# EFFECTIVENESS OF BIOMETRIC TECHNOLOGIES FOR ATTENDANCE AUTHENTICATION SYSTEM A COMPARATIVE STUDY AMONG EDUCATIONAL INSTITUTIONS IN COIMBATORE


**By**

**SURYA G**

**Roll No.: 0906MBA1830**

**Reg. No.: 68309200389**


A PROJECT REPORT

Submitted to the

**FACULTY OF MANAGEMENT SCIENCES**

*in partial fulfillment for the award of the degree*

*of*

**MASTER OF BUSINESS ADMINISTRATION**


**CENTRE FOR DISTANCE EDUCATION**

**ANNA UNIVERSITY CHENNAI**

**CHENNAI 600 025**


August, 2011

## BONAFIDE CERTIFICATE

Certified that the Project report titled "**EFFECTIVENESS OF BIOMETRIC TECHNOLOGIES FOR ATTENDANCE AUTHENTICATION SYSTEM - A COMPARATIVE STUDY AMONG EDUCATIONAL INSTITUTIONS IN COIMBATORE**" is the bonafide work of **Miss. Surya G** who carried out the work under my supervision. Certified further that to the best of my knowledge the work reported herein does not form part of any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

Signature of Student

Name: Surya G
Roll No.: 0906MBA1830
Reg. No.: 68309200389

Signature of Guide

Name: Mr. V.Kaarthiekheyan,
Designation: Assistant Professor,
KCT Business School,
Address: Kumaraguru College of Technology,
Coimbatore - 49, Tamilnadu.

Signature of Project Incharge
Name: Dr .V. R. Nedunchezhian
Designation: Professor, KCT Business School,
Address: Kumaraguru College of Technology,
Coimbatore - 49, Tamilnadu.

**Certificate of Viva-voce-Examination**

This is to certify that Miss. SURYA G (Roll No. 0906MBA1830; Register No. 68309200389) has been subjected to Viva-voce-Examination on 10.09.2011 (Date) at 11.45 Am (Time) at the Study centre KUMARAGURU COLLEGE OF TECHNOLOGY, COIMBATORE - 49, TAMIL NADU.

KUMARAGURU COLLEGE OF TECHNOLOGY ★ KCT STUDY CENTRE ★ COIMBATORE-6

**Internal Examiner**

Name: Mr. A. Senthil kumar,

Designation: Assistant professor (Senior Grade),

Address: KCT Business School, Kumaraguru college of Technology, Coimbatore - 49.

**External Examiner**

Name: Dr. N. Senthil Kumar,

Designation: Assistant professor (Senior Gra

Address: Department of Manage - nt Stu Anna University, Chennai - 600 025.

for

**Coordinator**
**Study centre**

Name: Dr.Vijila Kennedy

Designation: Professor & Director

Address: Kumaraguru College of Technology,

Coimbatore - 49, Tamilnadu.

# ABSTRACT

Biometrics can be defined as measurable physiological and/or behavioral characteristics that can be utilized to verify the identity of an individual, and include fingerprint verification, hand geometry, retinal scanning, iris scanning, facial recognition and signature verification. Biometric authentication is considered the automatic identification, or identity verification, of an individual using either a biological feature they possess. Traditionally, attendance is taken manually by using attendance sheet and not a system. With this manual system, there are some cases that person can cheat by asking their friends to tick or sign for them. Because of this problem, a system may be needed in order to records the attendance more accurately without have to trace manually by Administration .This paper discusses the effectiveness of Biometric technologies used for Attendance authentication System. This study uses the questionnaire method and conduct the survey among educational institutions in Coimbatore in order to evaluate the effectiveness of Biometric technologies used for Attendance authentication System. A detailed study is performed to check whether the current Biometric systems satisfy the requirements.

# ACKNOWLEDGEMENT

I express my sincere gratitude to our beloved Director, Centre for Distance Education, Anna University-Chennai, **Prof. Dr. VIJILA KENNEDY,** Professor and Director, KCT Business School, Coimbatore and Coordinator, KCT Study Centre, Coimbatore - 49.

Great honor and indebt gratitude to the Counselor **Mr.A.SENTHIL KUMAR,** Asst Professor (Sr. Grade), KCT Business School, Coimbatore and Counselor - MBA Programme, KCT Study Centre, Coimbatore – 49 and my inspiring guide **Mr. V.KAARTHIEKHEYAN,** Assistant Professor, KCT Business School, who have taken great interest in helping me on and often in the successful pursuit of my project. I am very much fortunate to get such a good guide, who encouraged me constantly with good counsel and helped me to complete the project successfully on time.

I express my heartfelt gratitude to all the respondents who have participated in the survey and have given the accurate information to their best.

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

## LIST OF SYMBOLS AND ABBREVIATIONS

NHS - National Health Service

DNA - Deoxyribonucleic Acid

PIN - Personal Identification Number

FBI - Federal Bureau of Investigation

UK - United Kingdoms

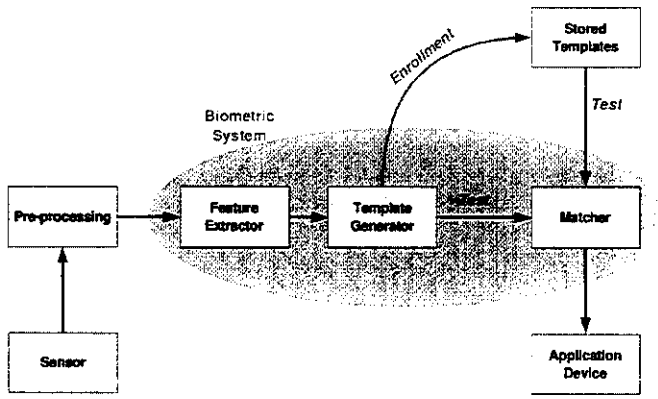
# CHAPTER I

# 1. INTRODUCTION

## 1.1 About Bio metric system and practices

Biometric devices is one which consist of a reader or scanning device software that converts the gathered information into digital form, and a database that stores the biometric data with comparison with existing records.

Figure 1.1: Working Principle of Bio Metric System




In Biometric systems, the modes are classified into two types. There are Enrollment Mode (A sample of the biometric trait is captured, processed by a computer, and stored for later comparison) and Verification mode (A biometric system authenticates a person's claimed identity from their previously enrolled pattern) .

The existing Biometric Practices are Fingerprints, Hand geometry, Face, Iris Recognition, Voice Recognition, Retinal Scanning, and Signature Recognition. Many biometric characteristics may be captured in the first phase of processing. However, automated capturing and automated comparison with previously stored data requires the properties such as universal, invariance of properties, measurability, singularity and acceptance.

## 1.2 Need for Study

Biometrics can be defined as measurable physiological and/or behavioral characteristics that can be utilized to verify the identity of an individual, and include fingerprint verification, hand geometry, retinal scanning, iris scanning, facial recognition and signature verification. Biometric authentication is considered the automatic identification, or identity verification, of an individual using either a biological feature they possess.

Traditional Authentication systems often lead to,

i. Confusion,

ii. losing of identity tokens,

iii. Possibility of data theft and etc…..

To eliminate above issues, biometric technology is evolved. This study is essential to know how the Biometric sensor mechanism is effective for Attendance Authentication System.

## 1.3 Statement of the Problem

Traditionally, attendance is taken manually by using attendance sheet and not a system. With this manual system, there are some cases that person can cheat by asking their friends to tick or sign for them. Because of this problem, a system may be needed in order to records the attendance more accurately without have to trace manually by Administration. A Biometric System will be provided at Colleges and this system will record the attendance.

These traditional methods of the Attendance authentication unfortunately do not authenticate the user as such. Traditional methods are based on properties that can

be forgotten, Stolen, disclosed or lost. To eliminate the above issues, biometric technology has been proposed for Attendance Authentication System.

### 1.4 Objectives and scope

#### 1.4.1 Primary Objective

To study the Effectiveness of Biometric Technologies for Attendance Authentication Systems and conduct a comparative study among educational institutes.

#### 1.4.2 Secondary Objectives

i. To identify the traditional authentication systems and to find out the constraints involved.

ii. Understanding of Biometric sensors and study their advantages and limitations.

iii. Survey among educational institutes on Effectiveness of Biometric technologies for Attendance authentication Purpose.

#### 1.4.3 Scope for further study

This study covers an automatic personal identification system based solely on any one of the Biometric technology which is often not able to meet the system performance requirements. For example, face recognition is fast but not reliable while fingerprint verification is reliable but inefficient in database retrieval. So further study has to be carried out to measure the effectiveness of two or more combined Biometric technology and to identify which combination will provide more effectiveness among other techniques.

## 1.5 Deliverables

i. Survey results and analysis taken from educational institutes.

ii. Accuracy of the Biometric Device.

iii. Security level of the Biometric system.

iv. Effectiveness of the Biometric System.

## 1.6 Limitations of the study

i. The respondents have given accurate and correct information without any bias, during the survey.

ii. In Coimbatore, only five to six Colleges are using this technology, hence the target respondents for the survey are less.

# CHAPTER II

# 2. LITERATURE SURVEY

## 2.1 Review of Literature

### 2.1.1 Definition of Biometrics

According to Bowman, E, 2000, biometric technologies are defined as "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic". Automated methods can be broken down into a mechanism used to scan, a processing or comparison unit and an interface with a variety of application systems. Identification refers to when characteristics are selected from a group of stored images; this produces a list of possible or likely matches.

### 2.1.2 History of Biometrics

The term biometrics comes from the Greek words bios, meaning life, and metrics, meaning measure. Biometrics can be defined as measurable physiological and/or behavioral characteristics that can be utilized to verify the identity of an individual, and include fingerprint verification, hand geometry, retinal scanning, iris scanning, facial recognition and signature verification.

In practice, the process of identification and authentication is the ability to verify and confirm an identity. It is accomplished by using any one or a combination of the following three traditional identification techniques: something you possess; something you know; or something you are.

A number of studies have been carried out in several countries by prospective users, vendors, and governments. The following is a sampling of these studies: A six month study was carried out in the UK in April 2004 to assess processes and record testimony of user experiences and attitudes to incorporate biometric information into new passports and the proposed national identity card. 10,016 users joined in the study which used facial, iris and fingerprint biometrics. Six static and one mobile centre in different regions of the UK were used to gather data. The study covered the testing of the use of biometrics through a simulated application process; measurement of the process times; assessment of customer perceptions and reactions; testing fingerprint and iris biometrics for one-to-many identification and testing; and facial, iris and fingerprint biometrics for one-to-one verification. However, the outcome of this study revealed high enrolment times: on average 8 minutes and 15 seconds, and 10 minutes and 20 seconds for disabled participants. A recommendation by the study's organizers was presented for example a number of such as good design and management of the enrolment, environment is significant to accomplish high success rates; a number of measures require to be put in place for the enrolment of disabled people; improved processes for failed enrolments are necessary; testing is essential.

## 2.2 Research Gap

Currently Biometric technologies are widely used in the areas such as Banks, Hospitals, and military offices. This project will helps to bridge the gap of application of Biometric technologies in attendance authentication system. This study will provide the effectiveness of Biometric technologies used for Attendance authentication system.

# CHAPTER 3

# 3. METHODOLOGY

## 3.1 Type of Research Design

This study involves collection of data directly from the target respondents, and the data collected is used for further analysis. The type of the research design adopted for the study is descriptive research.

## 3.2 Target Respondents

This study analyses the effectiveness of Biometric Technologies used for Attendance Authentication Purpose. So the population is characterized by colleges, which are all implemented this technology for Attendance Authentication Purpose. The region of study is Coimbatore. So the target respondents are Colleges (Lecturers / Students) in Coimbatore, using Biometric Technology for Attendance Authentication Purpose.

## 3.3 Sampling Method

### 3.3.1 Definition of the Target Population

The Target Population for this study is the Lecturers / Students of the institutions which are all using Biometric Technology for Attendance Authentication Purpose.

### 3.3.2 Sample population

The Sample Population is 60

The sampling methodology adopted is Area Sampling Method.

### 3.3.3 Source of Data Collection

The Source of Data Collection is Primary Data. The Data's are collected from the Lecturers / Students of the following Institutions,

1. Kumaraguru college of Technology
2. PSG college of Technology
3. Sri Krishna College of Engineering
4. Sri Ramakrishna College of Engineering

## 3.4 Data Processing

### 3.4.1 Method of Data Collection

The method of data collection involved is through primary data collection technique.

### 3.4.2 Tool for Data Collection

The tool used for data collection is Questionnaire.

## 3.5 Tools for Analysis

Following tools are used for analysis.

i. Percentage analysis

ii. Weighted average method

iii. Factor Analysis

## 3.6 Period of Study

The Duration taken to perform this study is 3 Months (June, 2011 to August 2011)

# CHAPTER IV

## 4. DATA ANALYSIS AND INTERPRETATION

Table 4.1: Table showing the familiarity of the respondent with the concept of collection of Biometric data

| S.no | Response | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Familiar with the concept | 56 | 93.33 |
| 2 | I heard something about it | 2 | 3.33 |
| 3 | I don't have any idea | 2 | 3.33 |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 56 (93.33%) of the respondents are familiar with the concept of collection of Biometric data, 2 (3.33%) of the respondents just heard something about the concept of collection of Biometric data and 2 (3.33%) of the respondents do not have any idea about the concept of collection of Biometric data. Hence majority (93.33%) of the respondents just heard something about the concept of collection of Biometric data.

Figure 4.1: Chart showing the familiarity of the respondent with the concept of collection of Biometric data

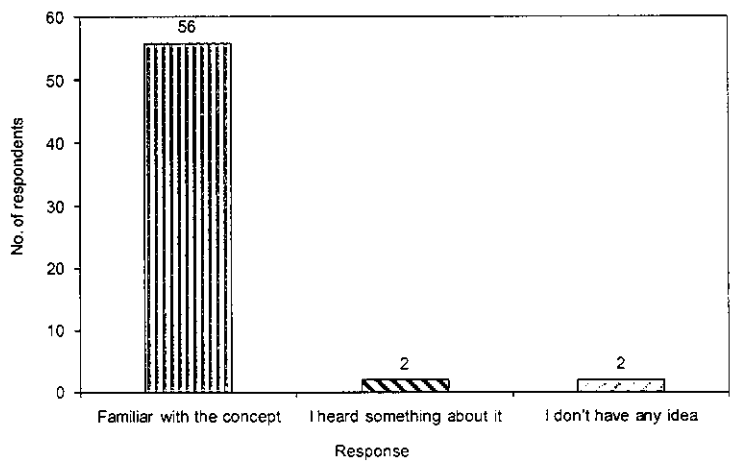


Table 4.2: Table showing ranking of types of functions might the respondent is willing to accept biometrics use (**Weighted Rank Analysis**)

| Functions | Rank1 | Rank2 | Rank3 | Rank4 | Weighted Rank Score | Rank |
|---|---|---|---|---|---|---|
| Attendance | 60 | - | - | - | 1 | I |
| Library | - | 21 | 37 | 2 | 2.68 | II |
| Security | - | 25 | 15 | 20 | 2.91 | III |
| Lab | - | 14 | 8 | 38 | 3.67 | IV |

**Interpretation**

From the above table, attendance ranks the top with weighted rank score 1, then library ranked second with weighted rank score 2.68, then security ranked third with weighted rank score 2.91 and lastly lab ranked fourth with weighted rank score 3.67. Hence attendance tops the rank 1. Weighted rank Score is computed as follows:

Weighted rank score = $\sum x_i f_i / \sum f_i$ , where $x_i$ is the rank assigned for that attribute and $f_i$ stands for number of responses for the respective factor or attribute & $f_i$=N (total responses).

For example, the rank for security is computed as

(1x0+2x25+3x15+4x20)/60= (50+45+80)/60=175/60=2.91.

Figure 4.2: Chart showing ranking of types of functions might the respondent is willing to accept biometrics use (Weighted Rank Analysis)

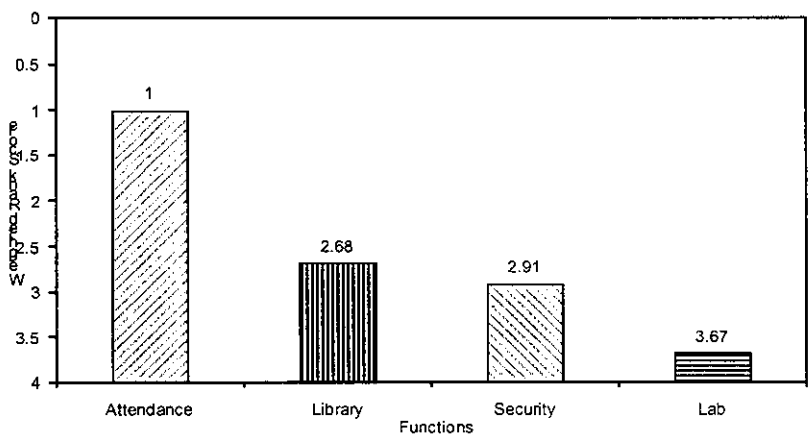


Table 4.3: Table showing whether the respondent is familiar with biometrics before reading the survey

| S.no | Response | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Yes | 54 | 90.00 |
| 2 | No | 2 | 3.33 |
| 3 | May be | 4 | 6.67 |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 54 (90%) of the respondents are familiar with biometrics before reading the survey, 2 (3.33%) of the respondents are not familiar with biometrics before reading the survey and 4 (6.67%) of the respondents have no opinion over biometrics before reading the survey. Hence majority (90%) of the respondents are familiar with biometrics before reading the survey.

Figure 4.3: Chart showing whether the respondent is familiar with biometrics before reading the survey

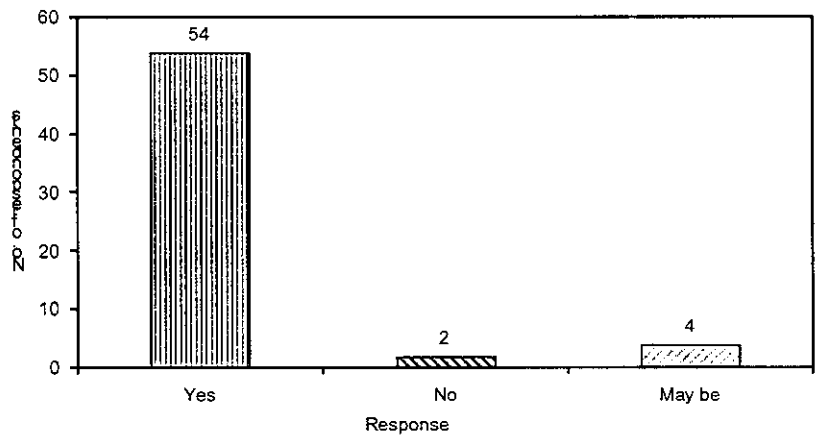


Table 4.4: Table whether the respondent believes that biometrics can be totally accurate

| S.no | Response | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Of course totally accurate | 35 | 58.33 |
| 2 | Somewhat accurate | 18 | 30.00 |
| 3 | Probably not accurate | 7 | 11.67 |
| 4 | Not accurate | - | - |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 35 (58.3%) of the respondents believe that biometrics can be totally accurate, 18 (30%) of the respondents believe that biometrics can be somewhat accurate, 7 (11.67%) of the respondents believe that biometrics can be probably not accurate and none of the respondents believe that biometrics can be totally not accurate. Hence majority (58.33%) of the respondents believe that biometrics can be totally accurate.

Figure 4.4: Chart whether the respondent believes that biometrics can be totally accurate

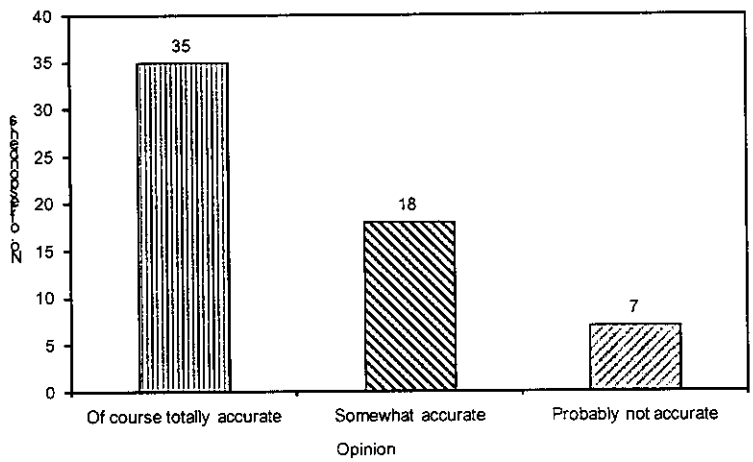


Table 4.5: Table showing the opinion about the security of biometrics

| S.no | Opinion | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Of course totally secure | 29 | 48.33 |
| 2 | Somewhat secure | 27 | 45.00 |
| 3 | Probably secure | 4 | 6.67 |
| 4 | Not secure | - | - |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 29 (48.33%) of the respondents believe that biometrics can be totally secure, 27 (45%) of the respondents believe that biometrics can be somewhat secure, 4 (6.67%) of the respondents believe that biometrics can be probably not secure and none of the respondents believe that biometrics can be totally not secure. Hence majority (48.33%) of the respondents believe that biometrics can be totally secure.

Figure 4.5: Chart showing the opinion about the security of biometrics

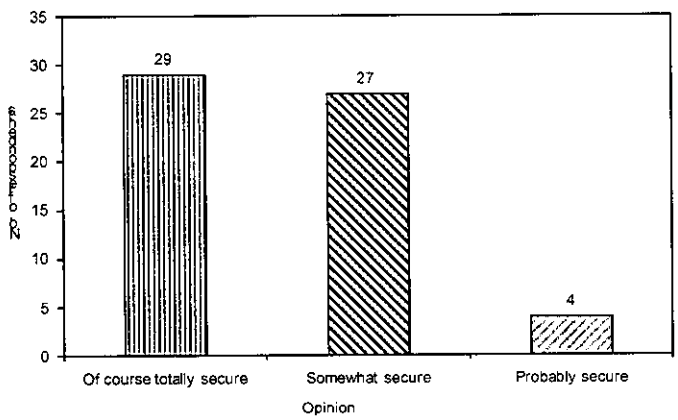


Table 4.6: Table showing agreeability level towards the statement "Passwords and ID cards are vulnerable to security attack"

| S.no | Agreeability level | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Strongly agree | 45 | 75 |
| 2 | Agree | 15 | 25 |
| 3 | Neither agree nor disagree | - | - |
| 4 | Disagree | - | - |
| 5 | Strongly disagree | - | - |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 45 (75%) of the respondents strongly agree the statement "Passwords and ID cards are vulnerable to security attack". 15 (25%) of the respondents agree the statement "Passwords and ID cards are vulnerable to security attack", p of the respondents are neutral towards / disagree / strongly disagree the statement "Passwords and ID cards are vulnerable to security attack".

Hence majority (75%) of the respondents strongly agree the statement "Passwords and ID cards are vulnerable to security attack".

Figure 4.6: Chart showing agreeability level towards the statement "Passwords and ID cards are vulnerable to security attack"

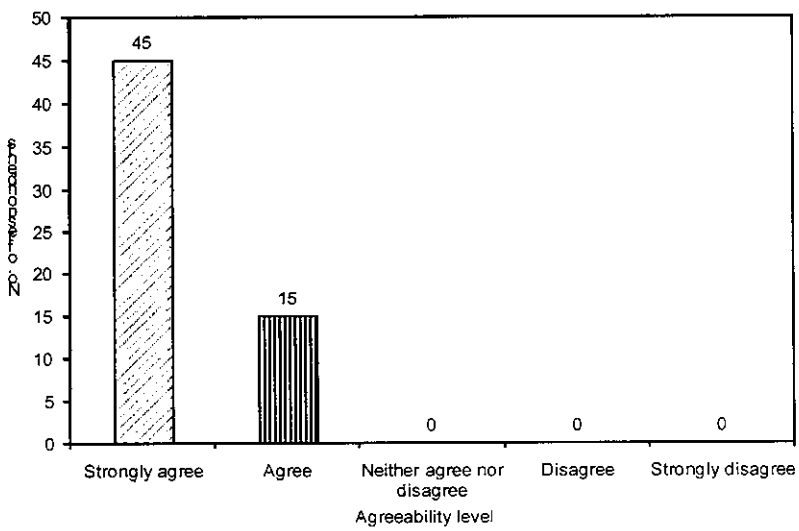


Table 4.7: Table showing agreeability level towards the statement "Biometrics are vulnerable to security attack"

| Sno | Agreeability level | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Strongly agree | 13 | 21.67 |
| 2 | Agree | 20 | 33.33 |
| 3 | Neither agree nor disagree | 2 | 3.33 |
| 4 | Disagree | 25 | 41.67 |
| 5 | Strongly disagree | - | - |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 13 (21.67 %) of the respondents strongly agree the statement "Biometrics are vulnerable to security attack", 20 (33.33 %) of the respondents agree the statement "Biometrics are vulnerable to security attack", 2 (3.33%) of the respondents are neutral to the statement "Biometrics are vulnerable to security attack", 25 (41.67%) of the respondents disagree the statement "Biometrics are vulnerable to security attack" and none of the respondents strongly disagree the statement "Biometrics are vulnerable to security attack". Hence majority (41.67%) of the respondents Disagree the statement "Biometrics are vulnerable to security attack".

Figure 4.7: Chart showing agreeability level towards the statement "Biometrics is vulnerable to security attack"

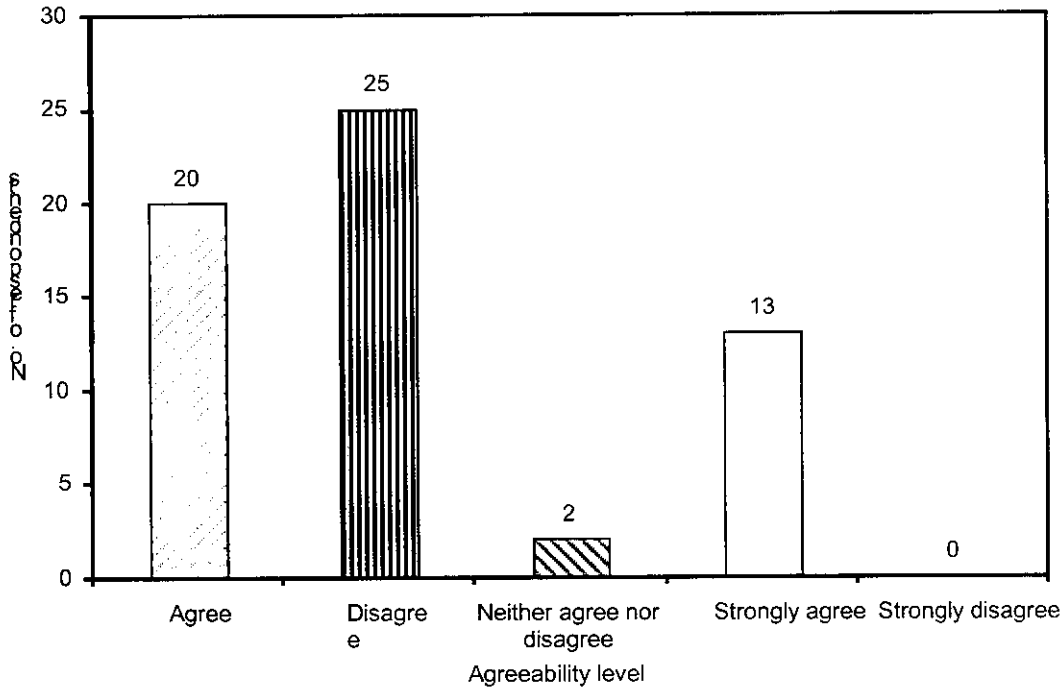


Table 4.8: Table showing agreeability level towards the statement "Finger print Biometric process would you believe to take over the future"

| Sno | Agreeability level | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Strongly agree | 42 | 70 |
| 2 | Agree | 18 | 30 |
| 3 | Neither agree nor disagree | - | - |
| 4 | Disagree | - | - |
| 5 | Strongly disagree | - | - |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 42 (70%) of the respondents strongly agree the statement "Finger print Biometric process would take over the future", 18 (30%) of the respondents agree the statement "Finger print Biometric process would take over the future" and none of the respondents are neutral towards / disagree / strongly disagree the statement "Finger print Biometric process would take over the future". Hence majority (70%) of the respondents strongly agree the statement "Finger print Biometric process would take over the future".

Figure 4.8: Chart showing agreeability level towards the statement "Finger print Biometric process would you believe to take over the future"

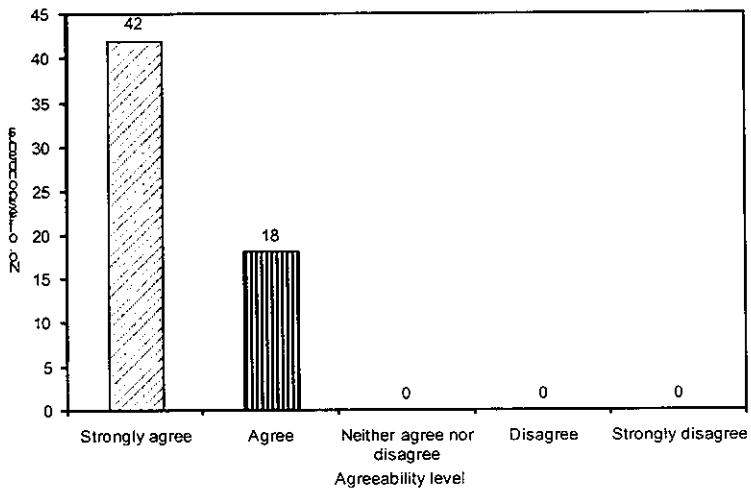


Table 4.9: Table showing agreeability level towards the statement "Iris – Retina (eyes) Biometric process would take over the future"

| S.no | Agreeability level | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Strongly agree | - | - |
| 2 | Agree | 36 | 60.00 |
| 3 | Neither agree nor disagree | 24 | 40.00 |
| 4 | Disagree | - | - |
| 5 | Strongly disagree | - | - |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that none of the respondents strongly agree the statement "Iris – Retina (eyes) Biometric process would take over the future", 36 (60%) of the respondents agree the statement "Iris – Retina (eyes) Biometric process would take over the future", 24 (40%) of the respondents are neutral to the statement "Iris – Retina (eyes) Biometric process would take over the future" and none of the respondents disagree / strongly disagree the statement "Iris – Retina (eyes) Biometric process would take over the future". Hence majority (60%) of the respondents agree the statement "Iris – Retina (eyes) Biometric process would take over the future".

Figure 4.9: Chart showing agreeability level towards the statement "Iris – Retina (eyes) Biometric process would take over the future"

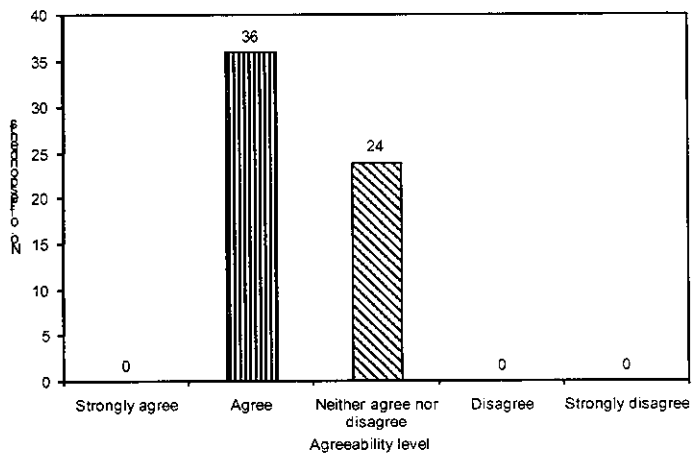


Table 4.10: Table showing agreeability level towards the statement "Voice recognition Biometric process would take over the future"

| Sno | Agreeability level | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Strongly agree | - | - |
| 2 | Agree | 52 | 86.67 |
| 3 | Neither agree nor disagree | 8 | 13.33 |
| 4 | Disagree | - | - |
| 5 | Strongly disagree | - | - |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that none of the respondents strongly agree the statement "Voice recognition Biometric process would take over the future", 52 (86.67%) of the respondents agree the statement "Voice recognition Biometric process would take over the future", 8 (13.33%) of the respondents are neutral to the statement "Voice recognition Biometric process would take over the future" and none of the respondents disagree / strongly disagree the statement "Voice recognition Biometric process would take over the future". Hence majority (86.67%) of the respondents agree the statement "Voice recognition Biometric process would take over the future".

Figure 4.10: Chart showing agreeability level towards the statement "Voice recognition Biometric process would take over the future"

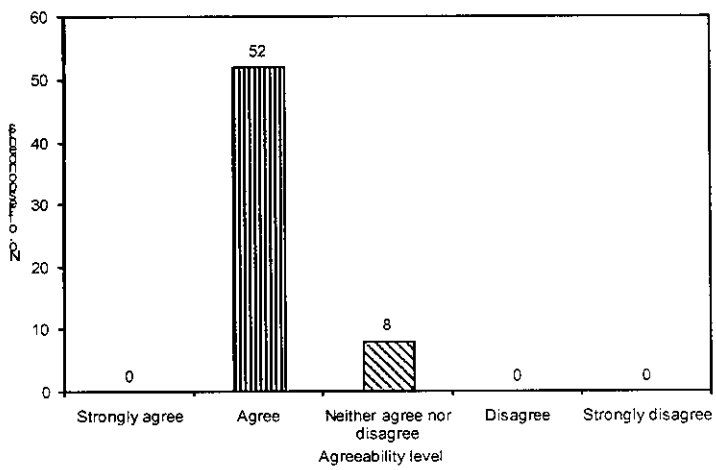


Table 4.11: Table showing agreeability level towards the statement "Face recognition Biometric process would take over the future"

| S.no | Agreeability level | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Strongly agree | 13 | 21.67 |
| 2 | Agree | 47 | 78.33 |
| 3 | Neither agree nor disagree | - | - |
| 4 | Disagree | - | - |
| 5 | Strongly disagree | - | - |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 13 (21.67%) of the respondents strongly agree the statement "Face recognition Biometric process would take over the future", 47 (78.33%) of the respondents agree the statement "Face recognition Biometric process would take over the future", none of the respondents are neutral towards / disagree / strongly disagree the statement "Face recognition Biometric process would take over the future". Hence majority (78.33%) of the respondents agree the statement "Face recognition Biometric process would take over the future".

Figure 4.11: Chart showing agreeability level towards the statement "Face recognition Biometric process would take over the future"

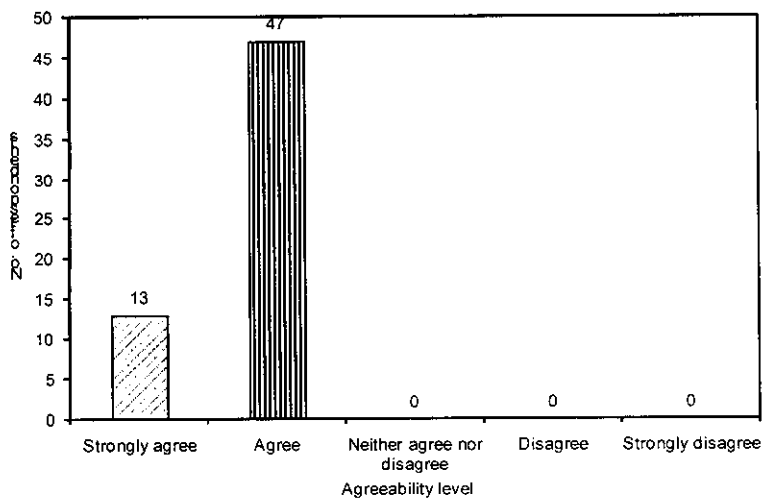


Table 4.12: Table showing agreeability level towards the statement "Combination of two or three Biometric process would take over the future"

| Sno | Agreeability level | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Strongly agree | 39 | 65 |
| 2 | Agree | 21 | 35 |
| 3 | Neither agree nor disagree | - | - |
| 4 | Disagree | - | - |
| 5 | Strongly disagree | - | - |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 39 (65%) of the respondents strongly agree the statement "Combination of two or three Biometric process would take over the future", 21 (35%) of the respondents agree the statement "Combination of two or three Biometric process would take over the future", (%) of the respondents are neutral towards / disagree / strongly disagree the statement "Combination of two or three Biometric process would take over the future". Hence majority (65%) of the respondents strongly agree the statement "Combination of two or three Biometric process would take over the future".

Figure 4.12: Chart showing agreeability level towards the statement "Combination of two or three Biometric process would take over the future"

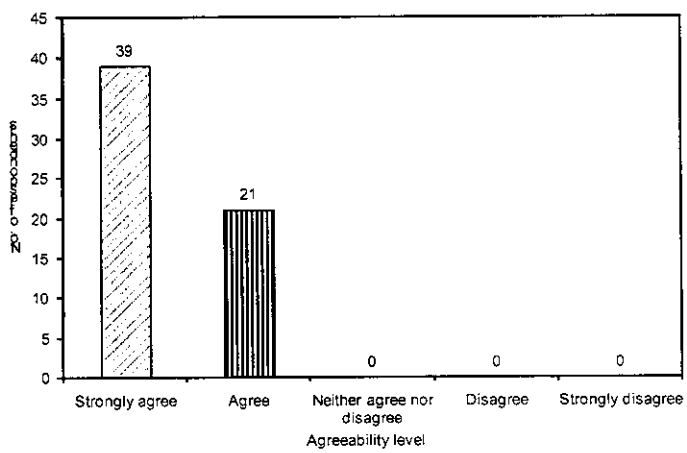


Table 4.13: Table showing whether the institute where the respondent is placed would likely to adopt Biometric process

| Sno | Response | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Most likely | 32 | 53.33 |
| 2 | Quite likely | 10 | 16.67 |
| 3 | Can't say | 18 | 30.00 |
| 4 | Most unlikely | - | - |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 32 (53.33%) of the respondents said that their institute would most likely to adopt Biometric process, 10 (16.67%) of the respondents said that their institute would quite likely to adopt Biometric process, 18 (30%) of the respondents said that they can't say their institute would likely to adopt Biometric process and none of the respondents said that their institute would most unlikely to adopt Biometric process. Hence majority (53.33%) of the respondents said that their institute would most likely to adopt Biometric process.

Figure 4.13: Chart showing whether the institute where the respondent is placed would likely to adopt Biometric process

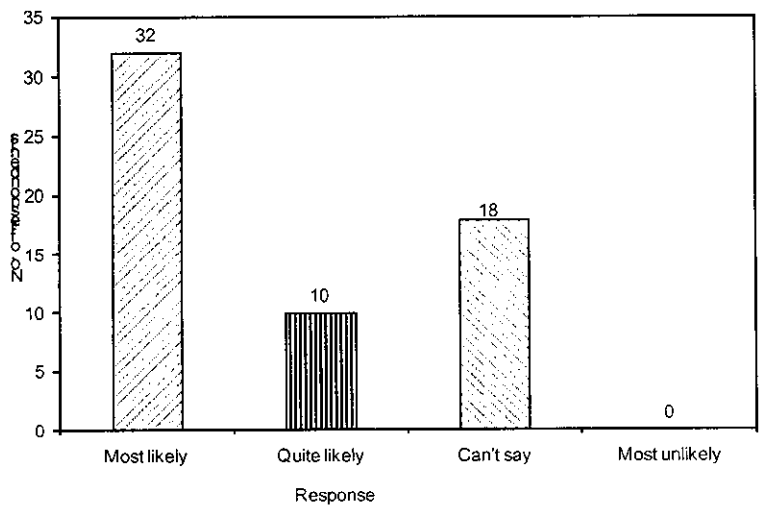


Table 4.14: Table showing places where the institute of the respondents implemented Biometric systems

| Sno | Places | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | All departments/offices | 1 | 1.67 |
| 2 | Only in Reception | 59 | 98.33 |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 1 (1.67%) of the respondents said that their institute implemented Biometric systems in all departments/office and 59 (98.33%) of the respondents said that their institute implemented Biometric systems only in reception. Hence majority (98.33%) of the respondents said that their institute implemented Biometric systems only in reception.

Figure 4.14: Chart showing places where the institute of the respondents implemented Biometric systems

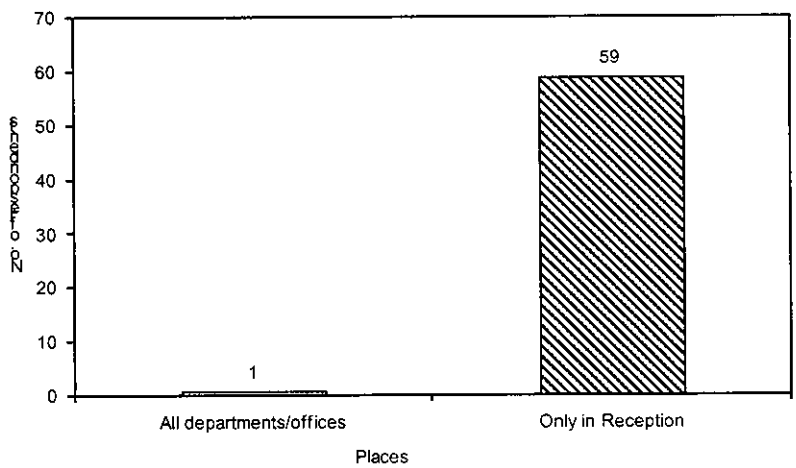


Table 4.15: Table showing agreeability level towards the statement "Biometric is more effective than the traditional authentication process"

| Sno | Agreeability level | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Strongly agree | 51 | 85 |
| 2 | Agree | 9 | 15 |
| 3 | Neither agree nor disagree | - | - |
| 4 | Disagree | - | - |
| 5 | Strongly disagree | - | - |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 51 (85%) of the respondents strongly agree the statement "Biometric is more effective than the traditional authentication process", 9 (15%) of the respondents agree the statement "Biometric is more effective than the traditional authentication process", none of the respondents are neutral towards / disagree / strongly disagree the statement "Biometric is more effective than the traditional authentication process". Hence majority (85%) of the respondents strongly agree the statement "Biometric is more effective than the traditional authentication process".

Figure 4.15: Chart showing agreeability level towards the statement "Biometric is more effective than the traditional authentication process"

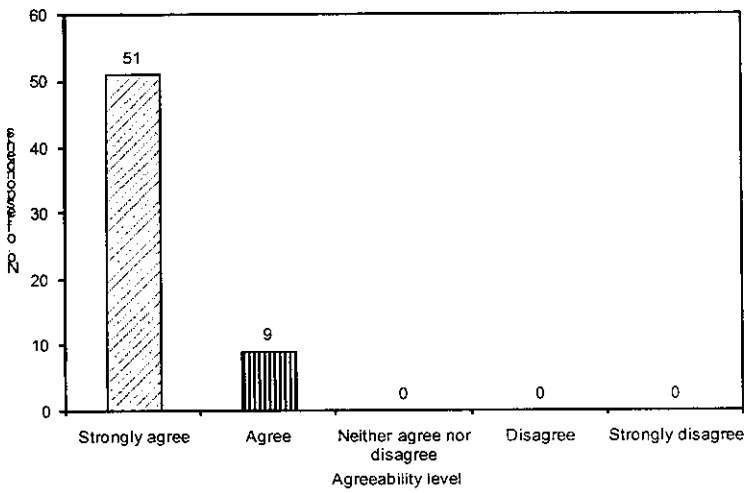


Table 4.16: Table showing whether the respondents have come across to a situation where their Institute's Biometric system failed to recognize them

| S.no | Response | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Yes | 2 | 3.33 |
| 2 | No | 50 | 83.33 |
| 3 | Don't remember | 8 | 13.33 |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 2 (3.33%) of the respondents have come across a situation where their institute's Biometric system failed to recognize them, 50 (83.33%) of the respondents have not come across a situation where their institute's Biometric system failed to recognize them and 8 (13.33%) of the respondents have not remembered a situation where their institute's Biometric system failed to recognize them. Hence majority (83.33%) of the respondents have not come across a situation where their institute's Biometric system failed to recognize them.

Chart 4.16: Chart showing whether the respondents have come across to a situation where their Institute's Biometric system failed to recognize them

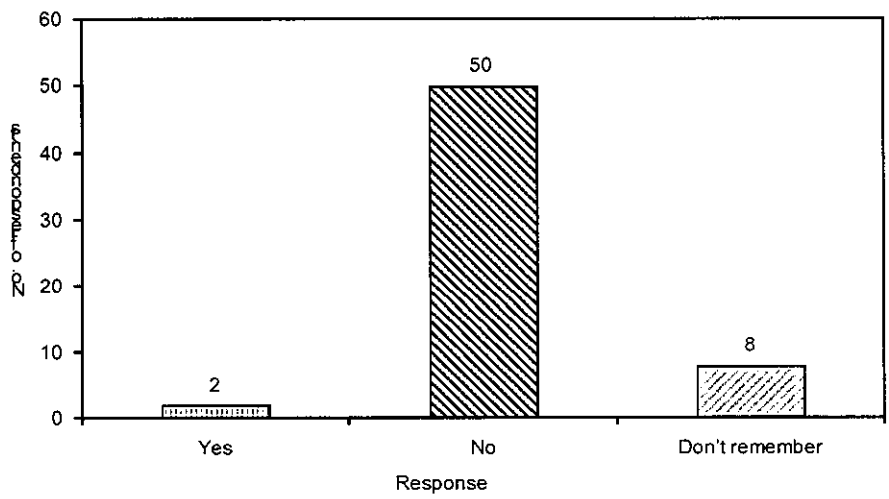


Table 4.17: Table showing no. of times the system failed to recognize the respondent

| Sno | No. of times | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | <3 times | 2 | 3.33 |
| 2 | 3 to 7 times | - | - |
| 3 | >7 times | - | - |
| | Total | 2 | 3.33 |

**Interpretation**

From the above table it is interpreted that 2 (3.33%) of the respondents said that they have come across a situation where the system failed to recognize them for less than 3 times.

Figure 4.17: Chart showing no. of times the system failed to recognize the respondent

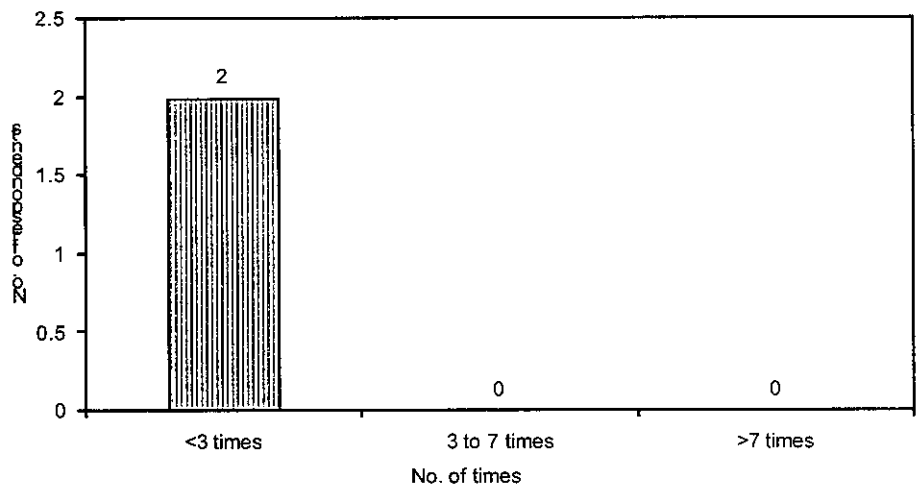


Table 4.18: Table showing the opinion about the ways to improve performance of Biometric system

| Sno | Ways to improve | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Error free | 31 | 51.67 |
| 2 | Increased process speed | 26 | 43.33 |
| 3 | Don't know | 3 | 5.00 |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 31 (51.67%) of the respondents said that Bio metric can be made error free to improve its performance, 26 (43.33%) of the respondents said that the speed of processing can be improved and 3 (5%) of the respondents did not give any opinion. Hence majority (51.67%) of the respondents said that Bio metric can be made error free to improve its performance.

Figure 4.18: Chart showing the opinion about the ways to improve performance of Biometric system

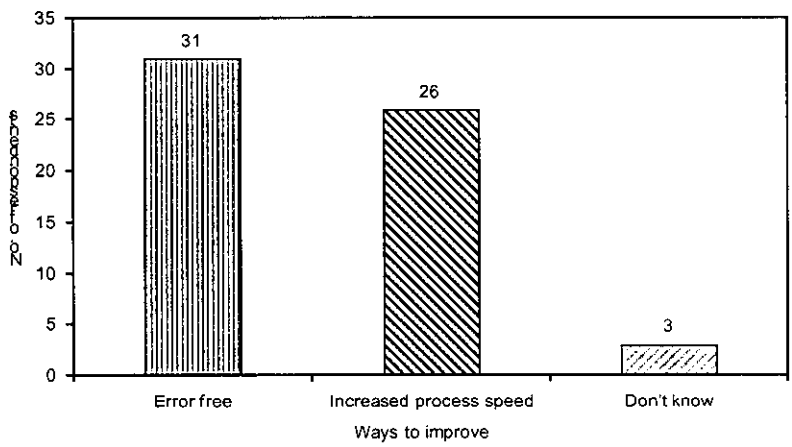


Table 4.19: Table showing whether the institute of the respondents has provided alternative arrangements to get the Biometric system in case of failure

| S.no | Response | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Yes | 46 | 76.67 |
| 2 | No | 1 | 1.67 |
| 3 | Don't know | 13 | 21.67 |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 46 (76.67%) of the respondents said that their institute has provided alternative arrangements to get the Biometric system in case of failure, 1 (1.67%) of the respondents said that their institute has not provided alternative arrangements to get the Biometric system in case of failure and 13 (21.67%) of the respondents said that they are not sure about whether their institute has alternative arrangements to get the Biometric system in case of failure. Hence majority (76.67%) of the respondents said that their institute has provided alternative arrangements to get the Biometric system in case of failure.

Figure 4.19: Chart showing whether the institute of the respondents has provided alternative arrangements to get the Biometric system in case of failure

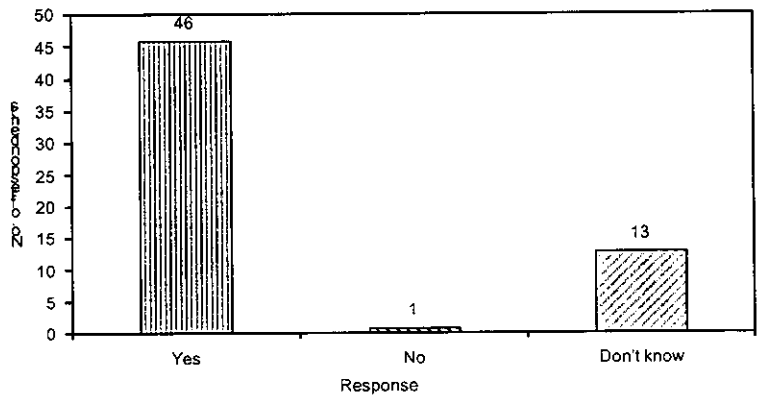


Table 4.20: Table showing the level of comfortability of the respondents to use Biometric system

| S.no | Level of Comfortability | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Very comfortable | 39 | 65 |
| 2 | Somewhat comfortable | 21 | 35 |
| 3 | Not at all comfortable | - | - |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 39 (65%) of the respondents are very much comfortable to use Biometric system, 21 (35%) of the respondents are somewhat comfortable to use Biometric system and none of the respondents are not at all comfortable to use Biometric system. Hence majority (65%) of the respondents are very much comfortable to use Biometric system.

Figure 4.20: Chart showing the level of comfortability of the respondents to use Biometric system

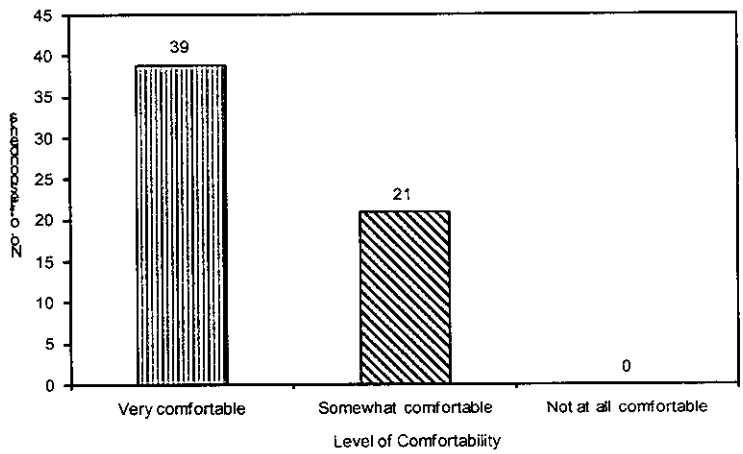


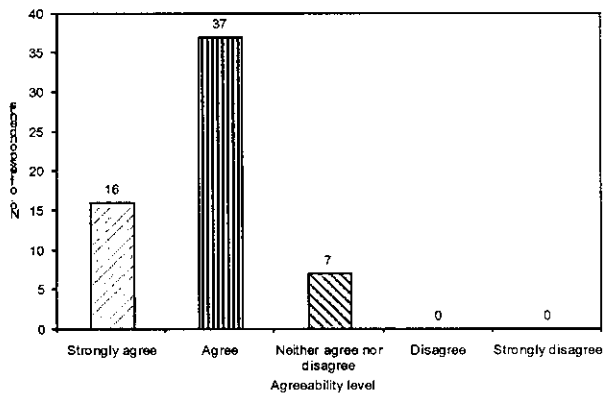
Table 4.21: Table showing agreeability level towards the statement "The performance of Biometric system can be improved in our Institute"

| S.no | Agreeability level | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Strongly agree | 16 | 26.67 |
| 2 | Agree | 37 | 61.67 |
| 3 | Neither agree nor disagree | 7 | 11.67 |
| 4 | Disagree | - | - |
| 5 | Strongly disagree | - | - |
| | Total | 60 | 100 |

**Interpretation**

From the above table it is interpreted that 16 (26.67%) of the respondents strongly agree the statement "The performance of Biometric system can be improved in our Institute", 37 (61.67%) of the respondents agree the statement "The performance of Biometric system can be improved in our Institute", 7 (11.67%) of the respondents are neutral to the statement "The performance of Biometric system can be improved in our Institute", none of the respondents disagree / strongly disagree the statement "The performance of Biometric system can be improved in our Institute". Hence majority (61.67%) of the respondents agree the statement "The performance of Biometric system can be improved in our Institute".

Figure 4.21: Chart showing agreeability level towards the statement "The performance of Biometric system can be improved in our Institute"



## 4.1 WEIGHTED AVERAGE SCORE ANALYSIS

### 4.1.1 Introduction

Weighted average score analysis is important in any study to know the impact of each variable (question) for easy comparison and prioritize the vital variables involved in the study. The weighted average score analysis in this study is carried out for nine agreeability level questions from 6 to 12, 15 and 21 (totally eight variables). The weights are assigned as follows:

| S.no | Agreeability level | Weight |
|---|---|---|
| 1 | Strongly agree | 5 |
| 2 | Agree | 4 |
| 3 | Neither agree nor disagree | 3 |
| 4 | Disagree | 2 |
| 5 | Strongly disagree | 1 |

The weighted average is computed as $\sum x_i w_i / \sum x_i$ where wi denotes weights and xi denotes the frequency of each category. For example, the weighted average score based on question No. 7 is 3.87 which is shown in the following table.

| S.no | Agreeability level | No. of respondents | % of respondents |
|---|---|---|---|
| 1 | Strongly agree | 20 | 33.33 |
| 2 | Agree | 25 | 41.67 |
| 3 | Neither agree nor disagree | 2 | 3.33 |
| 4 | Disagree | 13 | 21.67 |
| 5 | Strongly disagree | - | - |
| | Total | 60 | 100 |

Weighted average score = (20x5+25x4+2x3+13x2+0x5)/60 = (100+100+6+26)/60=232/60=3.87 which is considered to be just below or nearer to "agree" option on average. Similarly all the other weighted average scores are calculated which is given below:

**Weighted Average Score**

| Variable | q6 | q7 | q8 | q9 | q10 | q11 | q12 | q15 | q21 |
|---|---|---|---|---|---|---|---|---|---|
| Weighted Mean Score | 4.75 | 3.87 | 4.7 | 3.6 | 3.87 | 4.22 | 4.65 | 4.85 | 4.15 |
| Rank | II | VII | III | VIII | VII | V | IV | I | VI |

### 4.1.2 Interpretation

Among the above question 15 (agreeability level towards the statement "Biometric is more effective than the traditional authentication process") is having very high agreeability score (marked in green) whereas question 9 (agreeability level towards the statement "Iris – Retina (eyes) Biometric process would take over the future") is having the least agreeability score (marked in red) whereas question 11 (agreeability level towards the statement "Face recognition Biometric process would take over the future") has median agreeability score (marked in yellow).

## 4.2 Factor Analysis

Factor analysis is a statistical method used to describe variability among observed variables in terms of a potentially lower number of unobserved variables called factors. In other words, it is possible, for example, that variations in three or four observed variables mainly reflect the variations in a single unobserved variable, or in a reduced number of unobserved variables. Factor analysis searches for such joint variations in response to unobserved latent variables. The observed variables are modeled as linear combinations of the potential factors, plus "error" terms. The information gained about the interdependencies between observed variables can be used later to reduce the set of variables in a dataset.

Factor analysis is related to principal component analysis (PCA), but the two are not identical. Because PCA performs a variance-maximizing rotation of the variable space, it takes into account all variability in the variables. In contrast, factor analysis estimates how much of the variability is due to common factors ("communality"). The two methods become essentially equivalent if the error terms in the factor analysis model (the variability not explained by common factors, see below) can be assumed to all have the same variance.

Communalities

| Variable | Initial | Extraction |
|---|---|---|
| q6 | 1.000 | 0.828 |
| q7 | 1.000 | 0.664 |
| q8 | 1.000 | 0.814 |
| q9 | 1.000 | 0.681 |
| q10 | 1.000 | 0.746 |
| q11 | 1.000 | 0.859 |
| q12 | 1.000 | 0.834 |
| q15 | 1.000 | 0.874 |
| q21 | 1.000 | 0.823 |

Total Variance Explained

| Component | Initial Eigen values | | | Extraction Sums of Squared Loadings | | | Rotation Sums of Squared Loadings | | |
|---|---|---|---|---|---|---|---|---|---|
| | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % |
| 1 | 3.054 | 33.932 | 33.932 | 3.054 | 33.932 | 33.932 | 2.026 | 22.508 | 22.508 |
| 2 | 1.663 | 18.476 | 52.409 | 1.663 | 18.476 | 52.409 | 1.822 | 20.242 | 42.749 |
| 3 | 1.312 | 14.580 | 66.989 | 1.312 | 14.580 | 66.989 | 1.697 | 18.854 | 61.603 |
| 4 | 1.095 | 12.164 | 79.152 | 1.095 | 12.164 | 79.152 | 1.579 | 17.549 | 79.152 |
| 5 | .654 | 7.271 | 86.423 | | | | | | |
| 6 | .451 | 5.009 | 91.432 | | | | | | |
| 7 | .376 | 4.182 | 95.614 | | | | | | |
| 8 | .232 | 2.582 | 98.195 | | | | | | |
| 9 | .162 | 1.805 | 100.000 | | | | | | |

Extraction: Principal Component Analysis: Component Matrix

| Variable | Component | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| q6 | .187 | .805 | -.023 | -.380 |
| q7 | -.694 | .274 | .294 | -.143 |
| q8 | .584 | .236 | -.227 | .605 |
| q9 | -.752 | .197 | -.182 | .211 |
| q10 | -.516 | .680 | -.075 | -.106 |
| q11 | -.499 | .160 | .580 | .498 |
| q12 | .790 | .182 | .248 | -.340 |
| q15 | .385 | .009 | .850 | .048 |
| q21 | .585 | .569 | -.118 | .378 |

Rotated Component Matrix

| Variable | Component | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| q6 | 0.188 | 0.159 | -0.144 | **0.864** |
| q7 | -0.206 | -0.462 | **0.516** | 0.375 |
| q8 | 0.055 | **0.893** | -0.063 | -0.100 |
| q9 | -0.674 | -0.161 | **0.412** | 0.176 |
| q10 | -0.373 | -0.087 | 0.294 | **0.716** |
| q11 | -0.037 | -0.030 | **0.925** | -0.026 |
| q12 | **0.773** | 0.221 | -0.378 | 0.212 |
| q15 | **0.847** | 0.038 | 0.386 | -0.078 |
| q21 | 0.186 | **0.837** | -0.046 | 0.293 |

Component Transformation Matrix

| Component | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | .646 | .567 | -.498 | -.111 |
| 2 | -.019 | .381 | .210 | .900 |
| 3 | .718 | -.255 | .647 | -.028 |
| 4 | -.257 | .684 | .538 | -.420 |

### 4.2.1 Interpretation

From the above tables it is interpreted that questions 12 and 15 can be grouped together as factor 1 (can be called as implementation factor which contributes 34% to total variance), questions 8 and 21 constitute factor 2 (can be called as improvement factor which contributes 18% to total variance), questions 7, 9 and 11 can be grouped together (can be called as alternative factor which contributes 15% to total variance) and questions 6 and 10 constitute factor 4 (can be called as security factor which contributes 12% to total variance).

# CHAPTER V

# 5. FINDINGS AND CONCLUSION

## 5.1 Findings

### 5.1.1 Findings based On Percentage Analysis

1. Majority (93.33%) of the respondents just heard something about the concept of collection of Biometric data

2. Majority (90%) of the respondents are familiar with biometrics before reading the survey.

3. Majority (58.33%) of the respondents believe that biometrics can be totally accurate.

4. Majority (48.33%) of the respondents believe that biometrics can be totally secure.

5. Majority (75%) of the respondents strongly agree the statement "Passwords and ID cards are vulnerable to security attack".

6. Majority (41.67%) of the respondents agree the statement "Biometrics are vulnerable to security attack".

7. Majority (70%) of the respondents strongly agree the statement "Finger print Biometric process would take over the future".

8. Majority (60%) of the respondents agree the statement "Iris – Retina (eyes) Biometric process would take over the future".

9. Majority (86.67%) of the respondents agree the statement "Voice recognition Biometric process would take over the future".

10. Majority (78.33%) of the respondents agree the statement "Face recognition Biometric process would take over the future".

11. Majority (65%) of the respondents strongly agree the statement "Combination of two or three Biometric process would take over the future".

12. Majority (53.33%) of the respondents said that their institute would most likely to adopt Biometric process.

13. Majority (98.33%) of the respondents said that their institute implemented Biometric systems only in reception.

14. Majority (85%) of the respondents strongly agree the statement "Biometric is more effective than the traditional authentication process".

15. Majority (83.33%) of the respondents have not come across a situation where their institute's Biometric system failed to recognize them.

16. 3.33% of the respondents said that they have come across a situation where the system failed to recognize them for less than 3 times.

17. Majority (51.67%) of the respondents said that Bio metric can be made error free to improve its performance.

18. Majority (76.67%) of the respondents said that their institute has provided alternative arrangements to get the Biometric system in case of failure.

19. Majority (65%) of the respondents are very much comfortable to use Biometric system.

20. Majority (61.67%) of the respondents agree the statement "The performance of Biometric system can be improved in their Institute".

### 5.1.2 Findings based on Weighted Average Rank Analysis

In Biometric usage, Attendance ranks the top with weighted rank score 1, library ranked second with weighted rank score 2.68, security ranked third with weighted rank score 2.91 and lastly lab ranked fourth with weighted rank score 3.67.

### 5.1.3 Findings based on Weighted Average Score Analysis

Among all the questions, question 15 (agreeability level towards the statement "Biometric is more effective than the traditional authentication process") is having very high agreeability score, question 9 (agreeability level towards the statement "Iris – Retina (eyes) Biometric process would take over the future") is having the least agreeability score whereas question 11 (agreeability level towards the statement "Face recognition Biometric process would take over the future") has median agreeability score.

### 5.1.4 Findings based On Factor Analysis

Among the agreeability level type questions, the following groupings based on priority can be formed.

I factor: Questions 12 and 15 (implementation factor)

II factors: Questions 8 and 21 (improvement factor)

III factor: Questions 7, 9 and 11 (alternatives factor)

IV factor: Questions 6 and 10 (security factor).

## 5.2 Conclusion

A Biometric system which relies only on a single biometric identifier in making a personal identification is often not able to meet the desired performance requirements because of the demerits they have. Face & Fingerprint system overcomes the limitations of face recognition systems as well as fingerprint verification systems. An automatic personal identification system based solely on fingerprints or faces is often not able to meet the system performance requirements. Face recognition is fast but not reliable while fingerprint verification is reliable but inefficient in database retrieval

The integrated system operates in the identification mode with an admissible response time. Similarly other biometric systems can be integrated to achieve more accuracy. So it is recommended that multiple biometrics system is very effective and provides better performance.

# APPENDIX 1

## EFFECTIVENESS OF BIOMETRIC TECHNOLOGIES FOR ATTENDANCE AUTHENTICATION SYSTEM
## A COMPARATIVE STUDY AMONG EDUCATIONAL INSTITUTIONS IN COIMBATORE

Dear Respondent,

I, Surya Ganesan, working as Senior Software Engineer at BOSCH, pursue MBA in Anna University Chennai at the study centre Kumara guru College of Technology, Coimbatore. I invite you to take up this survey, carried out to study the effectiveness of Biometric Technologies for Attendance Authentication System.

Sincerely,

Surya Ganesan

Please complete the below details:

| | |
|---|---|
| 1. Locality | ○ Urban |
| | ○ Rural |

| | |
|---|---|
| 2. Type of Institution | ○ School |
| | ○ College |

| | |
|---|---|
| 3. No of Staff/student | ○ 1-50 |
| | ○ 50-100 |
| | ○ 100-200 |
| | ○ Above 200 |

| | |
|---|---|
| 4. Current System | ○ Manual attendance |
| | ○ Card Punching/Swiping |
| | ○ Biometrics |

| | |
|---|---|
| 1. How familiar are you with the concept of collection of biometric data? | a) Familiar with the concept<br>b) I heard something about it<br>c) I don't have any idea |
| 2. Are you familiar with biometrics before reading this survey? | a) Yes<br>b) No<br>c) May be |
| 3. For what types of functions might you be willing to accept biometrics use? Rank them on your preference. | ☐ Attendance<br>☐ Library<br>☐ Security<br>☐ Lab |
| 4. Do you believe that biometrics can be totally accurate? | ○ Of course totally accurate<br>○ Somewhat accurate<br>○ Probably not totally accurate, but enough to make them useful in many applications<br>○ Not accurate |
| 5. Do you believe that biometrics can be totally secure? | ○ Of course, totally secure<br>○ Somewhat secure<br>○ Probably not totally secure but secure enough to be used in many applications<br>○ Not Secure |

| | |
|---|---|
| 6. Do you think Passwords & ID cards vulnerable to security attack | ○ Strongly agree<br>○ Agree<br>○ Neither agree nor disagree<br>○ Disagree<br>○ Strongly disagree |
| 7. Do you think Biometrics sensors vulnerable to security attack | ○ Strongly agree<br>○ Agree<br>○ Neither agree nor disagree<br>○ Disagree<br>○ Strongly disagree |
| 8. Whether Finger print Biometric process would you believe to take over the future? | ○ Strongly agree<br>○ Agree<br>○ Neither agree nor disagree<br>○ Disagree<br>○ Strongly disagree |
| 9. Whether Iris – Retina (eyes) Biometric process would you believe to take over the future? | ○ Strongly agree<br>○ Agree<br>○ Neither agree nor disagree<br>○ Disagree<br>○ Strongly disagree |
| 10. Whether Voice recognition Biometric process would you believe to take over the future? | ○ Strongly agree<br>○ Agree<br>○ Neither agree nor disagree<br>○ Disagree |

| | |
|---|---|
| 1. Whether Face recognition Biometric process would you believe to take over the future? | ○ Strongly agree<br>○ Agree<br>○ Neither agree nor disagree<br>○ Disagree<br>○ Strongly disagree |
| 2. Whether a combination of two or three Biometric process would you believe to take over the future? | ○ Strongly agree<br>○ Agree<br>○ Neither agree nor disagree<br>○ Disagree<br>○ Strongly disagree |
| 13. Will your institute likely to adopt Biometric process? | ○ Most likely<br>○ Quite likely<br>○ Can't say<br>○ Most dislike<br>○ Dislike |
| 14. Whether have they implemented Biometric systems in all areas of the institute or in particular areas/places? | ○ All departments/offices<br>○ Only _____ |
| 15. Do you think it is more effective than the traditional authentication process? | ○ Strongly agree<br>○ Agree<br>○ Neither agree nor disagree<br>○ Disagree<br>○ Strongly disagree |

| | |
|---|---|
| 16. Have you come across to a situation where your institute's biometrics system failed to recognize you? | ○ Yes<br>○ No<br>○ Don't remember |
| 17. If yes, how many times? | ○ Less than 3 times<br>○ 3 to 7 times<br>○ More than 7 times |
| 18. In what ways the performance of Biometric process can be improved? | ○ Error free<br>○ Increased process speed<br>○ Don't know |
| 19. Does your institute provide alternate arrangements to get through the Biometric system in case of failure? | ○ Yes<br>○ No<br>○ Don't know |
| 20. How comfortable are you to use Biometric system in comparison with traditional one? | ○ Very Comfortable<br>○ Somewhat comfortable<br>○ Not comfortable at all |
| 21. Do you feel that the performance of Biometrics system in your institute can be improved? | ○ Strongly agree<br>○ Agree<br>○ Neither agree nor disagree<br>○ Disagree<br>○ Strongly disagree |

Thanks for your Participation!!!!

## REFERENCES


1. Arpita Gopal, Chandrani Singh (2009) "Emerging Trends in Information Technology", Excel Publication, New Delhi.
2. Ashbourn, Julian (2000) "Biometrics: Advanced Identity Verification", Springer, London.
3. Baird, Stephen (February 2002) "Biometrics", The Technology Teacher.
4. Jain, Anil et al (2000) "Biometric Identification", Communications of the ACM v43 n2.
5. Nanavati, Samir et al (2002)"Biometrics: Identity Verification in a Networked World", Wiley Computer Publishing, New York.
6. Pero, Jennifer (July 23, 2002) "Biometric standards pave the way for greater implementation", Government Security.
7. Prabhakar S, Pankanti S, and A.K. Jain (2003), "Biometric Recognition: Security and Privacy Concerns," IEEE Security & Privacy, vol. 1, no. 2, pp. 33–42.
8. Rula Abu Samaa (April 2003)"Biometrics Authentication Systems", PP 1-2.
9. Tilton, Catherine J (2000) "An Emerging Biometric API Industry Standard", IEEE Computer v33 n2.
10. Vicki Koerper (March 10, 1998) "Biometrics: A Brief Introduction".