Project Dissertation Report on

ON

ANALYSING THE EMPLOYEE PERCEPTION OF BIOMETRIC SYSTEM IN GOVERNMENT OFFICES

Submitted By:

Siddharth Pillai

2K17/MBA/091

Under the Guidance of:

Prof. P.K Suri

Professor

DELHI SCHOOL OF MANAGEMENT

Delhi Technological University
Bawana Road Delhi 110042

DECLARATION

I, Siddharth Pillai, student of MBA 2017-19, of Delhi School of Management, Delhi Technological University, Bawana Road, Delhi-42, declare that the final project report on "Analyzing the employee perception of biometric system in government offices", submitted in partial fulfillment of Degree of Masters of Business Administration, is the original work conducted by me.

The information and data given in the report is authentic to the best of my knowledge.

This report is not being submitted to any other University for award of any other Degree, Diploma and Fellowship.

Siddharth Pillai

Place:

Date:

CERTIFICATE FROM THE INSTITUTE

This is to certify that the Project Report titled "Analyzing the employee perception of biometric system in government offices", is a bona fide work carried out by Mr. Siddharth Pillai, of MBA 2017-19 and submitted to Delhi School of Management, Delhi Technological University, Bawana Road, Delhi-42 in partial fulfillment of the requirement for the award of the Degree of Master of Business Administration.

Signature of Guide

(Prof. P.K Suri)

Signature of HOD

(Dr. Rajan Yadav)

Place:

Date:

ACKNOWLEDGEMENT

I am using this opportunity to express my gratitude to everyone who supported me throughout the course of this MBA project at Delhi School of Management, Delhi Technological University. One of the most important tasks in every good study is its critical evaluation and feedback which was performed by my faculty guide Prof P.K Suri. I am thankful to faculty mentor as well as my colleagues for investing their precious time to discuss and criticize this study in depth and explain the meaning of different concepts and how to think when it comes to problem discussions and theoretical discussions.

My sincere thanks go to my Institute and family, who supported and encouraged me.

Siddharth Pillai

2K17/MBA/91

Contents

Executive Summary

This project discusses an exploratory study of government employees' perceptions of the introduction of biometric authentication at the workplace Government Offices. The author suggest that studying the factors affecting employees' acceptance of new technology will help ease the adoption of biometric technology in other e-government applications. A combination of survey and interviews was used to collect the required data. Interviews were conducted with managers and questionnaires were given to employees from two different government organisations in Government Offices to investigate the employees' perceptions of using biometrics. The results of this study indicate a significant digital and cultural gap between the technological awareness of employees and the preferred authentication solutions promoted by management. A lack of trust in technology, its potential for misuse and management motives reflect the managers' need to consider their responsibilities for narrowing these gaps. It was apparent that overcoming employees' resistance is an essential issue facing biometric implementation. Based on the research the authors recommend that an awareness and orientation process about biometrics should take place before the technology is introduced into the organisation.

As part of the "Digital India" program of Government of India, it has been decided to implement common Biometric Attendance System (BAS) in the Central Government Offices (Agencies) located in Delhi which may be extended to offices of the state and governments and other government institutions in future. The proposed system would enable an employee to register attendance by simply presenting his/her biometric (finger print/Iris). This event will be authenticated online after one to one match with the bio-metric attributes stored in the UIDAI data base against the employee's Aadhaar number.

For implementing this project, the Central Government Organizations need to follow a structured approach in coordinating with different stakeholders. The purpose of this document is to serve as handbook for the Central Government organizations that are implementing Bio-metric Attendance System for their employees.

Chapter-1
INTRODUCTION OF THE TOPIC

- **Profile of Industry**
- **Objectives of Study**

1.1 Profile of Industry

New technologies constantly evolve new dimensions to daily life. They can be used to provide interactions between users and their governments through electronic services. Governments are looking for more efficient and effective uses of technology in order to electronically deliver their services (Alharbi, 2006; Scott, 2005). Electronic government (e-government) has therefore become an important world-wide application area. With e-government applications, users are required to provide governments with personal information which necessitates an efficient, secure technology to provide reliable methods, particularly for users' identification as well as secure information systems. Thus, the implementation of e-government is facing important issues such as information security, user authentication and privacy in which biometric authentication is a potential solution to deal with such concerns (Dearstyne, 2001). It can provide reliable identification of individuals as well as the ability for controlling and protecting the integrity of sensitive data stored in information systems (McLindin, 2005). As a result, several governments have implemented biometric authentication systems in order to efficiently and securely provide their services.

However, the adoption of biometrics in e-government has become a major component of political planning for several governments. In particular, user acceptance can be an essential factor for the successful implementation of biometrics (Ashbourn, 2004; Giesing, 2003; Scott, 2005). Moreover, users can have a direct impact on the operational performance of biometric systems, so their concerns need careful consideration, even if their concerns are fairly rough and ill defined (Ashbourn, 2004).

This paper discusses a study conducted in the Kingdom of Saudi Arabia of government employees' perceptions of the introduction of biometric authentication at the workplace in 2008.

The aim is gain an understanding of factors affecting the employees' acceptance of biometrics and to advice on how to successfully adopt biometrics in e-government applications. The project is structured as follows. The relevant literature is reviewed followed by the description of the empirical study that involved a descriptive survey and interviews of the managers and employees in two organisations.

Electronic government involves the citizens of that country in certain government activities in order to help solve problems. E-government provides unparalleled opportunities to streamline and improve internal governmental processes, enhance the interactions between users and government, and enable efficiencies in service delivery (Scott, 2005). It refers to the use of information technology by government agencies in order to enhance the interaction and service delivery to citizens, businesses, and other government agencies (Alharbi, 2006; AlShihi, 2006). Thus, there are four categories of e-government applications which are: Government-to-Citizen (G2C); Government to- Business (G2B); Government-to-Government (G2G); and Government-to-Employee (G2E) (AlShihi, 2006).

Biometric Authentication Technology

Biometric technology provides a range of automated methods which can used to measure and analyze a person's physiological and behavioural characteristics. Physiological biometrics includes fingerprint recognition, iris recognition, facial recognition, and hand recognition. Behavioural biometrics contains voice patterns and signatures, which are usually taken for identification and verification purposes. Basic authentication is usually based on something somebody knows, like a pin or a password, or something somebody has, like a key, passport or driver's license. The limitations of these authentication measures in some application areas have

led to the development and adoption of biometric technology which is now used to identify individual behaviours and characteristics.

Biometric technology usually involves a scanning device and related software which can be used to gather information that has been recorded in digital form. Having digitally collected the information, a database is used to store this information for comparison with the previous records. When converting the biometric input, namely the already collected data in digital form, this software can now be used to identify the specific inputs into a value that can be used to match any data previously collected. By using an algorithm, the data points are then processed into a value that can be compared with biometric data in the database.

Examples of Biometric Technology in E-government Applications

By using biometric technology, e-government aims to give its citizens improved services with efficient and secure access to information by providing reliable identification of individuals as well as the ability for controlling and protecting the integrity of sensitive data stored in information systems. Most researchers such as Ashbourn, Bonsor and Johnson , Scott , and Wayman et al. argue that a wider use of biometric technology can be applied to e-government projects.

Currently biometric technology is used for applications like e-voting to ensure that voters do not vote twice. With biometric technology, governments are better able to prevent fraud during elections and other transaction types. Moreover, biometric technology has most recently been used to ensure correct working times are recorded and that only authorized personnel have access to government property and resources. Biometric technology can also be used by e-governments for business. For instance, banks frequently adopt a facial feature recognition system to ensure that there is a reduced potential for theft. For example, photos are taken on the bank slips

which are stored on computer software. As a result, this has avoided the issue of fraudulent bank slips when withdrawing money at ATMs. These technological advances in authenticating dealings with business have helped the government to conduct its activities more effectively and more securely.

In business transactions there is frequently the need for full authentication of employees to ensure that, in case of any problem, management is in a position to identify the person responsible for that act. Commercial applications may also require full identification capability, digital certificates, human interface, and one or more authentication devices to ensure that the business can run safely and effectively. People are also in a position to do their business with increased trust. Digital trust through public key cryptography, strong authentication and certification allows greater transaction confidence as long as that organisation has a certified identity as an effective and trustworthy company. Biometric technology is also used in the identification of citizens by e-government applications. Every nation could ethically be able to identify its citizens and differentiate non-citizens by using variations of national identification cards, visas, and passports with biometric data encoded within. Prior to the use of biometric data with such documents they were too easily forged or altered to allow unauthorized access to resources and facilities. As a result many nations have avoided the use of mechanisms such as a national identity card in the past.

Effective e-government biometric applications to authenticate and identify citizens have effectively been used in reducing the issues of illegal immigration, access bottlenecks in busy facilities and high costs of employing security personnel. The Australian Customs established an automated passenger processing system, that is, the e-passport SmartGate at Sydney and Melbourne airports, and it aims to introduce self-processing by employing facial recognition

systems to confirm identities and streamline the travellers'' facilitation procedures . E-government facilities use the various types of biometric identification in order to control certain illegal behaviour. For example, the Japanese government plans to use biometric technology in passports to tackle illegal immigration and to enable tighter controls on terrorists. This will be applied within a computer chip which can store biometric features like fingerprints and facial recognition. Other e-government applications are using the biometrics for certain defence bases for secure areas. For instance, hand recognition has been used at the Scott Air Force Base to save more than $400,000 in manpower costs through their metro-link biometric access gate.

Concerns about the Use of Biometric Technology

While biometrics can provide a high level of authentication through identifying people by their physiological and behavioural characteristics, there are also several negative aspects. Biometrics can sometimes be ineffective when using the various styles of identification. For instance, fingerprints can be saturated, faint, or hard to be processed with some of devices, particularly if the skin is wet or dry. Hand recognition can sometimes be ineffective when the hand is damaged, thereby no results will be obtained to match with the images already in the database. Few facilities have databases or hardware to employ iris recognition, which makes the upfront investment too high to initiate a worldwide iris ID system. Biometric technology has also been criticized for its potential harm to civil liberties. This is because people have been denied access to the various regions and countries simply because they do not have the correct identities for those places. Moreover, there is potential for people's privacy to be violated with this new technology.

Prime Minister Narendra Modi's Push For An Aadhaar-Enabled Biometric System May Have Increased Efficiency In Central Government Offices, But It Has Also Detected That A Large Number Of Employees Working In 169 Different Offices In The National Capital, Either Stay Away From Duties Or Don't Mark Their Attendance Through This New Biometric System

Out of 63,883 registered employees working in these offices, the system installed since last September has found that just 24,646 employees are registering their attendance through this system.

Top officials told dna, while it is early to conclude if they are "ghost employees" parasitizing on the state exchequer. Meanwhile, a final circular has been sent to all central government offices to explain such a large difference between the registered employees and the number of employees turning up to attend their duties.

An office memorandum has been sent to 169 different central government departments by the ministry of personnel, under prime minister has asked heads of these offices to explain the difference and if the employees are not using the AEBAS system, they be asked to use it forthwith.

"All employees are, therefore, required to register themselves in the system and mark their attendance. Instructions already exist for dealing with cases of late attendance/unauthorised absence, which may be followed," says the circular.

In the office of additional directorate general personnel of ministry of defence, out of 150 registered employees, no one has so far been marking their attendance, through the new system. In the Akanshka office of same ministry out of 99 employees, just seven are marking their

attendance. In the central water commission, which has total 1,012 employees at its sprawling office, last four months only 562 employees have been showing up. Also in the central ground board office, out of 37 employees, just seven are marking attendance. The biggest office in Delhi central public works department which has 10,514 employees, less than half 2,456 are marking attendance, as per the data.

Interestingly, in the Defence Research and Development Organisation (DRDO) which has 542 registered employees in Delhi, none is marking attendance, even though they played a role in designing the system. In the press council of India, which has 69 employees, only four have been marking attendance.

According to a study conducted by the government itself, the system has kept the employees on toes and on an average they are spending nearly twenty minutes extra in office every day.

"Ever since the system was launched, the average presence time in office of the registered employees has risen by about 20 minutes per day. Considering that over 47,000 employees are using it now, an average gain of 20-minutes per day means an approximate gain of 16,000 man-hours," said an official at the ministry of personnel.

Currently, 387 organisations have implemented the biometric system of attendance. Prime minister's office (PMO) has already asked all ministries to phase out the manual system of attendance. The government has also specified that disciplinary actions may be taken against officials who are habitual late-comers and also stated that early departure from work will also be treated as a violation similar to late-coming.

1.2 Objectives & Scope:

- To ascertain employee satisfaction towards biometric system
- To understand if biometric system maintain discipline at work
- To identify the extent to which biometric usage can affect the organizational performance

Chapter-2:

Theoretical Framework and Research Methodology

- **CONCEPTUAL FRAMEWORK**
- **LITERATURE REVIEW**
- **RESEARCH METHODOLOGY**

2.1 Conceptual framework

Biometrics technology can be used as a type of employee time management system because of its ability to recognize people's unique physiological characteristics. Biometrics based time and attendance terminals are becoming increasingly popular in today's market because of their many benefits (and, lets face it, hand or face scanning equipment is just pretty awesome). Because biometrics terminals read a person's unique fingerprint, iris, hand shape, or face shape, they ensure that employees cannot clock in for one another, thereby preventing employee time theft.

One of the most prevalent biometric technologies is the fingerprint recognition system; by placing a finger on the scanner, the time clock terminal reads the fingerprint and allows the person to clock in or out. Learn more about how fingerprint biometric time clocks work.

Another biometrics terminal that Acumen carries has the ability to recognize hand shape and size. I originally assumed that the device was capturing a three dimensional image of the hand being scanned when I first saw the system. However, in reality, it captures unique "minutia points" on the hand of the employee and measures between the points, then hashes the measurement to a single unique value that is transmitted for verification.

This technology is not restricted to just hands and fingers; there are terminals that scan a person's iris to recognize the individual. Additionally, certain systems capture an image of a person's unique face shape and use this to allow employees access to features on the terminal.

One of the newest and most interesting types of biometrics technology deals with recognizing the unique patterns that veins make in a person's hand. Because these patterns are intricate and highly complex, it is nearly impossible for one person to clock in as another. The technology,

therefore, has very low false acceptance and false rejection rates and is used in especially high security areas.

In this way, biometrics is extremely useful both in helping businesses feel secure and in eliminating employee time theft, as it relies on personal characteristics that vary between individuals. The wide variety of easy to use terminals ensures that biometrics is a smart (and cool) solution when deciding what kind of time and attendance system to purchase for your company.

5 Types of Biometric Devices!

There are many types of biometric devices, but there are five types of biometrics security that are most commonly used. You can often see these special biometric devices in movies and TV shows, but you will find that these types of biometric security devices can be found in the most mundane places.

Biometrics is basically the recognition of human characteristics that are unique to each human, which can include facial recognition, fingerprints, voice recognition, retina scans, palm prints, and more.

Using this biometric technology to keep your devices safe is the best way to ensure that people stay out of your valuable possessions and information, and you will find that using any one of these five biometrics security devices is a great way to keep things safe:

Types of Biometric Devices Available:

Retina Scanner - These scan the unique biometric pattern in each person's iris, and match it against a certain number of unique identifying marks that set every person apart from everyone else.

Iris scanning and retinal scanning are both used to identify a person according to their unique pattern, but they tend to be far costlier and more complex.

Finger Print Scanner - As far as price goes, the fingerprint scanning is on the lower end of the scale. The cheapest fingerprint scanners are the ones that only scan the actual print, though the costlier ones actually scan the presence of blood in the fingerprint, the size and shape of the thumb, and many other features. These costlier systems actually capture a 3D image of the fingerprint, thereby making it much more difficult for the fingerprint to be counterfeited.

Facial Biometrics - Each person around the world has a distinctly unique face, even two twins that the human eye cannot tell apart. It may be something as small as the slightly different placing of the eyebrows, the width of the eyes, or the breadth of the nose.

There are certain markers that enable these biometric recognition scanners to instantly identify the uniqueness of each person scanning their facial features, thus enabling the device to ensure that only the single person with the correct bone structure and feature placement can gain access.

Voice Recognition - Every person in the world has a unique voice pattern, even though the changes are slight and barely noticeable to the human ear. However, with special voice recognition software, those tiny differences in each person's voice can be noted, tested, and

authenticated to only allow access to the person that has the right tone, pitch, and volume of voice. It can be surprisingly effective at differentiating two people who have almost identical voice patterns.

Hand Print Patterns - When you place your hand on a scanner, you not only have a unique fingerprint pattern, but the size and shape of your entire hand is also very unique.

This includes the width and length of your palm, the width and length of your fingers, the distance between each knuckle, and the depth of each of the lines in your palm. This is more complex than regular fingerprint scanning, and will be much more accurate with less chance of falsification.

Some of these products will be far costlier than the others, as they feature technology that is much more complex. However, the amount that you spend on the various types of biometric devices will be directly proportionate to the level of security you need. The more secure you want your home or business to be, the more costly your device will be.

Goodness and weakness about the current technology

Each one of the Technologies used in our days bring us a manner to restrict the access to a system, allowing the entrance only to those persons who know a specific code, own a card or have determined physic marks. The more complex is the system, the most difficult is to be attacked, although it will be more expensive and will require more software and hardware resources. When a new authentication system is implanted, it is essential a judgement between simplicity, price and efficiency, as well as social acceptability.

The password method is the cheapest and simplest technology, because it only requires elementary software resources.

On the other hand, this system is easily attackable, since he is quite simple to obtain the data from a person, either extracting the information to the person itself using deceits, or attacking the software of the system. For example, it can be easily installed in the computer, a program that simulates the “user name and password” window, so that when the user introduces his data in that window, that will be collected by the “Spy” program. Immediately after this, it appears the true window, identical, and the user will simply believe that he has been mistaken. So, this method, in spite of being usually used, for example, to access banking accounts, is not at all the most indicated if we want a safe system, and in a short-time future is tried to be changed by most immune methods.

The Smart Cards are very useful since they can be easily combined with other authentication systems, serving as storage system. Self-containment of smart card makes it resistant to attack as it does not need to depend upon potentially vulnerable external resources. But its small size and bend requirements (which are designed to protect the card physically), limits the memory and

processing resources. And used like the only identification system, is not excessively trustworthy, since it can be easily stolen, lost or simply forgotten at home. Besides, sometimes they are combined with cryptography methods, which makes them more difficult (more expensive) to implement.

The Digital Signature is very difficult to falsify, since is encrypted by complicated mathematic operations. It is considered that is even less falsifiable than the manual signature recognition (although this last is already enough trustworthy).

The advantage that Biometrics presents is that the information is unique for each individual and that it can identify the individual in spite of variations in the time (it does not matter if the first biometric sample was taken year ago).The pillars of e-learning security are: authentication, privacy (data confidentiality) authorization (access control), data integrity and non-repudiation. Biometric is a technique that can provide all this requirements with quite lot reliability.

Although biometrics is considered the most effective and safe method (is very difficult to falsify), we have to bear in mind its disadvantages, for example, that since it is a relative new technology, it is not still integrated in PC, so IT departments need to make a conscious decision before making the purchase and change its structure.

We also have to consider the advantages and disadvantages of each individual system. In the next paragraphs, we will make an enumeration of the problems that these techniques can present:

Facial recognition:

Advantages:

a. Non intrusive

b. Cheap technology.

Disadvantages

a. 2D recognition is affected by changes in lighting, the person's hair, the age, and if the person wear glasses.

b. Requires camera equipment for user identification; thus, it is not likely to become popular until most PCs include cameras as standard equipment.

Voice recognition:

Advantages:

a. Non intrusive. High social acceptability.

b. Verification time is about five seconds.

c. Cheap technology.

Disadvantages:

a. A person’s voice can be easily recorded and used for unauthorised PC or network.

b. Low accuracy.

c. An illness such as a cold can change a person’s voice, making absolute identification difficult or impossible.

Signature recognition:

Advantages:

a. Non intrusive.

b. Little time of verification (about five seconds).

c. Cheap technology.

Disadvantages:

a. Signature verification is designed to verify subjects based on the traits of their unique signature. As a result, individuals who do not sign their names in a consistent manner may have difficulty enrolling and verifying in signature verification.

b. Error rate: 1 in 50.

DNA:

Advantages:

a. Very high accuracy.

b. It impossible that the system made mistakes.

c. It is standardized.

Disadvantages:

a. Extremely intrusive.

b. Very expensive.

Retinal scanning:

Advantages:

a. Very high accuracy.

b. There is no known way to replicate a retina.

c. The eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to been taken with retinal scans to be sure the user is a living human being.

Disadvantages:

a. Very intrusive.

b. It has the stigma of consumer's thinking it is potentially harmful to the eye.

c. Comparisons of template records can take upwards of 10 seconds, depending on the size of the database.

d. Very expensive.

Iris recognition:

Advantages:

a. Very high accuracy.

b. Verification time is generally less than 5 seconds.

c. The eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to been taken with retinal scans to be sure the user is a living human being.

Disadvantages:

a. Intrusive.

b. A lot of memory for the data to be stored.

c. Very expensive

Fingerprint:

Advantages:

a. Very high accuracy.

b. Is the most economical biometric PC user authentication technique.

c. it is one of the most developed biometrics

d. Easy to use.

e. Small storage space required for the biometric template, reducing the size of the database memory required

f. It is standardized.

Disadvantages:

a. For some people it is very intrusive, because is still related to criminal identification.

b. It can make mistakes with the dryness or dirty of the finger's skin, as well as with the age (is not appropriate with children, because the size of their fingerprint changes quickly).

c. Image captured at 500 dots per inch (dpi). Resolution: 8 bits per pixel. A 500 dpi fingerprint image at 8 bits per pixel demands a large memory space, 240 Kbytes approximately → Compression required (a factor of 10 approximately).

Hand Geometry:

Advantages:

a. Though it requires special hardware to use, it can be easily integrated into other devices or systems.

b. It has no public attitude problems as it is associated most commonly with authorized access.

c. The amount of data required to uniquely identify a user in a system is the smallest by far, allowing it to be used with SmartCards easily.

Disadvantages:

a. Very expensive

b. Considerable size.

c. It is not valid for arthritic person, since they cannot put the hand on the scanner properly.

2.2 Literature Review

Biometrics is the technology of identifying individuals or authenticating identity using distinctive physical or behavioural patterns. Biometric systems require two operational dimensions:

(a) Enrolment, in which biometric data are obtained and linked with a person's identity and

(b) Authentication or recognition, in which new biometric data are compared with the stored data. With biometrics, data from a fingerprint, for example, are collected and transmitted to a computer to processes to identify a match within the stored database, allow access to an area, and document the entry time of a given individual. This information can be printed or retrieved at a later time to determine all those who accessed the area in question. An inventory of biometric systems includes fingerprinting, face and voice recognition, hand geometry, handwriting pattern

recognition, and iris and retinal scanning. This data is accurate, convenient, and cannot be stolen or replicated because it is unique to only one subject. Thus, they are considered more reliable than the traditional recognition and identification systems.

The wide spread application of biometrics in personal identification of consumer goods such as portable computers has led to $3 billion in sales in 2012. Biometrics has also been applied in airports, by airlines, and check-out points of sales and has proven effective, convenient, and time saving. These point to the increased acceptance and trust of this technology by consumers. However, adoption of new technology is considered successful when employees embrace and use it effectively. The literature review revealed a gap in studies on biometrics acceptance by employees, yet employees are a major part of the equation when trying to implement such technology. Adoption of new technology is considered successful when employees embrace and use it effectively. Therefore, the purpose of this study was to explore perceptions and acceptance of biometric technology by employees in hotels: trying to find out the factors that influence employees. Attitudes and intentions to use biometric systems in hotels.

According to Lockie (2002, p. 10), the biometric industry did not really get established until the middle of the twentieth century. The researchers at that particular time were investigating whether various human parts and characteristics, such as the iris or the voice, could be used to identify an individual. This was made public by publishing papers and as a considerable number of these strands of research began to form a piece, the biometrics industry as we know it these days was established.

(Liu 2001, p.27). "As organization search for more secure authentication methods for user access, e-commerce, and other security applications, biometrics is gaining increasing attention"

Higgins, Orlan and Woodward (2003, p. xxiii), emphasized that even though biometrics have not become an essential part of all systems requiring controlled access, "the emerging industry has come a long way from its modern founding in 1972 with the installation of a commercial finger measurement device on Wall Street". He made reference to the highly respected MIT Technology Review called biometrics one of the "top ten emerging technologies that will change the world."

The growth in biometric industries is reflected in the numbers. The trio cited **Rick Noton**, the executive director of the International Biometric Industry Association (IBIA), who reported in the Biometrics 2002 Conference in London, United Kingdom, that the industry's trade association has indicated the surge in biometric revenues over recent years. From $20 million in 1996, it has increased to $200 million in 2001 and Norton believes they will increase as the years pass on significantly in 5 years time.

Also, a forecast made by the International Biometric Group (IBG), which is a biometric consulting and integration firm located in New York City, estimate that biometric revenues totaled $399 million in 2000 and will increase to $1.9 billion by 2005. Both IBIA and IBG believe that the private sector will be responsible for much of the growth. These give evidence of the relevance of biometrics in organizations in modern times.

Woodward (2003, p. 197) cited President Clinton's speech in his commencement address at Morgan State University in 1997: "The right to privacy is one of our most cherished freedoms...We must develop new protections for privacy in the face of new technological reality."

Recently, Biometrics has been increasingly deployed to improve security and a very important tool to combat terrorism. Privacy issue is central to biometrics and many people believe that deploying biometrics poses a considerable level of risk to human rights, even though some are of the opinion that biometrics actually protect privacy.

Human factors influence the success of a biometric-based identification system to a great extent. The ease as well as comfort in interaction with a biometric system contributes to how people accept it.

Jain, Ross and Prabhakar (2004 p. 24) stated an example of a biometric system being able to measure the characteristic of a users without touching, such as those using voice, face, or iris, and concluded that it may be perceived to be a more user-friendly and hygienic system by the users. They added that on the other hand, biometric characteristics not requiring user participation or interaction can be recorded without the knowledge of the user, and this is perceived as a threat to human privacy by many individuals.

According to Sim (2009, p. 81), biometrics compared to other security technologies has significant impacts on user's privacy (Civil Liberties). It can protect privacy when deployed in an appropriate manner; but when misused, it can result in loss of privacy.

Chapman,Uggerslev, Carroll, Piasentin, & Jones, 2005

Human capital is one of the most valuable assets of an organization and recruitment serves the important function of attracting the necessary talent (chapman,uggerslev, carroll, piasentin, & jones, 2005).

Demographic trends such as a smaller supply of younger workers and retirements among baby boomers indicate that recruitment and applicant attraction will be even more important in the future**(breaugh, 2008).**moreover, given that recruitment influences the quantity and quality of the applicant pool, it has implications for all other human resources practices **(carlson, connerley, & mecham, 2002).** As a result, recruitment has become one of the most critical humanresource functions for organizational success and survival **(saks, 2005).**previous research has demonstrated that organizations can benefit from actively involving their current employees in the recruitment of new personnel (breaugh, 2008). In fact, positive employee referrals have been found to be one of the most effective recruitment sources, given their positive impact on pre-hire recruitment outcomes such as organizational attractiveness and application decisionsas well as on post-hire attitudes and job performance(van hoye & lievens, 2009; weller, holtom, matiaske, & mellewigt, 2009; zottoli & wanous, 2000). In addition, recent research suggests that negative organizational information from current employees can have a detrimental impact on organizational attraction **(kanar, collins, & bell, 2010; van hoye & lievens, 2007 b).**

ULLMAN, 1966

Job seekers learn about job openings through a wide array of sources such as advertising, job sites, and word-of-mouth. Word-of-mouth as a recruitment source is defined as an interpersonal communication about an organization as an employer or about specific jobs, that is not under the direct control of the organization(for a detailed overview of the literature, see van hoye, in press).

Employee referrals can be regarded as a specific kind of word-of-mouth communication, with current employees of the recruiting organization acting as the source of interpersonal employment information(ullman, 1966).

BREAUGH, 2008

Although the effectiveness of recruitment sources is one of the most intensely researched aspects of recruitment, the focus has been on post-hire instead of pre-hire outcomes (breaugh, 2008). The main finding is that employees recruited through informal sources such as employee referrals show higher job satisfaction, better job performance, and lower turnover than employees recruited through formal sources such as advertising(welleret al., 2009; williams, labig, & stone, 1993; zottoli & wanous, 2000). In addition, recent studies indicate that recruitment sources can also have differential effects on pre-hire outcomes such as organizational attractiveness, application decisions, and the quantity and quality of the applicant pool, with informal sources generally outperforming formal sources (collins & han,2004; collins & stevens, 2002; jaidi, van hooft, & arends, 2011; van hoye, 2012; van hoye & lievens, 2009).

KANAR ET AL., 2010

Although most research has focused on sources of positive employment information, a few studies have also considered the effects of sources of negative information such as negative word- of-mouth and negative publicity on organizational attraction (kanar et al., 2010; van hoye & lievens, 2005, 2007b). This is important because if job seekers are not initially attracted to organizations, they disappear from the recruitment process and cannot be reached by later recruitment or selection activities (carlson et al., 2002). With respect to employee referrals, van

hoye and lievens (2007b)and kanar et al. (2010)found that negative word-of-mouth can have a detrimental impact on organizational attraction. Moreover, negative word-of-mouth had a stronger effect on attraction than positive word-of-mouth.

AMBROSE & KULIK, 1999

Work motivation can be defined as the set of internal and external forces that initiate work-related behavior and determine its form, direction, intensity, and duration (ambrose & kulik, 1999). Traditionally, motivation research has distinguished between intrinsic and extrinsic motives (deci, koestner, & ryan, 1999; mayer, faber, & xu, 2007). Whereas intrinsic motivation refers to the motivation to engage in work behavior primarily for its own sake because it is interesting or satisfying, extrinsic motivation is the motivation to perform work behaviors primarily in response to something apart from the behavior itself such as rewards or punishments(amabile, hill, hennessey, & tighe, 1994; ryan & deci, 2000). More recent research has added a third kind of motivation, namely prosocial motivation or the motivation to engage in work behavior primarily to benefit other people(grant, 2007).this three-component theory of work motivation has received substantial empirical support in that intrinsic, prosocial, and extrinsic motives have been shown to predict a wide range of work-related behaviors(amabile et al., 1994; ambrose & kulik, 1999; deci et al., 1999; grant, 2008; grant & mayer, 2009; ryan & deci, 2000).

RYAN & DECI, 2000

First, some employees are likely to recommend their organization as an employer to others (or not) because they are intrinsically motivated (ryan & deci, 2000). Along these lines, marketing

research has found that satisfaction with products or services is one of the main intrinsic determinants of word-of-mouth behavior(bone, 1992; brown, barry, dacin, & gunst, 2005; mangold, miller, & brockway, 1999; wirtz & chew, 2002). Whereas satisfied consumers recommend the product to others, dissatisfied consumers advise against buying the product(de matos & rossi, 2008). This represents an intrinsic motive for making referrals, given that the referral is based on the individual's own attitudestoward the product (shinnar et al., 2004).

Applied to a recruitment context, it is expected that employees who are satisfied with their jobare intrinsically motivated to provide positive referrals while dissatisfied employees are likely to provide negative referrals.

2.3 Research Methodology

Methodology is the systematic, theoretical analysis of the methods applied to a field of study. It comprises the theoretical analysis of the body of methods and principles associated with a branch of knowledge. Typically, it encompasses concepts such as paradigm, theoretical model, phases and quantitative or qualitative techniques.

A methodology does not set out to provide solutions - it is, therefore, not the same thing as a method. Instead, it offers the theoretical underpinning for understanding which method, set of methods or so called “best practices” can be applied to specific case, for example, to calculate a specific result.

It has been defined also as follows:

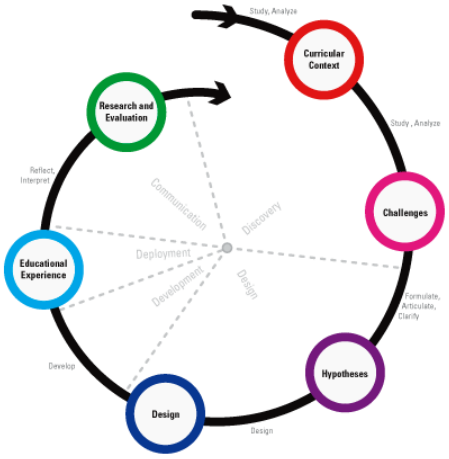
1. "the analysis of the principles of methods, rules, and postulates employed by a discipline"
2. "the systematic study of methods that are, can be, or have been applied within a discipline"
3. "the study or description of methods”

Research Design

The research design is purely and simply the framework of plan for a study that guides the collection and analysis of data. Types of Research Design:

- **Exploratory Research** – The main purpose of such studies is that of formulating a problem for more precise investigation or of developing the working hypotheses from an operational point of view.
- **Descriptive Research** – Those studies which are concerned with describing the characteristics of a particular individual, or of a group.
- **Hypothesis Testing Research** – They are those where the researchers tests the hypotheses of casual relationships between variables.

Descriptive research design was used for this research.



A **research design** is a systematic plan to study a scientific problem. The design of a study defines the study type (descriptive, correlation, semi-experimental, experimental, review, meta-

analytic) and sub-type (e.g., descriptive-longitudinal case study), research question, hypotheses, independent and dependent variables, experimental design, and, if applicable, data collection methods and a statistical analysis plan.

Design types and sub-types

There are many ways to classify research designs, but sometimes the distinction is artificial and other times different designs are combined. Nonetheless, the list below offers a number of useful distinctions between possible research designs.

- Descriptive (e.g., case-study, naturalistic observation, Survey)
- Co relational (e.g., case-control study, observational study)
- Semi-experimental (e.g., field experiment, quasi-experiment)
- Experimental (Experiment with random assignment)
- Review (Literature review, Systematic review)
- Meta-analytic (Meta-analysis)

Sometimes a distinction is made between "fixed" and "flexible" or, synonymously, "quantitative" and "qualitative" research designs. However, fixed designs need not be quantitative, and flexible design need not be qualitative. In fixed designs, the design of the study is fixed before the main stage of data collection takes place. Fixed designs are normally theory driven; otherwise it is impossible to know in advance which variables need to be controlled and measured. Often, these variables are measured quantitatively. Flexible designs allow for more freedom during the data collection process. One reason for using a flexible research design can be that the variable of interest is not quantitatively measurable, such as culture. In other cases, theory might not be

available before one starts the research. However, these distinctions are not recognized by many researchers, such as Stephen Gorard who presents a simpler and cleaner definition of research design.

SAMPLE SIZE

Detail:

Size of Data : 100

Area : New Delhi,Goa

Sampling Technique

Sampling techniques can be broadly classified in to two types:

- Probability Sampling.
- Non Probability Sampling.

METHODS OF DATA COLLECTION--- TESTING OF QUESTIONNAIRE

Primary Data:

Primary data is basically the live data which I collected on field while doing cold calls with the customers and I shown them list of question for which I had required their responses.

Source: Main source for the primary data for the project was questionnaires which I got filled by the customers or some times filled myself on the basis of discussion with the customers.

Secondary Data:

Secondary data for the base of the project I collected from intranet, magazines, newspapers etc.

Statistical Analysis

In this segment I will show my findings in the form of graphs and charts. All the data which I got form the market will not be disclosed over here but extract of that in the form of information will definitely be here.

Tools and techniques of analysis

Tools for analysis

- Bar chart (Bar charts will be used for comparing two or more values that will be taken over time or on different conditions, usually on small data set)
- Pie-chart (Circular chart divided in to sectors, illustrating relative magnitudes or frequencies)

Tools and Techniques

As no study could be successfully completed without proper tools and techniques, sames with my project. For the better presentation and right explanation I used tools of statistics and computer very frequently. And I am very thankful to all those tools for helping me a lot. Basic tools which I used for project from statistics are-

- Bar Charts

- Pie charts

- Tables

Bar charts and pie charts are really useful tools for every research to show the result in a well clear, ease and simple way. Because I used bar charts and pie cahrts in project for showing data in a systematic way, so it need not necessary for any observer to read all the theoretical detail, simple on seeing the charts any body could know that what is being said.

Technological Tools

Ms- Excel

Ms-Access

Ms-Word

Above application software of Microsoft helped me a lot in making project more interactive and productive.

Chapter: 3

Data Presentation & Analysis

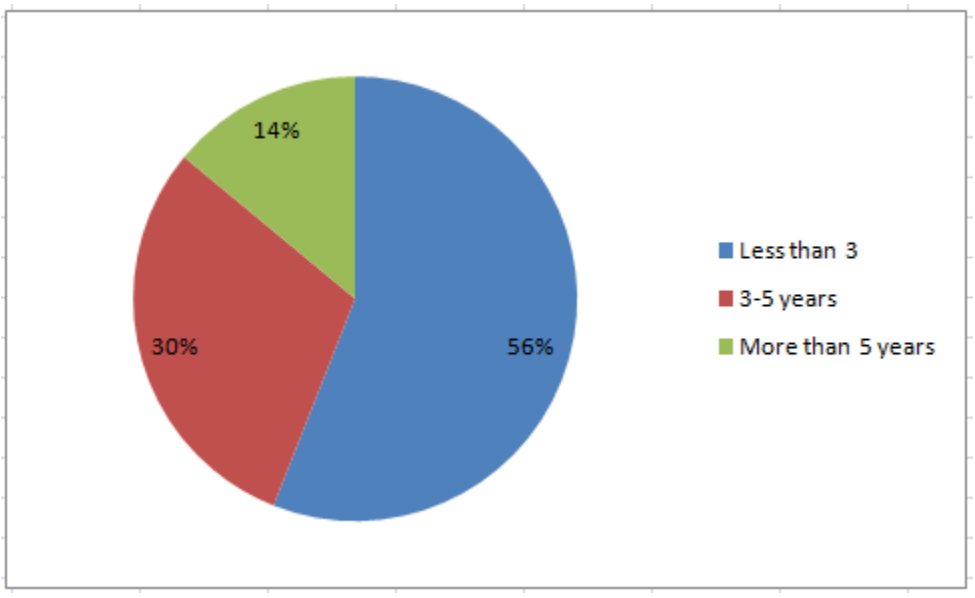
Data Analysis and Interpretation

1. How long have you been working in the Government Offices?

Table no. 1

YEARS	NO. OF EMPLOYEE	PERCENTAGE
Less than 3	56	56%
3-5 years	30	30%
More than 5 years	14	14%
Total	100	100%

Graph No.1



Interpretation:

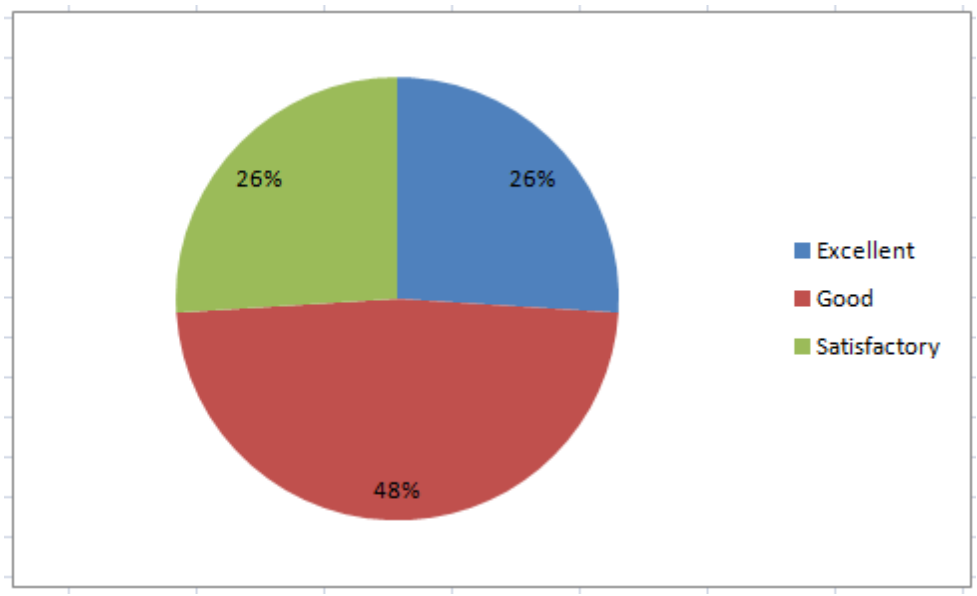
In the above figure shows that most of the employee approx 56% of employee working less than 3 years in the Government Offices.

2. How do you feel the working environment in Government Offices?

Table no. 2

FEEL	NO. OF EMPLOYEE	PERCENTAGE
Excellent	26	26%
Good	48	48%
Satisfactory	26	26%
Total	100	100%

Graph No.2



Interpretation :

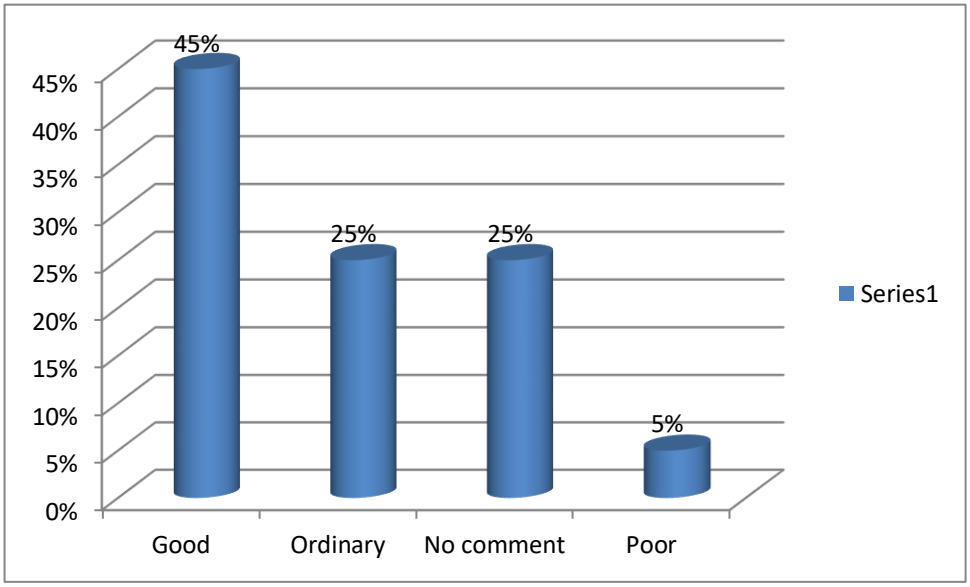
In the above figure shows that 26% of employee feel excellent the working environment, 48% feel good and rest 26% feel satisfactory.

Q.3. What is your perception about Biometric System in Government Offices?

Table No. 3:

Particulars	No. of Respondents	Percentage
Good	45	45%
Ordinary	25	25%
No comment	25	25%
Poor	5	5%
Total	100	100%

Graph No.3:



Interpretation:

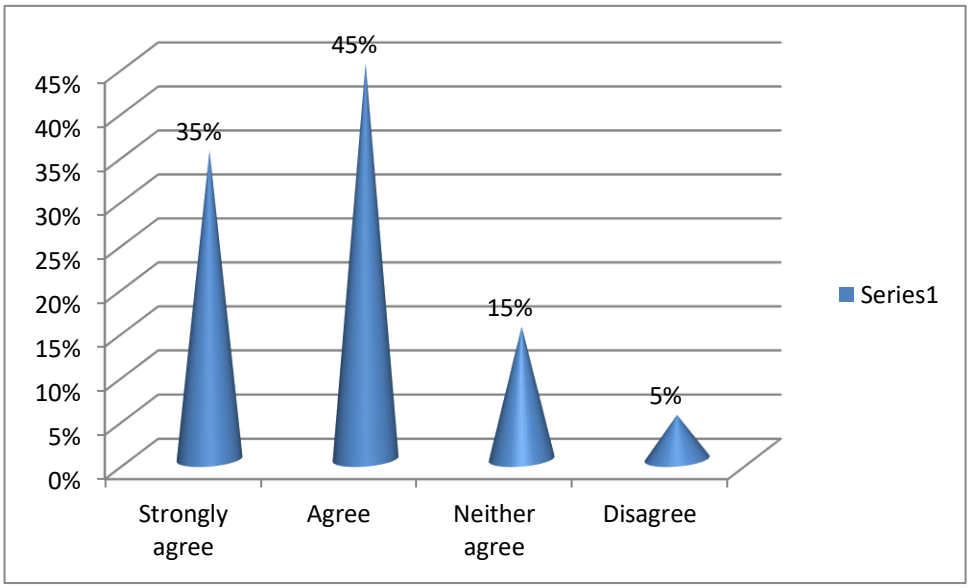
The above graph reveals that good perception comes from 45%, 25% have ordinary perception about the Biometric System in Government Offices and rest by 25% have No Comment, 5% have poor perception.

4.: Biometric System in Government Offices have Good Quality?

Table No.4

Particulars	**Number of Respondent**	**Percentage**
Strongly agree	35	35%
Agree	45	45%
Neither agree	15	15%
Disagree	5	5%
TOTAL	100	100%

Graph No. 4



Interpretation:

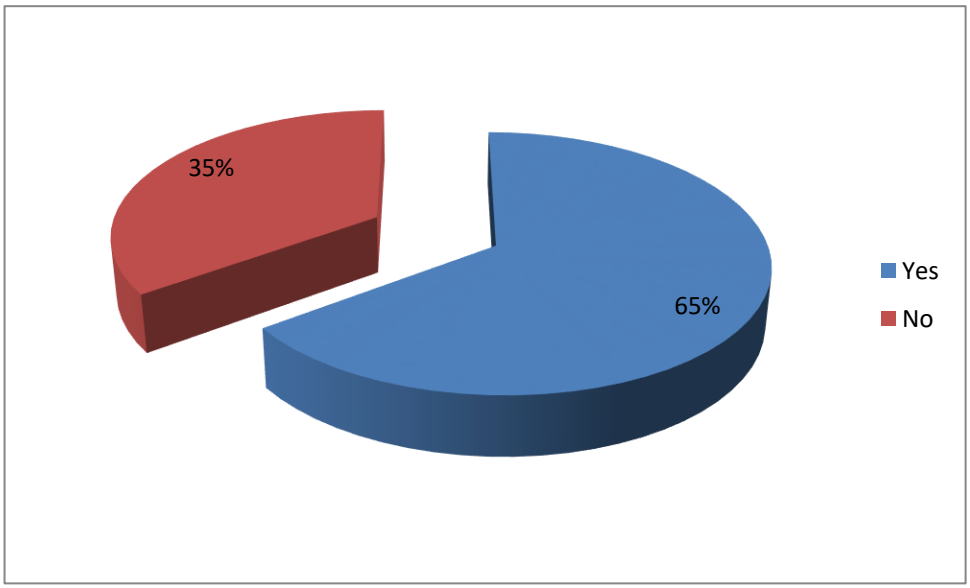
The above graph shows that 35% of respondents strongly agree Biometric System in Government Offices have Good Quality, 45% agree, 15% Neither agree and 5% of respondents disagree.

5. Do you think Biometric System in Government Offices products are more Quality & beneficial than others?

Table No.5:

Product	**No. of Respondent**	**Percentage**
Yes	65	65%
No	35	35%
Total	100	100%

Graph No.5:



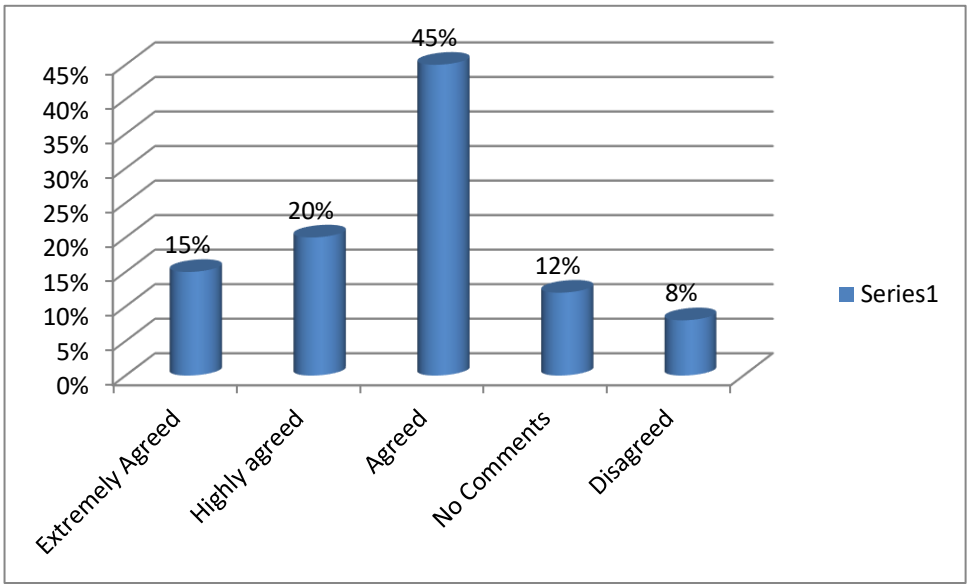
Interpretation: The above graph showing is 65% of respondents says Biometric System in Government Offices are more quality and beneficial than others. Only 35% of respondents Says No.

6.: On the basis of price and feature comparison, is Biometric System in Government Offices economical?

Table. No.6:

	No. of respondents	**Percentage**
Extremely Agreed	15	15%
Highly agreed	20	20%
Agreed	45	45%
No Comments	12	12%
Disagreed	8	8%
Total	100	100%

GRAPH No. 6:



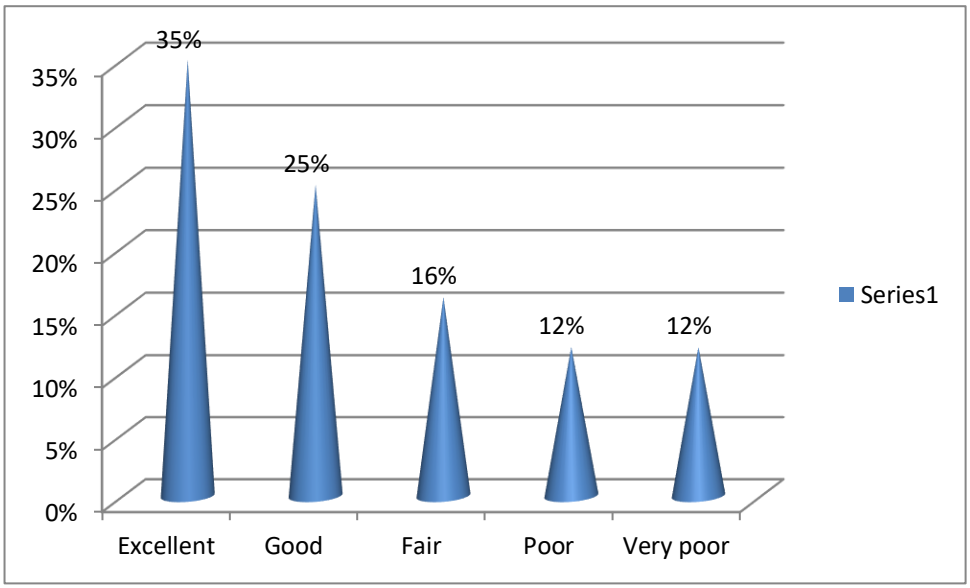
Interpretation: The above graph showing is Biometric System in Government Offices are economical. 15% of public is extremely agreed with this statement, 20% is highly agreed, 45% is agreed and rest of peoples answer is negative.

7. What is the Selling scale System of Biometric System in Government Offices?

Table No.7

	No. of Respondents	**Percentage**
Excellent	35	35%
Good	25	25%
Fair	16	16%
Poor	12	12%
Very poor	12	12%
Total	100	100%

Graph No. 7



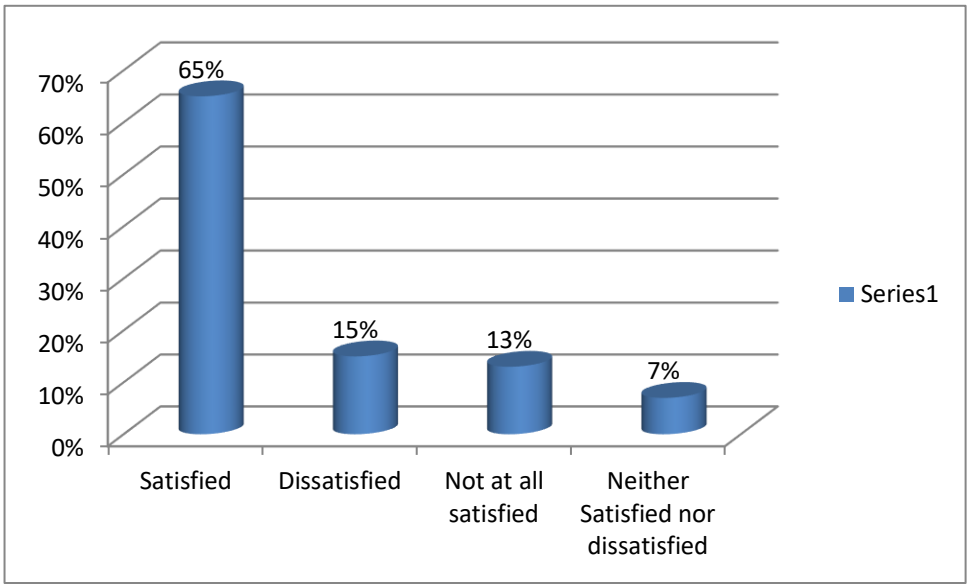
Interpretation: In the above graph shows that 35% of people says excellent about selling scale system of Biometric System in Government Offices, 25% Good, 16% Fair, 12% Poor and rest 12% says very poor.

8. State the level of satisfaction for the Biometric System in Government Offices Products?

Table No.8

	No. of Respondents	**Percentage**
Satisfied	65	65%
Dissatisfied	15	15%
Not at all satisfied	13	13%
Neither Satisfied nor dissatisfied	7	7%
Total	100	100%

Graph No. 8



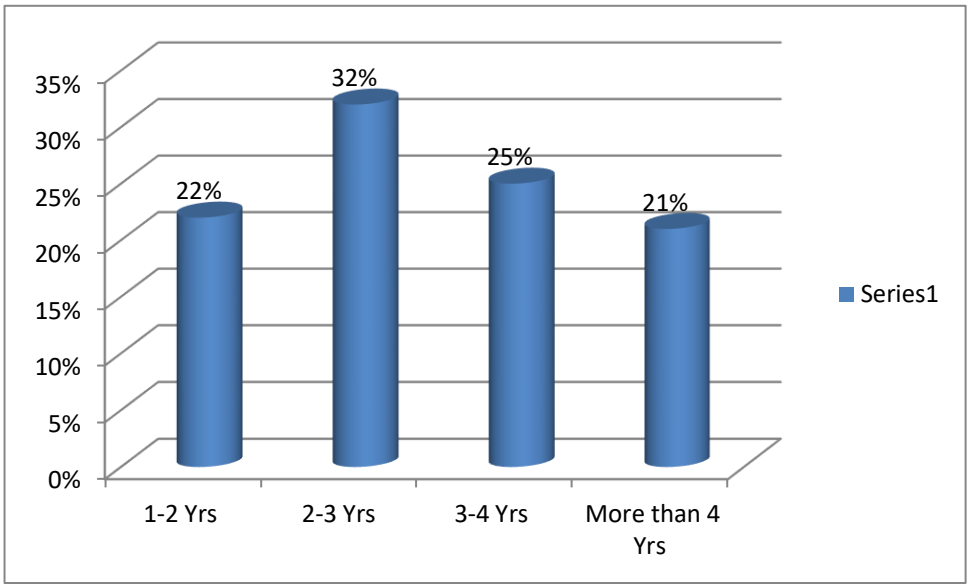
Interpretation: The above graph shows that 65% of respondents satisfied with Biometric System in Government Offices Products. Only 15% of respondents dissatisfied with its products.

9. How many years have you been using Biometric System in Government Offices?

Table No.9:

Years	**No. of Respondent**	**Percentage**
1-2 Yrs	22	22%
2-3 Yrs	32	32%
3-4 Yrs	25	25%
More than 4 Yrs	21	21%
Total	100	100%

Graph No.9:



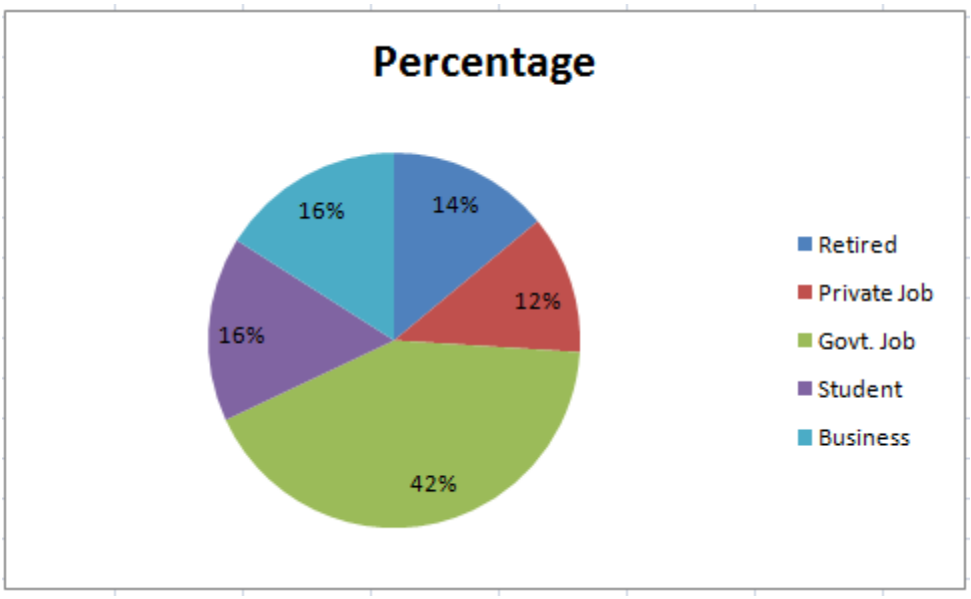
Interpretation: In the above graph shows that 22% of people using Biometric System in Government Offices 1-2 years, 32% respondents using 2-3 years, 25% respondents using for 3-4 years and rest 21% respondents using More than 4 years.

10. Distribution of Respondents According to Occupation

Table No. 10

OCCUPATION	**RESPONDENTS**	**PERCENTAGE**
RETIRED	14	14%
PRIVATE JOB	12	12%
GOVT JOB	42	42%
STUDENT	16	16%
BUSINESS	16	16%
TOTAL	100	100

Graph No. 10



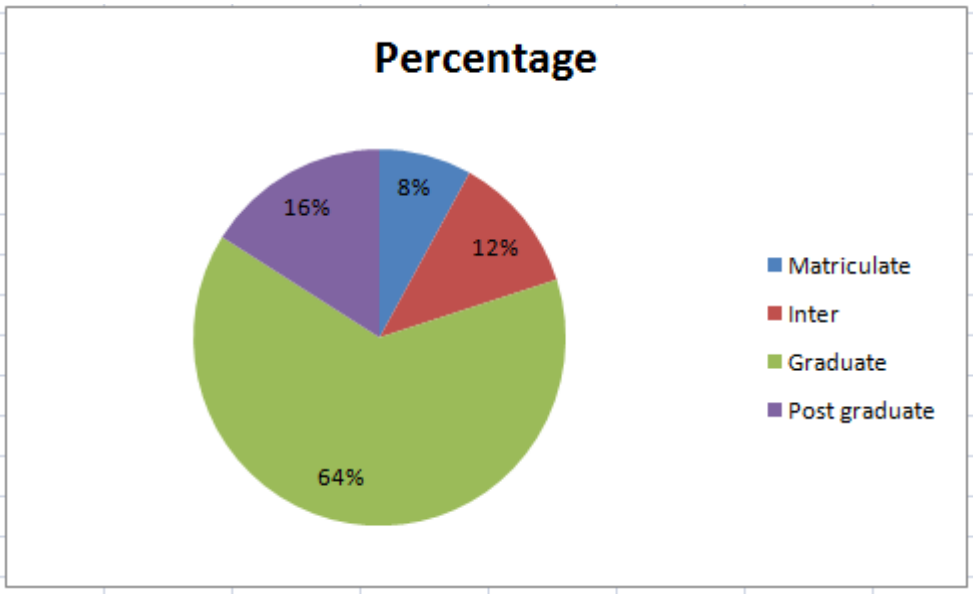
Interpretation : Out of 100 respondents 14% were retired,12% were private job holders, 42% were government job officials, 16% were students and 16% were businessman.

11. Distribution Of Respondents According To Qualification

Table No. 11

QUALIFICATION	RESPONDENTS	PERCENTAGE
MATRICULATE	8	8%
INTER	12	12%
GRADUATE	64	64%
POST GRADUATE	16	16%
TOTAL	100	100%

Graph No. 11



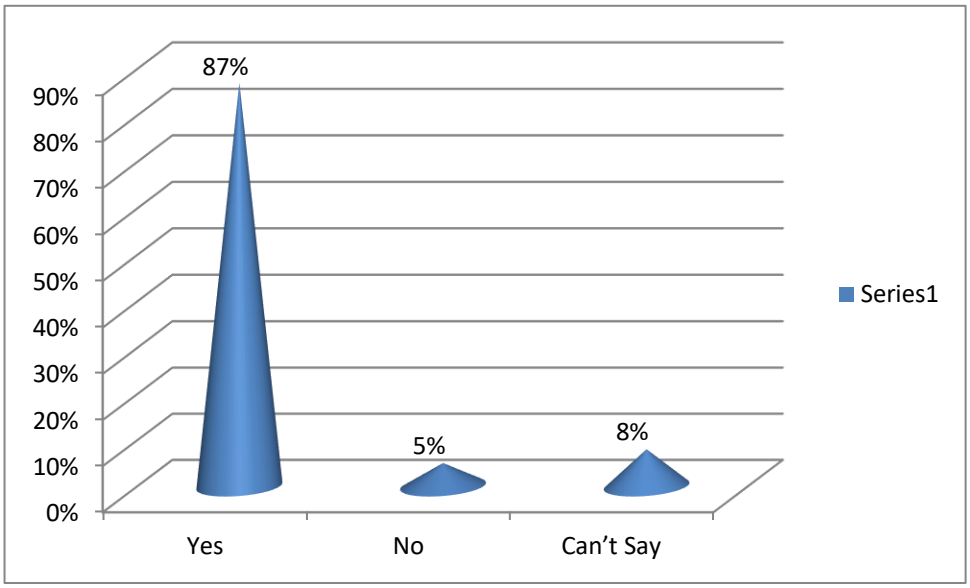
Interpretaion : Out of 100 respondents, 8% were matriculate, 12% were intermediate, 64% were graduate and 16% were post graduate.

12. Does Advertisement Influence your decision in choosing Biometric System in Government Offices Products?

Table No. 12

	No. of Respondents	**Percentage**
Yes	87	87%
No	5	5%
Can't Say	8	8%
Total	100	100%

Graph No. 12



Interpretation: In the above graph shows that 87% of customer says yes advertisement influence decision in choosing a Biometric System in Government Offices.

Chapter-4
Summary and Conclusions

Findings

1. It reveals that most of the employee approx 56% of employee working less than 3 years in the Government Offices.

2. It reveals that 26% of employee feel excellent the working environment, 48% feel good and rest 26% feel satisfactory.

1. It reveals that 33% of the respondents came to know of Biometric System in Government Offices through TV ads, 24% of the respondents through magazines, 21% of the respondents through the existing customers and 12% of respondents from friends, 10% of respondents through internet. The above graph explained that majority of respondents are TV ads and Magazines.

2. It reveals that good perception comes from 45%, 25% have ordinary perception about the Biometric System in Government Offices and rest by 25% have No Comment, 5% have poor perception.

3. It is observed that 35% of respondents strongly agree Biometric System in Government Offices have Good Quality, 45% agree, 15% Neither agree and 5% of respondents disagree.

4. It reveals that 35% of people says excellent about selling scale system of Asian Paints, 25% Good, 16% Fair, 12% Poor and rest 12% says very poor.

5. It is observed that Biometric System in Government Offices are economical. 15% of public is extremely agreed with this statement, 20% is highly agreed, 45% is agreed and rest of peoples answer is negative.

6. It reveals that 65% of respondents says Biometric System in Government Offices are more quality and beneficial than others. Only 35% of respondents Says No.

7. It is observed that 65% of respondents satisfied with Biometric System in Government Offices Products. Only 15% of respondents dissatisfied with its products.

8. It reveals that 87% of customer says yes advertisement influence decision in choosing a Biometric System in Government Offices.

LIMITATIONS

As I was asked to carry on my project training, I found the following limitations during my training period. So, it was very difficult for me to collect all the relevant information regarding my project report.

1. Shortage of time factor was one of the biggest constraints.
2. More stress was faced during collection of primary data through questionnaires and also to collect secondary data from the organization in terms of organizational profile, product and Services.
3. Due to time constraint, a large number of respondents could not be selected for the study and few of the respondents selected did not disclose any information since they felt it was a confidential.
4. Employees were reluctant to give sufficient information for the study.

CONCLUSION

A study was undertaken to investigate government employees' perceptions of factors relating to the introduction of biometric authentication at the workplace. This was undertaken to determine how best to gain employees' acceptance of biometric in order to successfully adopt biometrics in e-government applications. Results supported a number of findings reported in literature regarding user acceptance and adoption of biometrics and e-government technology. Analysis of results shows that an awareness and orientation process about biometrics should take place before the technology is introduced into the organisation. This is highlighted as all managers expressed employees' resistance to the technology's installation at the beginning of its implementation. The employees should be made aware about the use of the new technology, the purpose of its implementation and the benefits. Since about half of the managers had not considered their responsibilities for narrowing the digital and cultural gap regarding the fingerprint technology, it is recommended that managers should be made aware of their responsibilities in this issue. They should recognize that digital and cultural gap in technological awareness exists and that they have to act as leaders and role models for their employees. Finally, as the managers have a big part of the responsibility to successfully implement biometric technology in their organisations, they need to gain a detailed understanding of this technology and preferably have a basic background about Information Technology as well.

ANNEXURE:

BIBLIOGRAPHY

WEBSITES:

- http://www.exlservice.com/locations/
- http://ir.exlservice.com/events.cfm
- https://en.wikipedia.org/wiki/EXL
- http://www.exlindia.com/
- http://asq.org/learn-about-quality/total-quality management/overview/overview.html
- https://www.ukessays.com/dissertation/examples/information-systems/advantages-and-disadvantages-of-biometrics.php
- http://www.biometricsinstitute.org/pages/types-of-biometrics.html
- http://www.biometric-security-devices.com/types-of-biometric-devices.html
- https://en.wikipedia.org/wiki/Perception_management
- https://en.wikipedia.org/wiki/Biometrics
- https://www.researchgate.net/publication/47398070_Employees'_Perceptions_of_Biometric_Technology_Adoption_in_E-Government_An_Exploratory_Study_in_the_Kingdom_of_Saudi_Arabia
- http://www.irma-international.org/viewtitle/41932/
- http://www.tsijournals.com/articles/exploring-employees-perceptions-of-biometric-technology-adoption-in-hotels.pdf
- http://www.tsijournals.com/abstract/exploring-employees-perceptions-of-biometric-technology-adoption-in-hotels-9328.html

QUESTIONNAIRE

NAME : ……

AGE : ……

CONTACT NO. ……

SPECIALIZATION : ……

1. How long you have been working in the Government Offices?

a) less than 3 b) 3-5 years c) more than 5 years

2. How do you feel the working environment?

a) Excellent b) good c)satisfactory

3. What is your Perception about Biometric System in Government Offices Products?

a) Good b) Ordinary

c) No Comments d) Poor

4. Biometric System in Government Offices Products has Good Quality?

a) Strongly agree b) Agree

c) Neither agree d) Disagree

5. Do you think Biometric System in Government Offices products are more Quality & beneficial than others?

a) Yes b) No

6.: On the basis of price and feature comparison, is Biometric System in Government Offices Products economical?

a) Extremely Agreed b) Highly agreed

c) Agreed d) No Comment e) Disagreed

7. What is the selling scale System of Biometric System in Government Offices Products?

a) Excellent b) Good c) Fair

d) Poor e) Very poor

8. State the level of satisfaction for the Biometric System in Government Offices Products?

a) Satisfied b) Dissatisfied

c) Not al all satisfied d) neither satisfied nor dissatisfied

9. How many years have you been using Biometric System in Government Offices Products?

a) 1-2 Yrs b) 2-3 Yrs.

c) 3-4 Yrs d) More Than 4 Yrs

10. Distribution of Respondents According to Occupation

a) Retired b) Private Job

c) Govt. Job d) Student

11. Distribution of Respondents According To Qualification

a) Matriculate b) Inter

c) Graduate d) Post Graduate

12. Does Advertisement Influence your decision in choosing a Biometric System in Government Offices Products?

a) Yes b) No c) Can't Say

13. Any Suggestions?

……