# Design and Implementation of Integrated Counseling HIV Testing using AADHAR and Fingerprint Identification Technique

Vivek Girish Dhamne
UG Student, Computer Engineering
PSGVPM's D. N. Patel college of Engineering, Shahada, INDIA 425409

Vaibhav Rupesh Jain
UG Student, Computer Engineering
PSGVPM's D. N. Patel college of Engineering, Shahada, INDIA 425409

Hiren Maheshkumar Gohel
UG Student, Computer Engineering
PSGVPM's D. N. Patel college of Engineering, Shahada, INDIA 425409

Nilesh Jagdishbhai Chaudhari
UG Student, Computer Engineering
PSGVPM's D. N. Patel college of Engineering, Shahada, INDIA 425409

Purushottam R. Patil
Professor, Computer Engineering
PSGVPM's D. N. Patel college of Engineering, Shahada, INDIA 425409

Nitin K. Mandlik
District Programme Officer, MSc microbiologist with Hospital Management DYPT, DMLT
Nandurbar, INDIA 425409

## ABSTRACT
In our society AIDS disease is seen from different point of view, so person tries to hide his identity at testing centers by providing the fake personal details such as name, address and mobile number. Due to this medical course treatment is not done properly and government cannot arrange various benefits programs. Fake details provided by patient, storing the record & generating reports are some of the major problem faced in manual ICTC by Mr. Nitin Mandlik, District Programme Officer (DPO), Nandurbar. To overcome the drawback he has suggested us to develop Integrated Counselling and Testing Centers (ICTC) Database Portal. The System will help us to maintain AIDS Patient exact information with their Bio-metrics Fingerprint. It will also maintain the record of the treatment and testing reports. After implementing the system, when any patient comes to the testing centers he will be ask to scan the fingerprint on the device instead of oral details. As the scanning is finished exact information will be fetch from legal like database system i.e. AADHAR system, knowingly or unknowingly he could not give the fake details. The project is basically designed for the district level where admin is District Programme Officer. He will be responsible for the maintaining the details of technicians and patients at Testing Centre's. He can add or related information.remove the technician. The technician will be responsible for scanning patient fingerprint and fill test.

## Keywords
AADHAR, Fingerprint Identification Technique

## 1. INTRODUCTION
Testing of diseases has become increased due to the people concern about their health now a days. So it is becoming very important to make the testing process more easy and efficient. In other hand the rapid development in online platform gives rise to the development of portal on the large scale. The main reason behind the tremendous development in online portal is that the portal can be access anywhere easily and developed using open source languages. It means that the developers can have customization rights. As well as various tools are available to build and test the portal. This project is designed for the testing centers of AIDS patient only. The Human immunodeficiency Virus (HIV) and AIDS continue to be issue public health concern in spite of containment of HIV epidemic in recent times. National AIDS Control Organization (NACO), Government of India had promptly and adequately responded to this epidemic through creation of HIV laboratory network across the country. As a result, a decentralized approach of the laboratory network starting from one apex laboratory supporting the national and state reference laboratories which in turn provide technical and monitoring support to over 18000 Integrated Counselling and Testing Centers throughout the country, has been created. Though Government of India has created the ICTC throughout the country, but there is some problems that the technicians are facing at testing centers. That includes the identity of the patient, maintaining the data record of the patient manually, generating the report of the patient according to the test report status (i.e. HIV +ve/ HIV –ve) and so on. We are designing these project for resolving the above problems faced by the technicians. In this we will use the Fingerprint Recognition technique to authenticate the patient information from local AADHAR Database.

## 2. PROBLEM IDENTIFICATION
### 2.1 Problem Definition
A Portal, ICTC, is to be designed to fetch legal patient information via legal like database. Unlike other database portal systems this portal should not be just for the technician, instead it should also provide facility to ADMIN i.e. DPO to maintain portal.

This will help admin as:

- There will be no need to get new software every time to conduct patient information.

Also like other online portal, it will help technician by:

- Saving the extra time for paper work.

Also this portal will remove the flaws of existing Manual Systems like:

- Reducing the manual labor (Decreases Overheads).
- Will Increase Efficiency and Save Time.
- Will Allow Neat Handling Of Data Rather Than Error Prone Records.

The Admin/DPO will register themselves with a unique login name and password, the unique id will be issued by default the Portal.

After login:

- Admin will change their password.
- Admin add/remove technicians
- Technician can login with their credential provided by admin.
- Admin will be able to view the patients list along with their respective reports.
- Also for Technician:
- They should be able to login with their id, name and ICTC centers.
- Also they should be able to view patient's reports and information.

Fingerprint Recognition Technique is to be used for authenticating the person personal information from a legal AADHAR database.

## 2.2 Existing System

The problems of the Manual System of ICTC are:

**a)** Not user friendly: The existing system is not user friendly because the retrieval and storing of data is slow and data is not maintained efficiently.

**b)** Manual operator control: Manual operator control is there and lead to a lot of chaos and errors.

**c)** Lot of paperwork: Existing system requires lot of paper work. Moreover any unnatural cause (such as fire in the organization) can destroy all data of the organization. Loss of even a single paper led to difficult situation because all the papers are interrelated.

**d)** Poor identification of patient: In exiting system patient tries to hide information such as name, address, mobile number, etc, because in our society this disease is seen from some different point of view so to escape from this they provide fake details.

**e)** Difficulty in reports generating: Reports generating in a current system are generated with great difficulty. It take time to generate report in the current system.

## 2.3 Need For The New System

In order to solve these problems there is a need of ICTC Portal in addition to manual ICTC system. After implementing this system, patient information will be filled from local AADHAR database by verifying the patient biometric fingerprint which will avoid the patient fake information.

In this system at testing centers patient's data is recorded, stored and processed primarily as digital information. If a secure and convenient system is provided, it will be used more frequently to collect patient's information through cyberspace. Traditional paper-based generating and maintaining test reports can be time consuming and inconvenient. This system not only accelerates the whole process, but makes it less expensive and more comfortable for the patients and the technicians as well. It also, reduces the chances of the errors. This system will provide all basic features that traditional system does, further will furnish more services in order to make the process more trusted and secure.

# 3. FINGERPRINT BIOMETRIC

Biometrics is the identification of an individual using a distinctive aspect of their biology or behavior. Two same types biometric property (traits) of different person can't be matched. It is divided in two characteristic (i) Physiological and (ii) behavioral. Behavioral aspect includes speech, keyboard typing, Signature and Physiological includes fingerprint, hand, eyes and face.

## 3.1 Fingerprint Identification Terminology

Fingerprints are extremely complex. Defining characteristics are used, many of which have been established by law enforcement agencies, to "read" and classify fingerprints. Even though biometrics companies like Digital Persona do not save images of fingerprints and do not use the same manual process to analyze them, many of the same methodologies established over the years in law enforcement are used for our digital algorithms.

Biometric systems authenticate users by comparing the ridges and patterns on the finger. To break it down further, the software looks for distinctions within these areas:

**Ridges**

The skin on the inside surfaces of our hands, fingers, feet, and toes is "ridged" or covered with concentric raised patterns. These ridges are called friction ridges and they provide friction making it easier for us to grasp and hold onto objects and surfaces without slippage. It is the many differences in the way friction ridges are patterned, broken, and forked which make ridged skin areas, including fingerprints, distinctive.

**Global Features**

Pattern Area – The pattern area is the part of the fingerprint that contains the global features. Fingerprints are read and classified based on the information in the pattern area. Certain minutia points that are used for final recognition might be outside the pattern area.

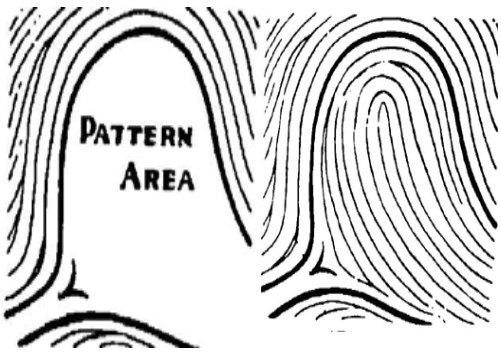


**Figure 1. Pattern Area**

**Core Point --** The core point, located at the approximate center of the finger impression, is used as a starting reference point for reading and classifying the print.

**Type Lines –** Type lines are the two innermost ridges that start parallel, diverge, and surround or tend to surround the pattern area. When there is a definite break in a type line, the ridge immediately outside that line is considered to be its continuation.

**Delta –** The delta is the point on the first bifurcation (where the ridge forks into two different directions), abrupt ending ridge, and meeting of two ridges, dot, fragmentary ridge, or any point upon a ridge at or nearest the center of divergence of two type lines. The delta is located directly in front of the line's point of divergence. It is a definite fixed point used to facilitate ridge counting and tracing.

**Figure 2. Delta**

**Ridge Count –** The ridge count is most commonly the number of ridges between the delta and the core. To establish the ridge count, an imaginary line is drawn from the delta to the core; each ridge that touches this line is counted.

**Basic Ridge Patterns**
To make fingerprints easier to search against large fingerprint databases, experts categorize fingerprints into groups based on patterns in the ridges. These groupings or basic ridge patterns are not sufficient for identification in themselves, but they help narrow down the search and speed up the processing time. Once a fingerprint is identified as a particular group like a whorl, the search only continues to compare the print to all other whorl types in the database and ignores the other groupings.

There are a number of basic ridge pattern groupings which have been defined. Three of the most common are loop, arch, and whorl.

**1. LOOP**
The loop is the most common type of fingerprint pattern and accounts for about 65% of all fingerprints.

**2. ARCH**
The arch pattern is a more open curve than the loop. There are two types of arch patterns – the plain arch and the tented arch.

**3. WHORL**
Whorl patterns occur in about 30% of all fingerprints and are defined by at least one ridge that makes a complete circle.

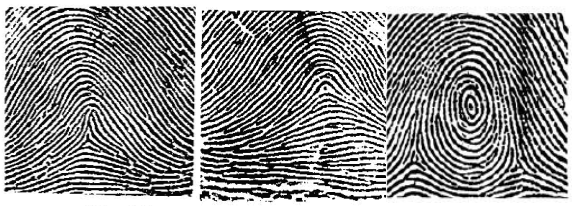

**Figure 3. Loop, Arch & Whorl**

Certain biometric products base identification on correlation of global ridge patterns, or matching one fingerprint pattern image to another. Digital Persona believes that high quality fingerprint recognition algorithms must go one step further making the algorithm based on minutia points in addition to global features.

**Minutia Points**
Fingerprint ridges are not continuous, straight ridges. Instead, they are broken, forked, interrupted or changed directionally. The points at which ridges end, fork, and change are called minutia points which provide distinctive, identifying information.

There are five characteristics of minutia points in fingerprints:

**1. Type**
There are several types of minutia points. The most common are ridge endings and ridge bifurcations.

**Ridge Ending –** occurs when a ridge ends abruptly.

**Ridge Bifurcation –** the point at which a ridge divides into branches.

**Dot or Island –** a ridge that is so short it appears as a dot.

**Enclosure –** a ridge that divides into two and then reunites to create an enclosed area of ridge-less skin.

**Short Ridge –** an extremely short ridge, but not so short that it appears as a Dot or an Island.

**2. Orientation**
The point on the ridge on which a minutia resides is called the orientation of the minutia point.

**3. Spatial Frequency**
Spatial frequency refers to how far apart the ridges are in relation to the minutia point.

**4. Curvature**
The curvature refers to the rate of change of ridge orientation.

**5. Position**
The position of the minutia point refers to its location, either in an absolute sense or relative to fixed points like the delta and core points.

## 3.2 Fingerprint Recognition

The Digital Persona fingerprint recognition system uses the processes of fingerprint enrollment and fingerprint verification, which are illustrated in the block diagram in Figure 4. Some of the tasks in these processes are done by the fingerprint reader and its driver; some are accomplished using One Touch for Windows: COM/ActiveX Edition API functions, which use the Engine; and some are provided by your software application and/or hardware.

### 3.2.1 Fingerprint Enrolment

Fingerprint enrollment is the initial process of collecting fingerprint data from an enrollee and storing the resulting data as a fingerprint template for later comparison. The following procedure describes typical fingerprint enrollment. (Steps preceded by an asterisk are not performed by the One Touch for Windows SDK: COM/ActiveX Edition.)

a) *Obtain the enrollee's identifier (Subject Identifier).

b) Capture the enrollee's fingerprint using the fingerprint reader.

c) Extract the fingerprint feature set for the purpose of enrollment from the fingerprint sample.

d) Repeat steps 2 and 3 until you have enough fingerprint feature sets to create a fingerprint template.

e) Create a fingerprint template.

f) *Associate the fingerprint template with the enrollee through a Subject Identifier, such as a user name, email address, or employee number.

g) *Store the fingerprint template, along with the Subject Identifier, for later comparison.

Fingerprint templates can be stored in any type of repository that you choose, such as a fingerprint capture device, a smart card, or a local or central database.

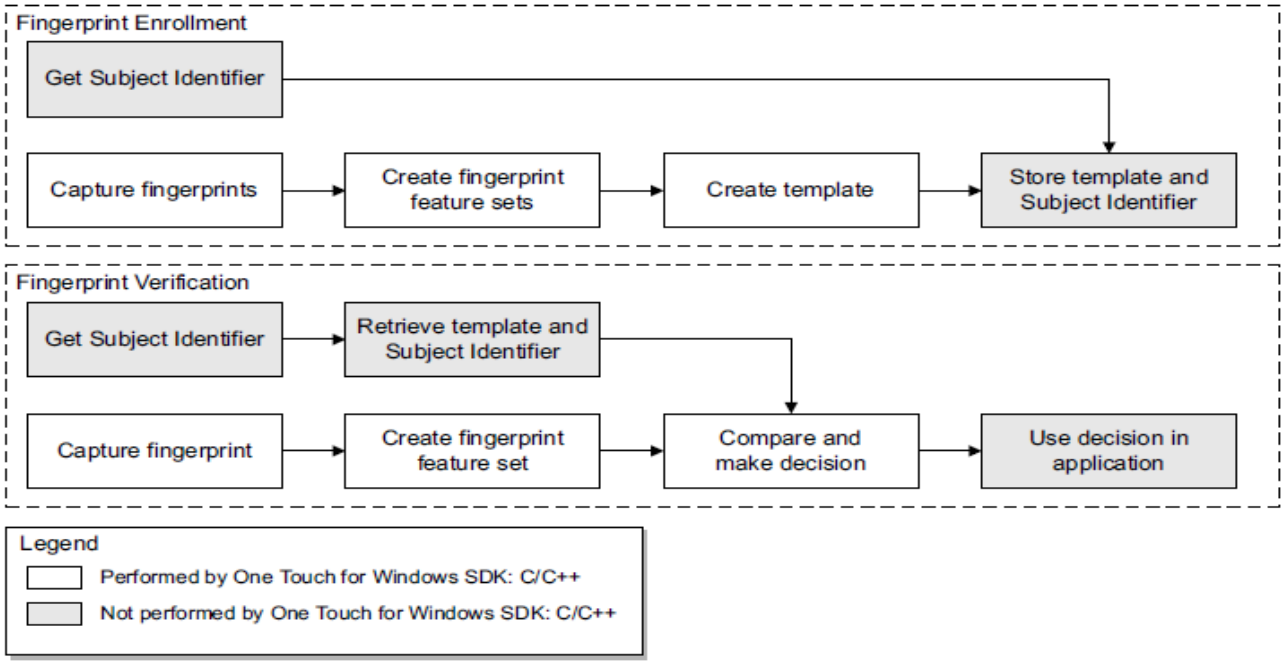


**Figure 4. Fingerprint Recognition System**

### 3.2.2 Fingerprint Verification

Fingerprint verification is the process of comparing the fingerprint data to the fingerprint template produced at enrollment and deciding if the two match. The following procedure describes typical fingerprint verification. (Steps preceded by an asterisk are not performed by the One Touch for Windows SDK: COM/ActiveX Edition.)

a) *Obtain the Subject Identifier of the person to be verified.

b) Capture a fingerprint sample using the fingerprint reader.

c) Extract a fingerprint feature set for the purpose of verification from the fingerprint sample.

d) *Retrieve the fingerprint template associated with the Subject Identifier from your repository.

e) Perform a one-to-one comparison between the fingerprint feature set and the fingerprint template, and make a decision of match or non-match.

f) *Act on the decision accordingly, for example, unlock the door to a building for a match, or deny access to the building for a non-match.

### 3.2.3 False Positive and False Negative

Fingerprint recognition systems provide many security and convenience advantages over traditional methods of recognition. However, they are essentially pattern recognition systems that inherently occasionally make certain errors, because no two impressions of the same finger are identical. During verification, sometimes a person who is legitimately enrolled is rejected by the system (a false negative decision), and sometimes a person who is not enrolled is accepted by the system (a false positive decision).

The proportion of false positive decisions is known as the false accept rate (FAR), and the proportion of false negative decisions is known as the false reject rate (FRR). In fingerprint recognition systems, the FAR and the FRR are traded off against each other, that is, the lower the FAR, the higher the FRR, and the higher the FAR, the lower the FRR.

A One Touch for Windows: COM/ActiveX Edition API function enables you to set the value of the FAR, also referred to as the security level, to accommodate the needs of your application. In some applications, such as an access control system to a highly confidential site or database, a lower FAR is required. In other applications, such as an entry system to an entertainment theme park, security (which reduces ticket fraud committed by a small fraction of patrons by sharing their entry tickets) may not be as significant as accessibility for all of the patrons, and it may be preferable to decrease the FRR at the expense of an increased FAR.

It is important to remember that the accuracy of the fingerprint recognition system is largely related to the quality of the fingerprint. Testing with sizable groups of people over an extended period has shown that a majority of people have feature-rich, high-quality fingerprints. These fingerprints will almost surely be recognized accurately by the Digital Persona Fingerprint Recognition Engine and practically never be falsely accepted or falsely rejected. The Digital Persona fingerprint recognition system is optimized to recognize fingerprints of poor quality. However, a very small number of people may have to try a second or even a third time to obtain an accurate reading. Their fingerprints may be difficult to verify because they are either worn from manual labor or have unreadable ridges. Instruction in the proper use of the fingerprint reader will help these people achieve the desired results.

## 4. PROPOSED SYSTEM

The proposed system based on fingerprint template matching as authentication techniques in ICTC. It focuses on the endings of ridges and bifurcations. Consequently the central area in fingerprint image is very important and this techniques keenly relies on the quality of the input images. Systems detect the fingerprint using a biometrics fingerprint scanner and recognize it from local AADHAR database and check for

the two template matches. If a match occurs, the patient personal information such as name, address, etc. will be fetch which will be filled automatically in the forms designed and then technician will fill rest of medical test related information.

## 4.1 System Architecture

The System Architecture of ICTC is shown in the figure 6 There are three layers Client, Application and Database Layer. The Admin and Technicians are the user of the system at the client side. There are various module at the application layer that are DPO module, Report Generation Module, Fingerprint Authentication Module and ICTC Module. An ICTC is a system in which all data is recorded, stored and processed primarily as digital information into the ICTC database. The local Aadhar Database is use for fetching the patient personal information by comparing the image capture using the fingerprint scanner. The DPO database will only contain the details of DPO.

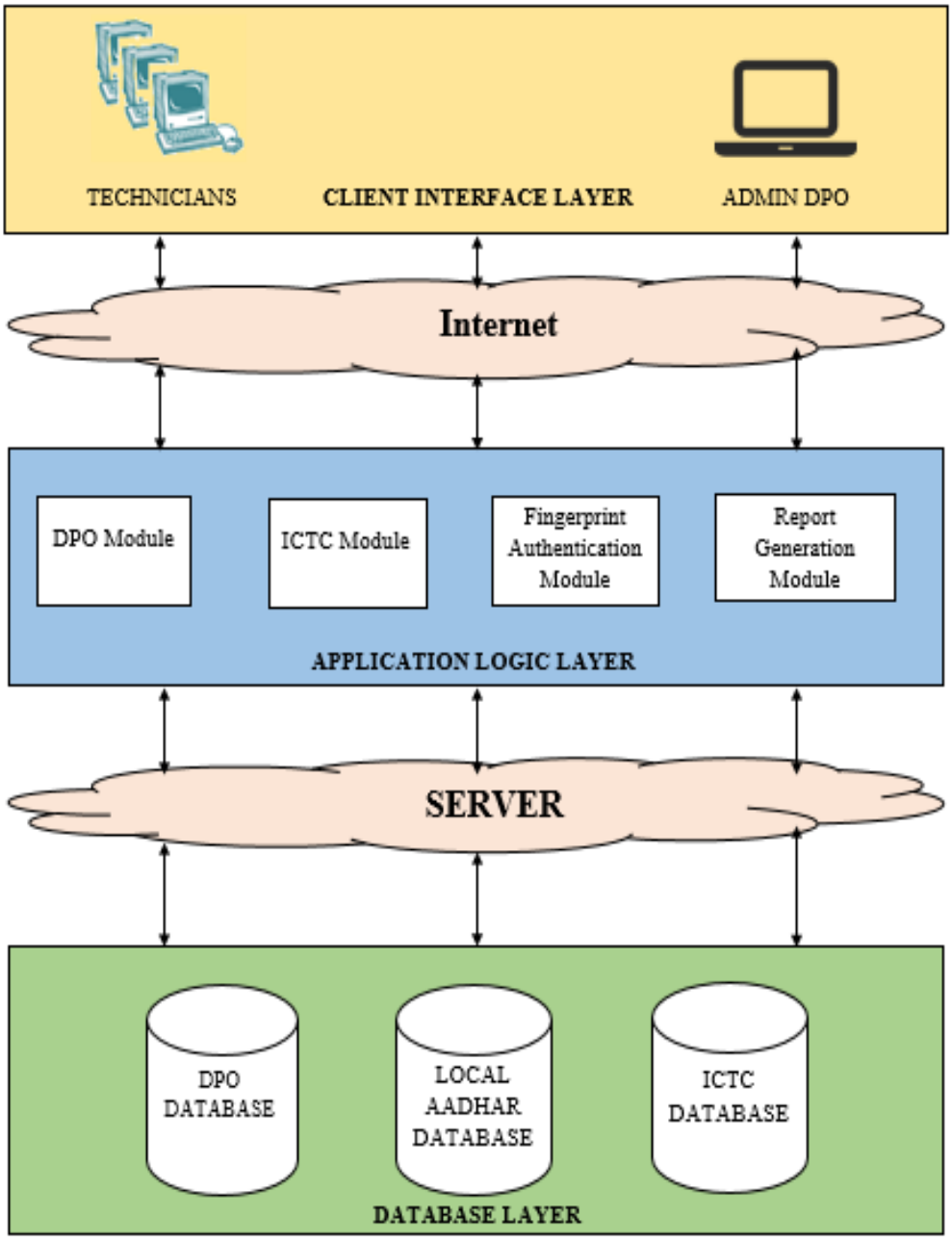


**Figure 5. System Architecture**

## 4.2 Functional Modules

### [1] ADMIN MODULE

DPO is the system administrator who controls the entire ICTC. Responsible for storing the information of the new technicians & also modify or delete any technician's information. Administrator can see the results of the patient who are HIV POSITIVE and HIV NEGATIVE with graphical data representation.

### [2] ICTC MODULE

It is the most important module where technician plays an important role. They fill test related information and update it to respective database. They also conduct the fingerprint scan

of the patient using scanner to identify the identity of the patients.

### [4] FINGERPRINT AUTHENTICATION MODULE

This module to authenticate the patient real information details by scanning their fingerprint and matching it with the template in the database.

### [4] REPORT GENERATION MODULE

This module will generate the report of the patients who has been found HIV+ve. The generated report will be helpful for the government to provide proper medical treatment and arranging various benefit programs.

### [5] LOCAL AADHAR DATABASE

As we are not getting access to the legal AADHAR database, the local database is developed. This database will be working somewhat similar to the actual database. There will be all necessary fields such as name, date-of-Birth, address, mobile number, etc. As we are dealing with Fingerprint authentication there will be only fingerprint field.

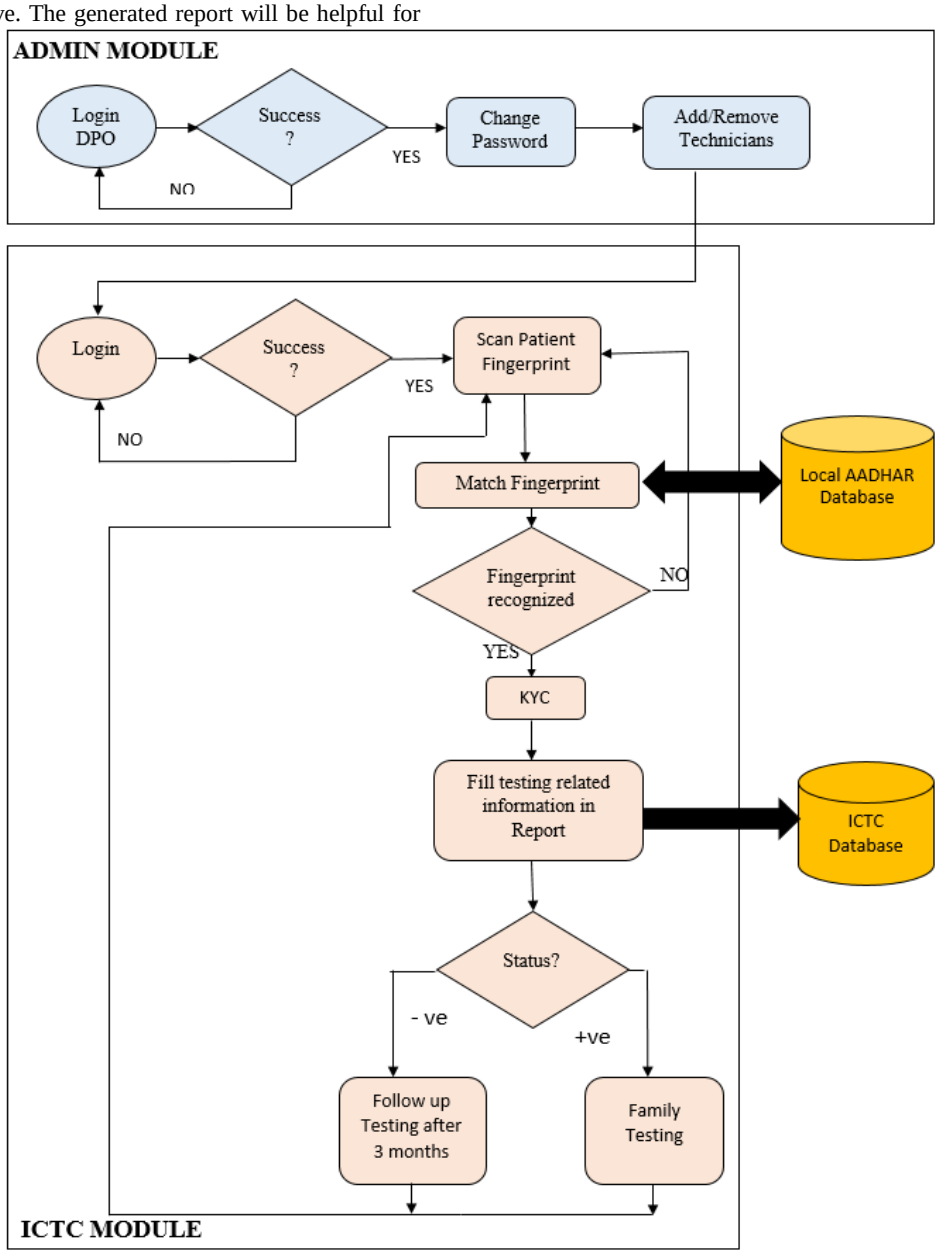


**Figure 6. Working Flow of ICTC**

# 5. IMPLEMENTATION

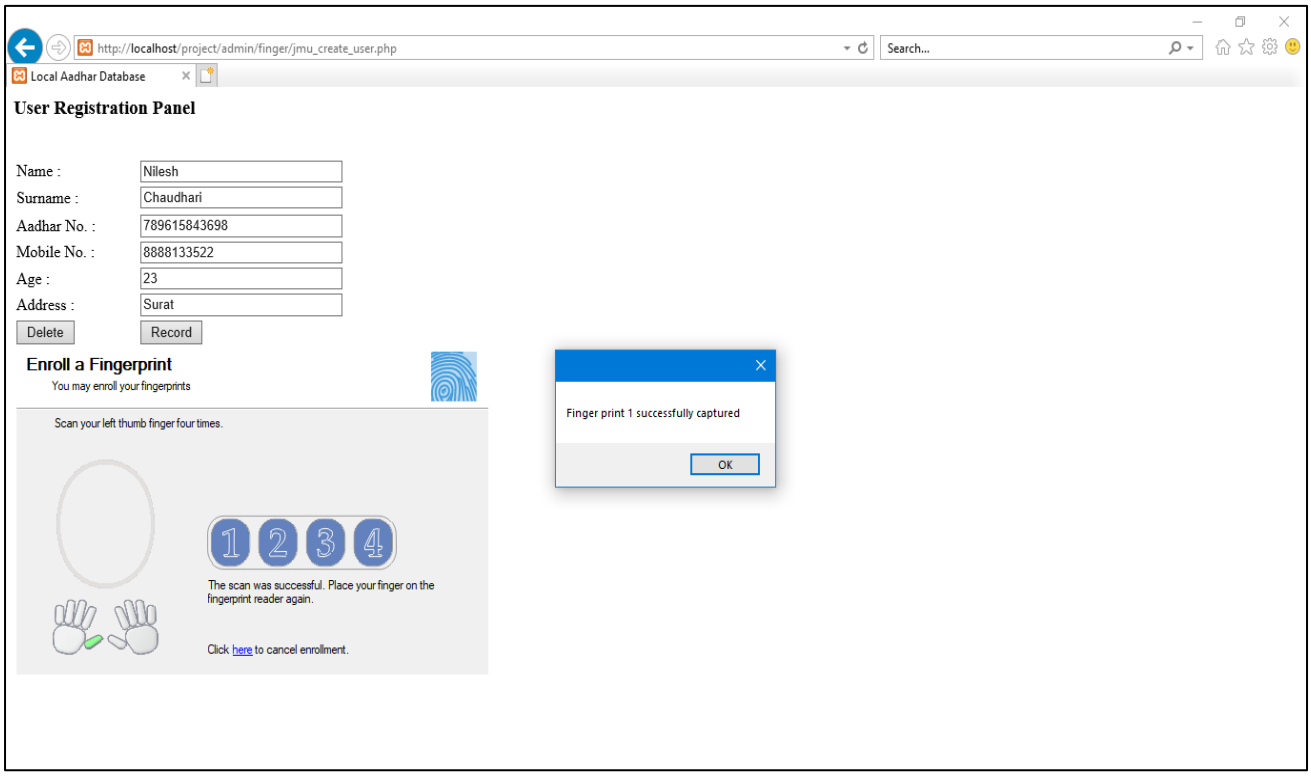


**Figure 7. LOCAL AADHAR Database**

It is the local AADHAR Database form, shown in the Figure 8, having the field required for registering person details for authentication. It will be used for storing the AADHAR details.

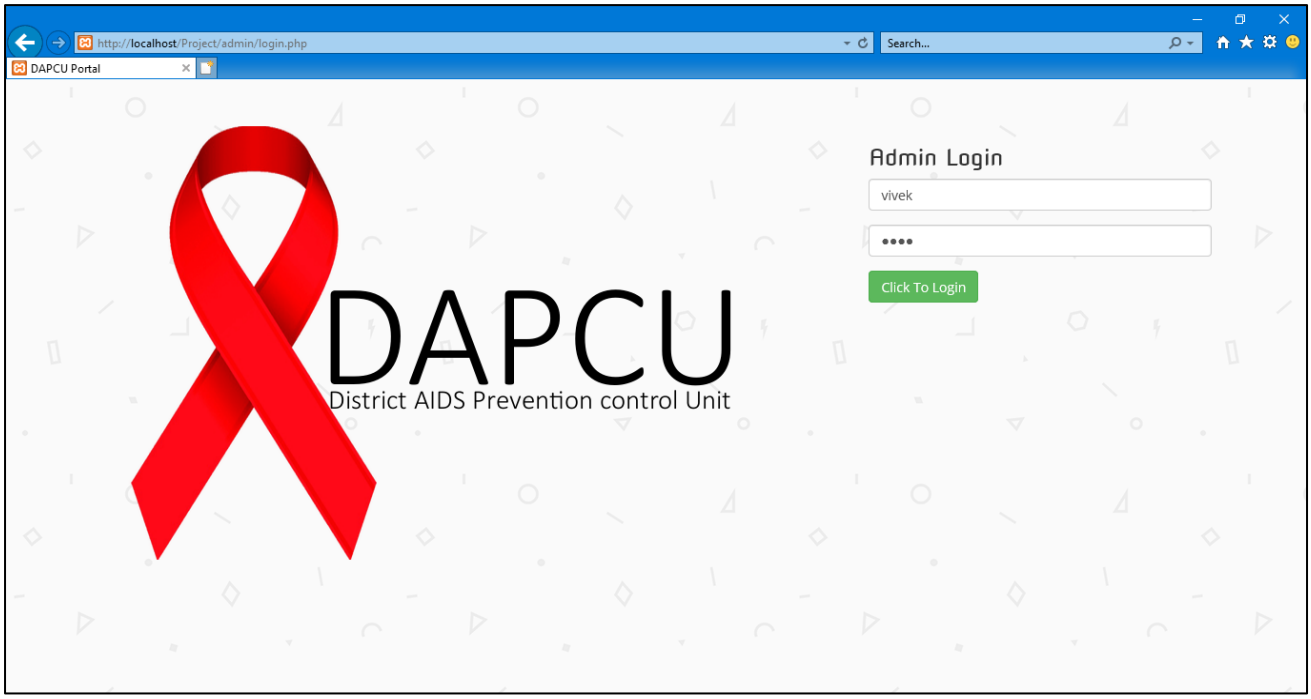


**Figure 8. Admin Page**

It is the Admin Page of the DPO, shown in Figure 8, after login it will redirect to the main Home page of the site. The ICTC login page design is also somewhat similar.

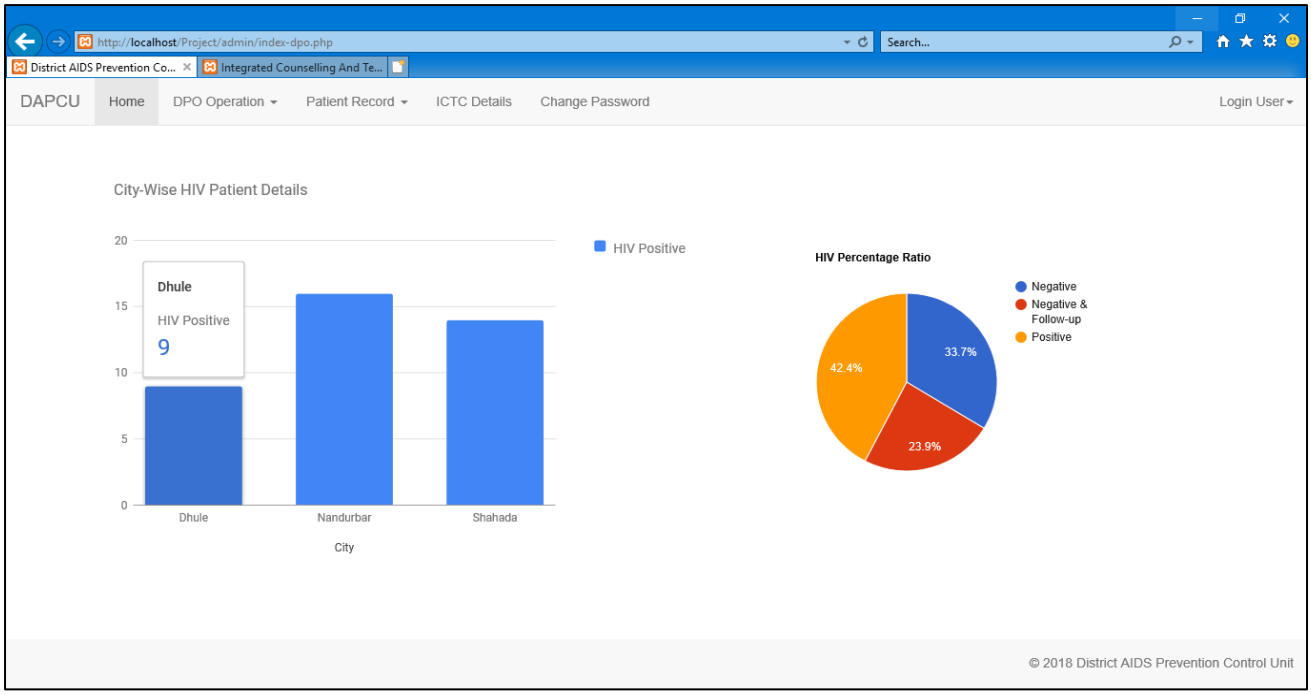


**Figure 9. Home Page**

It is the Home page, shown in Figure 9, having all the feature options to the website. It also show data representation in graphical form. Performing the basic operation such Add, Delete, Edit, etc.

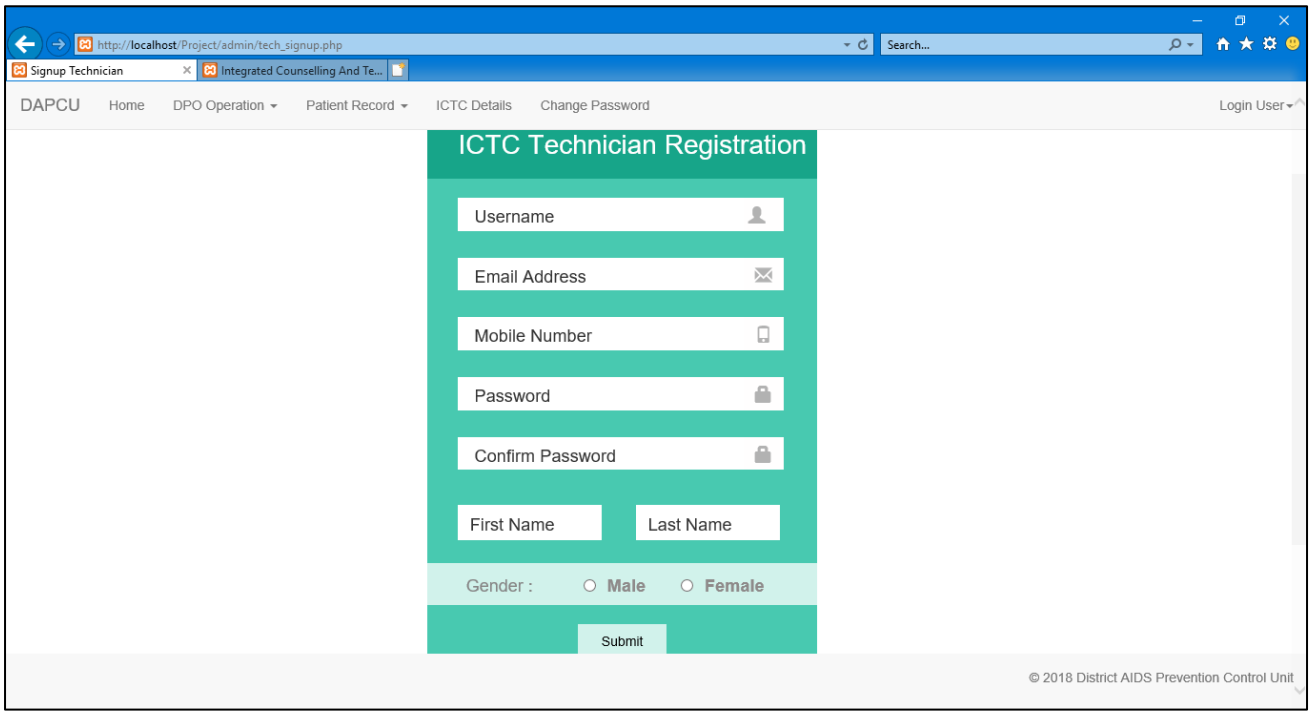


**Figure 10. Signup for Technician**

It is the Signup form for technician, shown in Figure 10, the technician will be allow to login only after the DPO had assign the username and password to it.

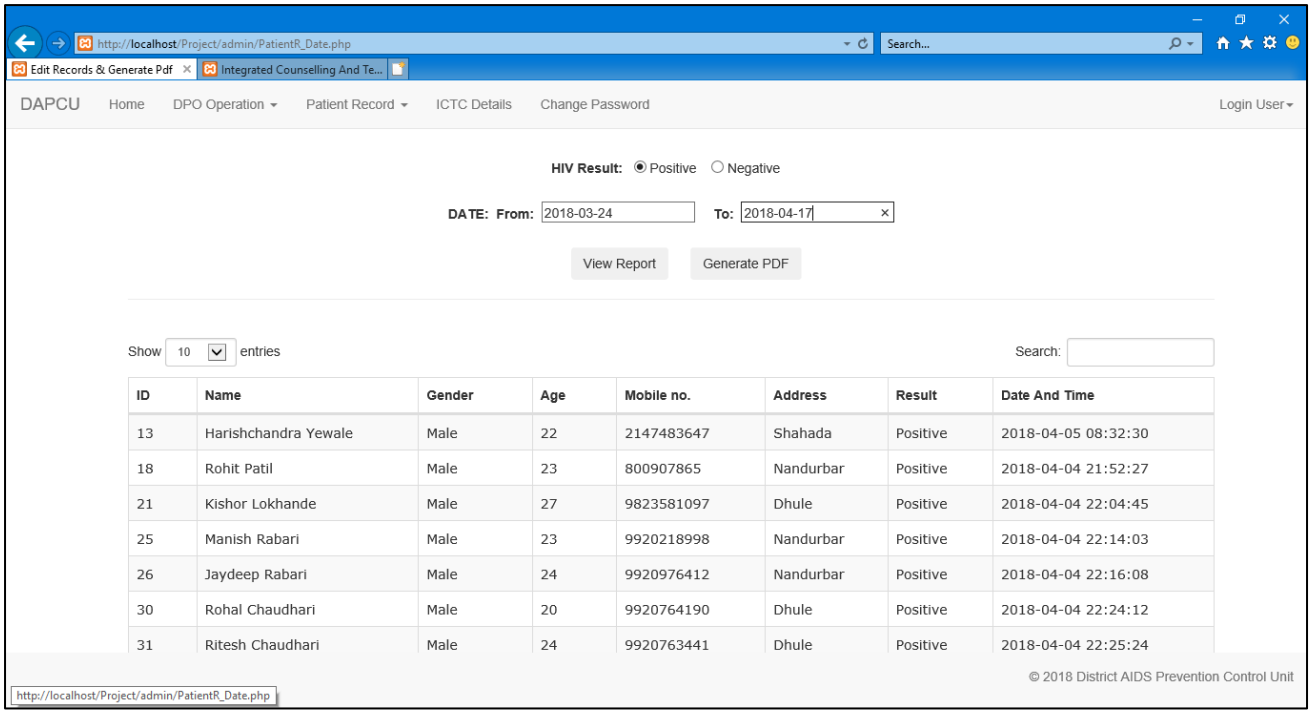


**Figure 11. View Report & Generate PDF date-wise**

It is the Date-wise Report generating form, shown in Figure 11, the DPO can only generate the date-wise report and maintaining the patient details according to the test result status.

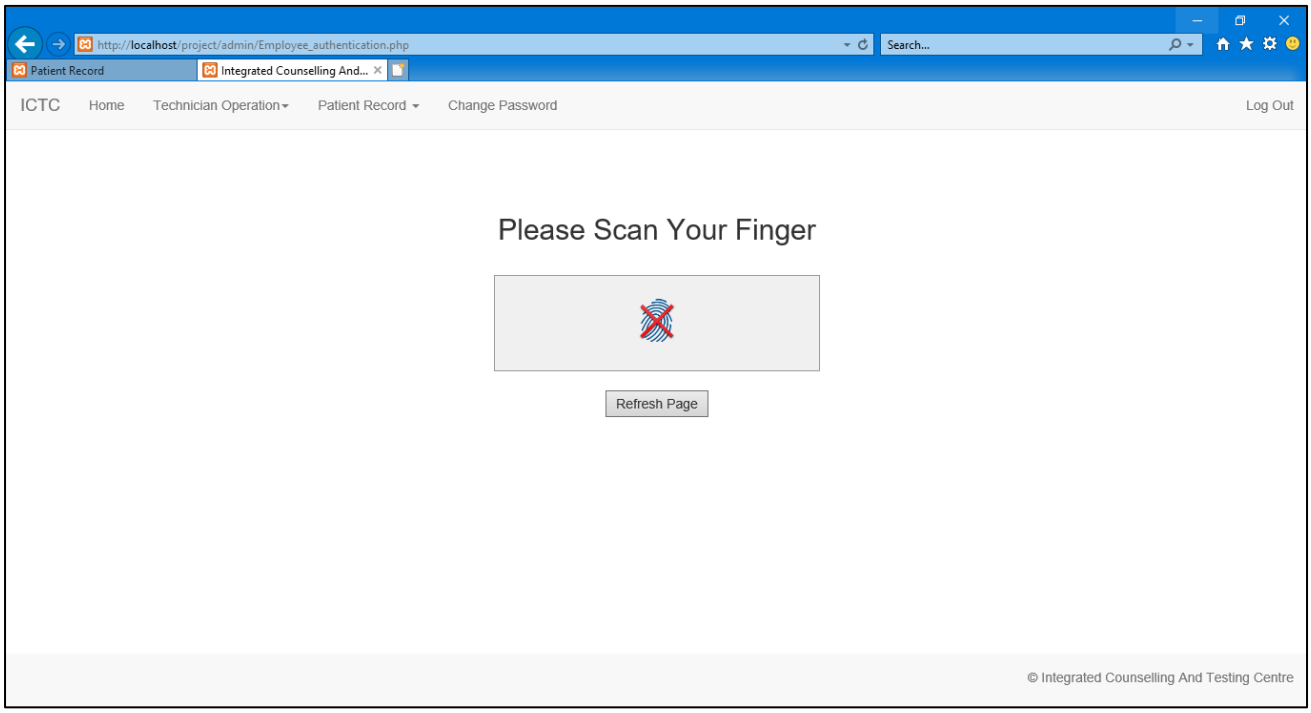


**Figure 12. Patient Finger Scan**

It is the patient finger scan page, shown in Figure 12, technician will scan patient's finger on fingerprint scanner if fingerprint matches with Local AADHAR Database fingerprint template then it will be redirect to test form.

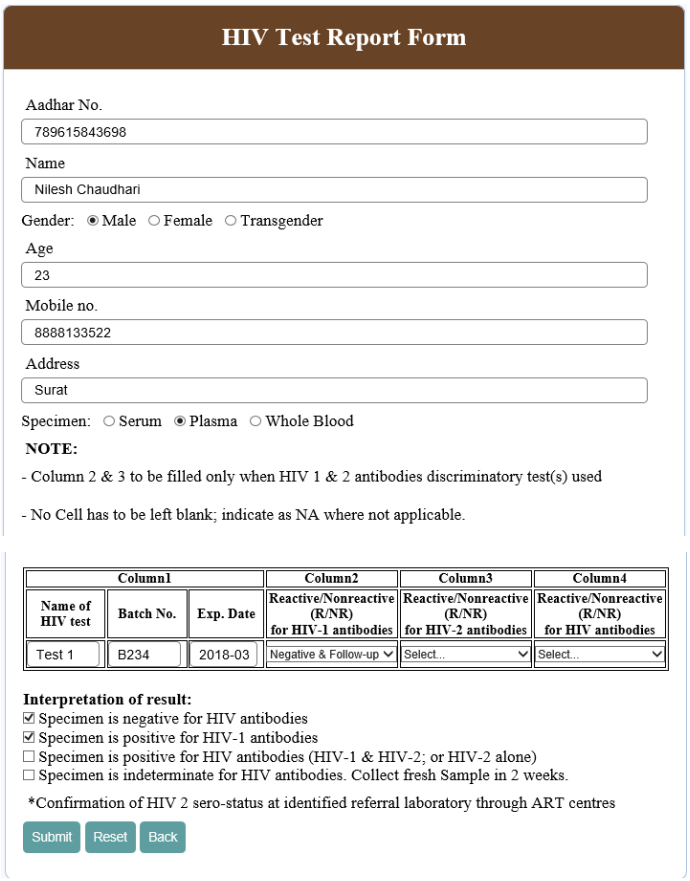


**Figure 13. Test Report**

It is main test report form, shown in Figure 13, as the fingerprint authentication is done successfully the personal details will be fetch from the database and technician will fill the remaining test-related details and generate the report.

## 6. RESULT

The Proposed System is fully automated compared to the existing system as shown in the table 1.1. System serve more advanced feature than existing system. In this system, patient's data is recorded, stored and processed primarily as digital information. The time required by technician in existing system to fill test report was 30-35 min based on the technician capability. In proposed system it takes only 05-10 min. Filling test details in less time has increases the efficiency of the system. Patient Identification was inaccurate in existing system as there was no Legal database to authenticate but now due to the presence of Local AADHAR Database it is highly accurate. The overall performance of the system is extremely good than existing system.

**Table 1: Comparison of Manual ICTC vs. Proposed System**

| | **Time Accuracy** | **Efficiency** | **Fill Test Report** | **Reliable** | **Performance** | **Patient Identification** | **Legal AADHAR Database** |
|---|---|---|---|---|---|---|---|
| **Manual ICTC** | 30-35 min | Low | Slow | Consistently Worst | Low | Less Accurate | No |
| **Proposed System (Automated)** | 05-10 min | High | Fast | Consistently Good | High | Highly Accurate | Yes |

## 7. CONCLUSION

The complete system is thoroughly tested with the availability of data and throughput reports which are prepared manually. Design Procedure and output reports are presented in this paper. The design is easy to understand so that any new module can be incorporated easily.

- It has been designed only for district level work, in future it can be designed and implemented for state, and national level health organization like WHO.
- At present our system support Microsoft IE 8.0 and above, in future it can support all browser for fingerprint authentication (Mozilla Firefox, Opera, Google Chrome etc.)

- Future improvement in developed system can pay closer attention to the more efficiency & high security of the system.
- Optimizing the patients large data stored in the database to avoid the crash of the system.
- System can provide two step authentication to the user.

## 8. REFERENCES

[1] Cynthia D'Souza N, Leeda Jovita Rodrigues and Nausheeda B.S, "A Survey On Fingerprint Recognition Techniques", International Journal of Latest Trends in Engineering and Technology, Issue SACAIM 2016, pp. 441-447 e-ISSN: 2278-621X.

[2] Mehnaz Tabassum, "A New Method for Biometric Based Recognition", International Journal of IJCA

[3] Scientific and Research Publications, Volume 3, Issue 9, September 2013, ISSN 2250-3153

[4] "One Touch® for Windows® SDK COM/ActiveX® Developer Guide", Version 1.6, June 22, 2010.Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems.

[5] M.Abinaya, K.Gowthami, M.Abinaya, "ONLINE VOTING SYSTEM POWERED BY AADHAR AUTHENTICATION", Vol-3 Issue-2 2017, IJARIIE-ISSN(O)-2395-4396

[6] Mrs. Hemlata Patel, Pallavi Asrodia, "Fingerprint Matching Using Two Methods", Vol. 2, Issue 3, May-Jun 2012, ISSN: 2248-9622

[7] Roger S. Pressman, "Software Engineering: A Practitioner's Approach", Fifth Ed., MGH, ISBN 0-07-365578-3