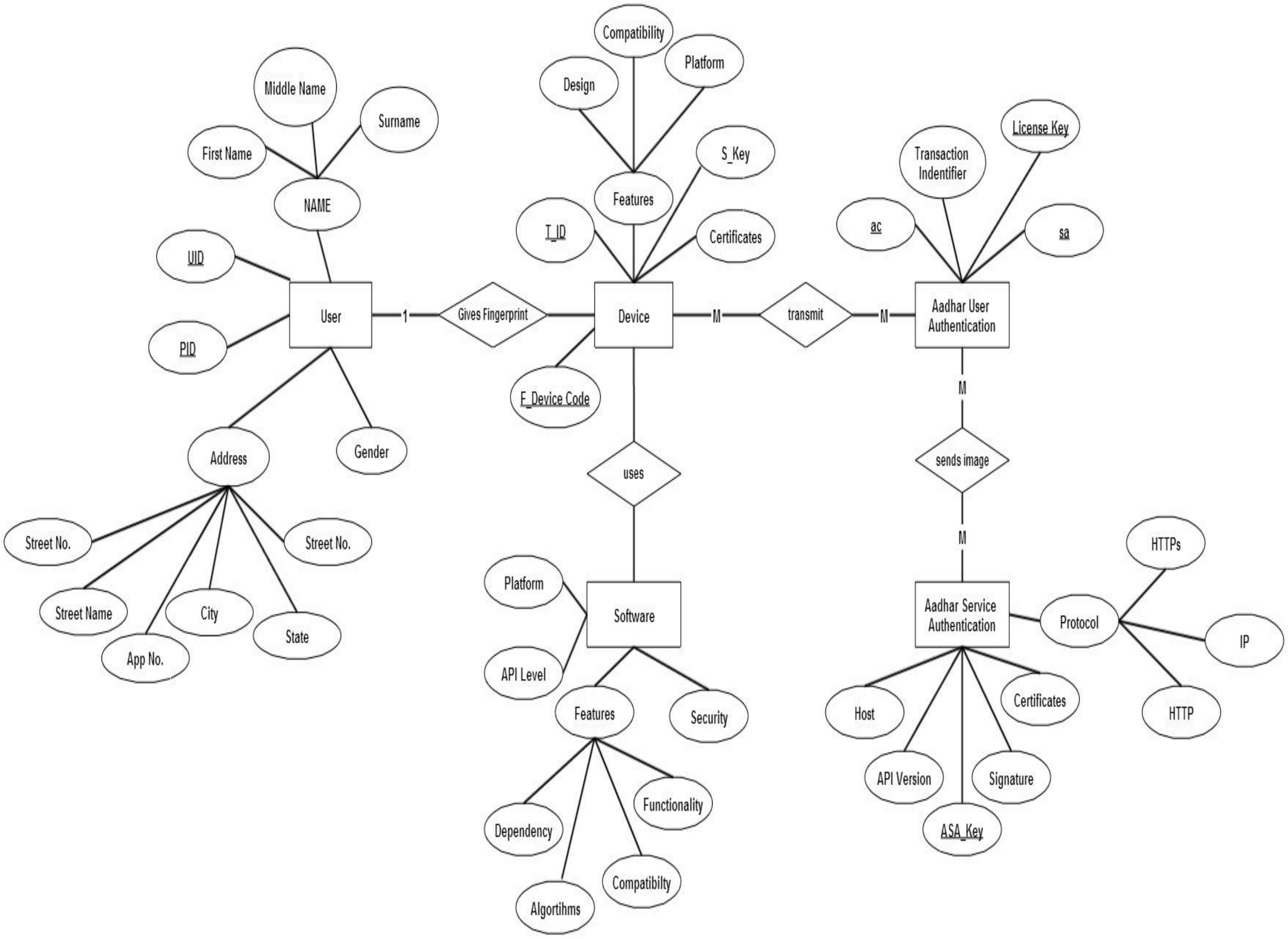


Fig-7 ER Diagram

C) Sequence Diagrams:

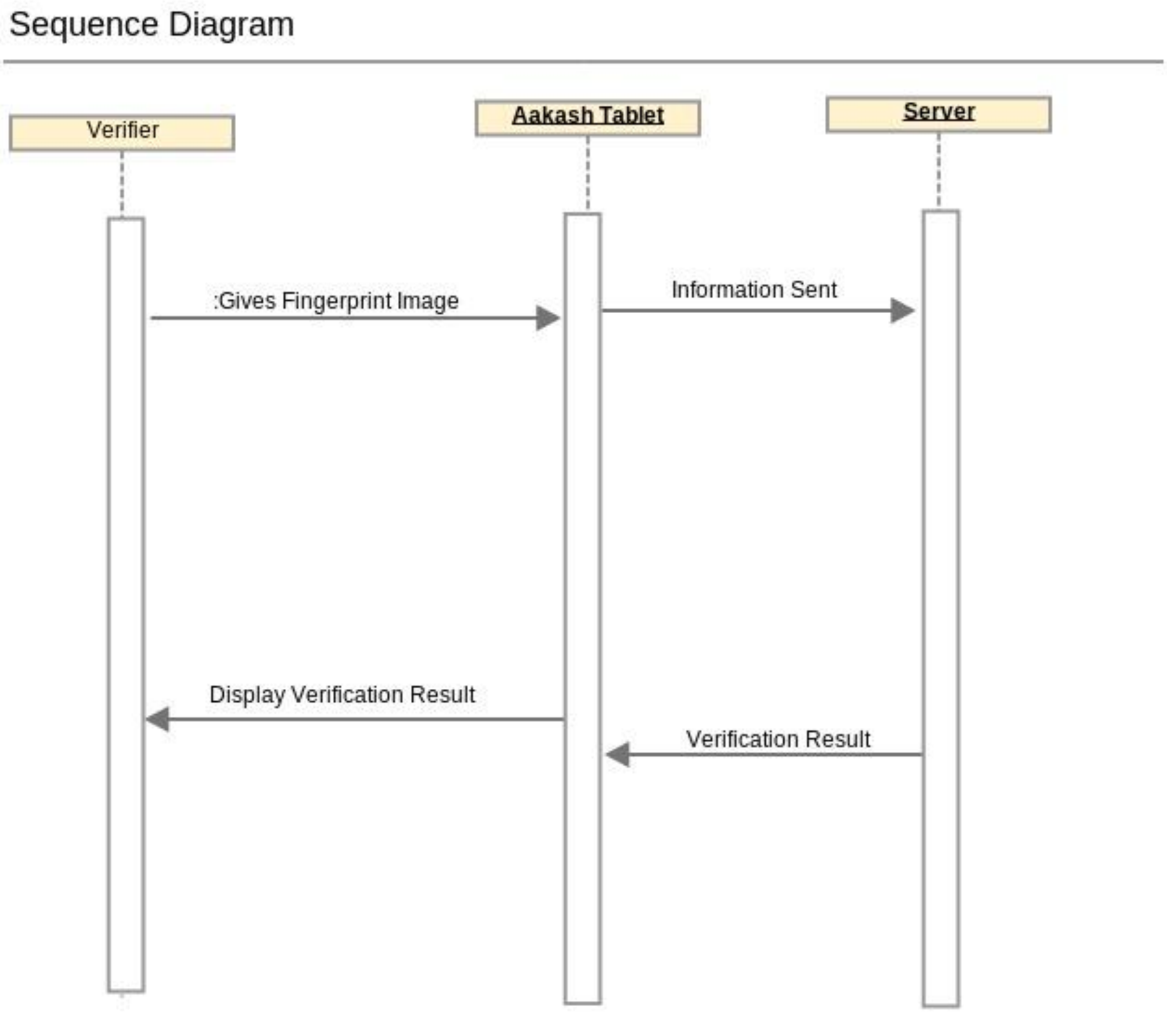
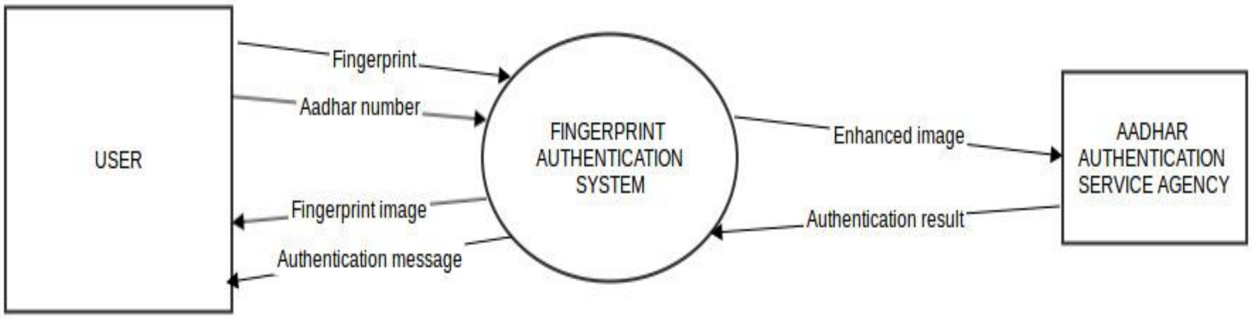


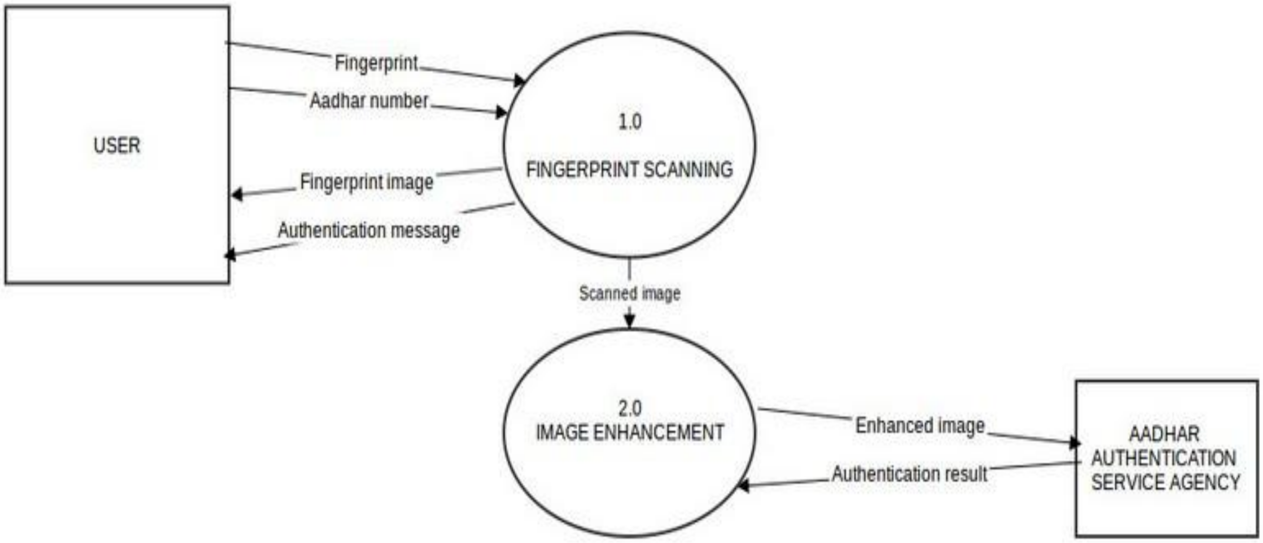
Fig-7 Sequence diagram

D) Data Flow Diagrams:

LEVEL 0 DFD



LEVEL 1 DFD



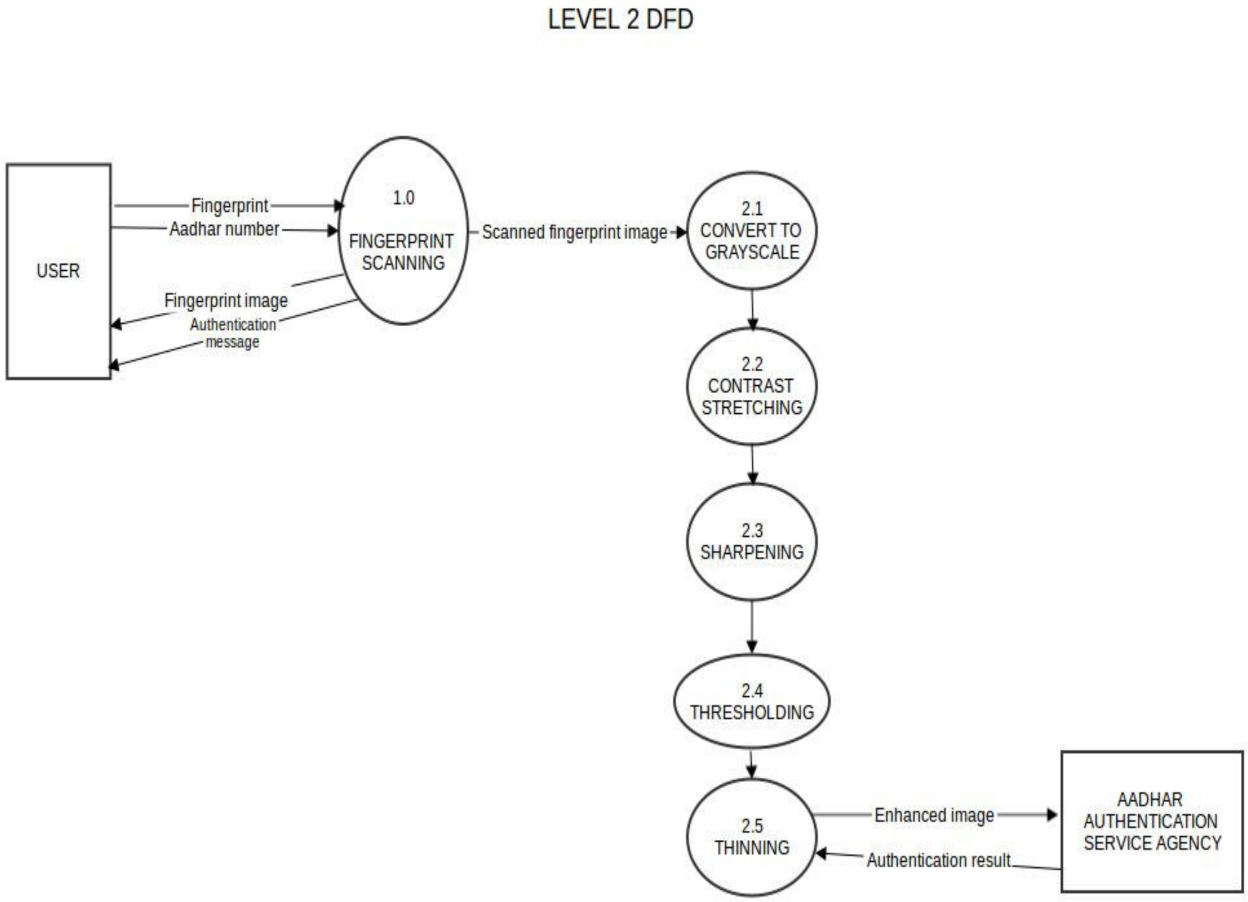

LEVEL 2 DFD
USER
Fingerprint
Aadhar number
Fingerprint image
Authentication message
1.0
FINGERPRINT SCANNING
Scanned fingerprint image
2.1
CONVERT TO GRAYSCALE
2.2
CONTRAST STRETCHING
2.3
SHARPENING
2.4
THRESHOLDING
2.5
THINNING
Enhanced image
Authentication result
AADHAR AUTHENTICATION SERVICE AGENCY

Fig-8 DFD

3.4 Non-functional Requirements:

Non-functional requirements basically include:

A) Performance:

The system must be interactive and the delays involved must be less. The loading of images on the user interface after fingerprint image has been taken should be less.

B) Safety:

On Internet service disruption while sending information to the ASAs, the verifier need not take the fingerprint image again.

C) Reliability:

The software should perform reliable identification at the server end and also the fingerprint image provided to the server should be clear enough.

D) Availability:

If the Internet service gets disrupted, while sending information to the server. The information can be sent again for verification.

E) Security:

Personal Information is first entered by the user and then is asked for fingerprint recognition. Hence, security is provided from unwanted use of recognition software.

F) Maintainability:

If the Internet service gets disrupted, while sending information to the server, the verifier need not take the fingerprint image again, as it will still be available on the tablet.

G) Compatibility:

The Software built for fingerprint image enhancement is only restricted to the usability for Android 4.0 Ice cream Sandwich Operating System.
Also the hardware built for fingerprint image recognition Is only restricted for low resolution camera.

4.0 Conclusion:

In Today's world, it is important to be secure from every possible areas which has threads of been attacked. With emerging technology the security can be much effectively used.

The reliability of any automatic fingerprint system strongly relies on the precision obtained in the minutia extraction process. A number of factors are detrimental to the correct location of minutia. Among them, poor image quality is the most serious one. In this project, we have combined many methods to build a minutia extractor and a minutia matcher. The following concepts have been used- segmentation using Morphological operations, minutia marking by specially considering the triple branch counting, minutia unification by decomposing a branch into three terminations and matching in the unified x-y coordinate system after a 2-step transformation in order to increase the precision of the minutia localization process and elimination of spurious minutia with higher accuracy.

The proposed alignment-based elastic matching algorithm is capable of finding the correspondences between minutiae without resorting to exhaustive research. There is a scope of further improvement in terms of efficiency and accuracy which can be achieved by improving the hardware to capture the image or by improving the image Enhancement techniques. So that the input image to the thinning stage could be made better this could improve the future stages and the final outcome.