CHAPTER I

INTRODUCTION

1.1 Basic Introduction

The major factor in the growth of Indian organizations is Information Technology. With the day-by-day improvement of information technology, the organizations are viewing positive as well as negative impacts. By introducing information technology, we can manage the information related to employees, like personal, professional or official in a systematic way.

With this systematic method of data storage and retrieval, it is noticed that there are many problems which are persisting. As the people have started increasing their knowledge in IT sector, hacking and sending or running malicious codes on the servers and system where the data is stored is also increasing.

Security of the various assets has emerged as a critical issue for any organization. The lapse in security like unauthorised personnel gaining access to critical asset can be very harmful to the organizational growth.

To avoid such kind of IT related problems and to allow only the authentic people to access the information in the system, so that it does not reach in wrong hands. The organizations are required to have an absolute trust in the identity of their employees, customers, contractors and partners; that is, that they are really who they say they are. Here we need to understand the concept of “Authentication”.

1.2 Authentication

Authentication is the method used to identify the users by the system. Authentication system gives answers to the following questions:

- Who is the user?
- Is the user really a person representing himself/ herself to be?
An authentication system can be password protected system or it can be a system using Smart cards. In all such systems, authentication depends on each information known to the employee identified and security system. This is also called as a shared secret.

This can be:

- a classical password,
- smart card system.

In order to authenticate a user, system asks user to provide his exclusive information.

If it is verified then the user is authenticated.

We can define authentication as a process of confirming that this is the same person as he is saying. To have a better understanding, let’s take an example. If I say I am Mr. X, authentication confirms this by some tests that I am actually Mr. X.

If we want a better understanding of authentication, we will have to start from the olden days when we did not have any technical devices.

Let us consider this situation; Mr. X and Mr. Y are friends. Mr. Y calls Mr. X and Mr. X identifies that this call is from Mr. Y. How does this happen? The reason is Mr. X identifies Mr. Y by his face, colour of his eyes, some special body feature, and voice or even by smell.

So, we can say that we can identify our friends by face, colour of eyes, skin colour, some special feature, voice or smell. All these things about a person are already stored in our brain. When we see or feel or listen to any of them, we try and match it with the pre-stored detail and then identify the person or in other words “authenticate” him/her as a particular person.

Now in case of friends, this approach is perfectly correct as we will have a limited number of friends and we will be in regular touch with them. When this concept is stretched to the organizational level, where there are thousands of employees who are not in touch with each other on a regular basis, then the above described approach is not possible.
If it is small organization, for example an owner driven organization with 20-25 employees, the owner can still remember the names of all the employees and recognize them individually. This will help the owner keep a check on the employees as to who has come, who is on leave, who came late and who left early. All this can be done mentally by him.

But when it comes to a very big organization which has more than 100 employees or which is stretched in a very large geographic area, then keeping in mind the details of every employee becomes very difficult and then management of their time and attendance becomes impossible. The problem of security breach, wrong time in and time out and incorrect attendance increases tremendously.

Any organization cannot grow and earn profit by giving so much leverage to some employees and keep stringent rules for others. Keeping a proper check on the employees as far as time and attendance is concerned gives organization new avenues for growth.

Also, to keep other employees who are putting in extra efforts toward their targets and work needs to be motivated on the regular basis so that they continue the good work and finally earn more and more profits for the organization.

Now, if the employee who is putting in his 100% for the organization and another employees who is bunking the organization or who is irregular or who is insincere, are given equal appraisals then naturally the first employee who is hard working and sincere will get de motivated and as a result his performance will be affected negatively.

So, the top management needs to keep a check on all the employees and make sure that the deserving employees should be properly benefited. For this they need to know the details of all their employees and for knowing the details, they need to properly identify or in proper technical terms authenticate the employees.
To solve this problem on the organizational level, identification of people is done using identification cards (I-Cards). I-card was provided to every individual who is working with the organization which contains the recent photograph of the card holder, his name, employee-id and designation, looking at which we can authenticate that person is working in the organization.

For solving the problem of authentication of the people in the large organizations, the concept of identification card was introduced.

In this concept, all the employees are provided with a card which contain the employees name, latest photograph, employee identification number (can be numeric or alphanumeric), his or her designation, etc.

So, this I-card was used for the employee identification and was used for authenticating him. Along with this, a register was maintained to note the time and attendance of the employee. The employee himself filled what time he came in the organization and what time he left, which all days he has come and when he has taken leaves and that too of which type, whether it is a CL, PL, Sick leave or any other.

In this case, the organization is showing complete faith on the employees and allows him to fill in the time and attendance details.

But the HR of the organization found that the employees are very smart. They give their I-Cards to their colleagues or friends and tell him to sign the attendance book and enter the time.

This approach also has a problem that the I-card could be stolen or exchanged among the friends working in the company. This could also be a way of playing with the authentication.

So, this approach of maintaining the employee details failed. With the development in the technology, the I-cards were replaced by the smart cards.
What is a smart card?

A smart card is a card with a silicon chip inbuilt in it. It is a pocket sized card and it has a microchip placed in it which holds all the details of the card holder like the employee’s identification number and other details.

In order to use this smart card for time check, attendance check and security check, the entry and exit doors need to be kept fixed and common. A mechanism needs to be installed on the door which reads the card and matches the details with the details already stored in the company’s database. If the details matched, like his time-in, attendance are noted and the door are opened then he is allowed to enter in to the office. Otherwise the employee is not allowed.

This card is a better option than password as the person will have to carry it and once it is accepted then only he will be allowed to enter but there are some major flaws with this approach:

- if the person/employee forgets the card, then his entry will be restricted and time and attendance will not be noted. The organization will need a person for the manual entry in such a case.
- If the card gets stolen, other person who is not supposed to enter in a particular secured area will get entry/access to that area.
- This card could be easily shared amongst the employees for misuse like false time and attendance entry. Misguiding the organization.

It is very good approach for maintaining the organizational security and managing the time and attendance automatically but the flaws or problems with this approach are many more than its actual advantages.
For solving this problem, the concept of smart card has been introduced, which contained the Identification number in the chip and the employee details as well. Whenever employee tries to enter into the organization, he first has to swipe the card, if the identification number in the card is matched with the previously stored number then only he/she is allowed to enter in the organization else the doors do not open. This system of card swipe is attached with the opening and closing of the door. But this could also be stolen or exchanged or shared amongst the employees for misuse. And also, the biggest flaw with this system is that even if no cheating is done by the employee but he really forgets the card at home then also he will not be allowed to enter the organization and even if he enters, his attendance is not marked. As this system helps in opening the doors and that it also helps the organizational administration to automatically maintain the attendance.

To resolve all the problems discussed, the new concept has been introduced. This concept is Biometrics. This resolves all the problems up to a large extent. In this approach, a person need not remember his password or even eavesdropping of password cannot be done as in the case of the password protection it was there. Employee does not need to carry the identity card along with him all the time. He need not carry the swipe card all the time. If he forgets the card, either he is not allowed to enter in the organization or if he enters somehow then his attendance is not marked. Also the problem of buddy punching was sorted out up to a large extent.

The organizations could not completely rely on this approach as far as security and bring in more strictness, a new approach is introduced. In order to understand this new concept we will have to discuss authentication in detail.
There are basically three ways to authenticate a person.

1.2.1 Providing the person with the unique user name and his own defined password.

Something that you “know” – e.g., PIN or Password

In this approach, the organization gives a user name and password to each employee. The user can enter in to the system or the organizational database only by putting in the password, like we do in case of E-mail systems.

This password can also be called as a PIN. That is the Personal Identification Number.

It can be an alphanumeric value with some special characters included in it.

The organizations can fix the length of the password/ PIN to say 7-8 characters or can define the minimum acceptance digits of passwords/PIN as 4 characters, etc.

This password would be associated with the username and would not be disclosed to anyone by the system.

But there are many disadvantages associated with this method:

a) This approach is weak and prone to a number of attacks.

There can be n number of ways to actually identify the passwords and enter in to the system. There are different types of software available to help hack the passwords and enter in to the system. That is why this approach is very prone to the attacks.

b) The security depends upon how the user maintains his user ID and password secret.

As a human being, we can be ill or be away from the work for some professional or personal commitments. There can be some urgent requirements of some data kept in that employee’s system which is required by the top management urgently for some policy decision making.
Naturally, the employee will have to share his password with another employee working in the same organization. Now, once the password is out, it can be very easily misused.

So, in other words, maintenance of secrecy sometimes becomes a major issue with the people.

c) The password can be easily hacked and security can be breached easily.

Always at the work place, there will be employees or people with a notorious mind and these kinds of people are generally problem creaters.

The people can only for fun, hack the passwords of the employee and enter in his system and create problems.

This can be done only for fun or can be done with a very wrong intention so as to create problems in the organizational work or with intend to degrade a particular employee.

This type of attack can be directly on the management or in order to stop or tamper with the growth of the organization or it can be done in order to harass some employee.

This concept of providing password can be easily hacked and the security can be easily breached.

Because of these major disadvantages, this method of security is not very much used by the organizations.
1.2.2 **Using Security Token which may be Hardware tokens i.e. Smart Cards or Software Tokens or Out-of-Band Authentication.**

Something that you “have” – e.g., Key, Magnetic Card or Smart card

In this case person needs to physically have something like a magnetic card or a smart card, using which; they can get access to a secured area.

So, a security Token is a physical device provided to any authorised user to ease the authentication. They help in proving the employee’s identity electronically.

Now, these tokens will be holding some code which will help the person owning the card gets access to that secured area. Once this card gets misplaced, whoever receives the card automatically gets authority to enter the secured area.

So, in such cases, security breach is very easy and obvious.

They can be smart cards which can store cryptographic keys like digital signatures or special designs which may include USB connector, RFID functions or Bluetooth.

But even these methods have a number of flaws and security breach is easily possible. For example:

a) **Hardware Tokens :**

It can be a card which when swiped through the machine (card swiping machine) gives the access to the secured area, or entry in the organization.

A small hardware device that is carried by the owner using which he/she can authorize access to a particular network service is called as a security token or an authentication token. This hardware token can be a smart card or it can be embedded in any object such as a key fob. This is a better approach to authenticate a person then just using a password because it is a two-factor authentication. In this, the person who is seeking the authentication has a personal identification number (PIN). This PIN authorizes the person to be the owner of that particular device. Once the PIN is entered, the device displays a number which uniquely
identifies the user to the service and gives him the permission to log in to the system.

The properties of such hardware tokens are as mentioned below:

i) Involves additional costs (Token etc.)

The flaw this approach has is that the end user needs to carry the token. This token needs to be provided to every employee working in the organization so that he/she can be authenticated. This involves an additional cost to the organization.

ii) User needs to carry the token along with him

Every time the user wants to enter into the organization, he/she needs to carry the token with him/her. Suppose he forgets the token at home, his attendance will not be accounted or he will not be authenticated to enter into the reserved area.

iii) Different tokens needed for different devices

Till now a common token for all the devices is not created. Every device used in the organization needs a different token. So, in a way it is an extra cost to the organization.

iv) It does not protect fully from Man-In-Middle attack.

b) Software Tokens

A software token is a type of two-factor authentication. In the two-factor authentication, the person who is seeking the authentication has a personal identification number (PIN). This PIN authorizes the person to be the owner of that particular device. Once the PIN is entered, the device displays a number which uniquely identifies the user to the service and gives him the permission to log in to the system. The Software tokens are stored on any electronic device such as a computer, laptop, PDA, or mobile phone. This can be easily duplicated.

The software tokens are physically not in possession of anyone that is the reason they are exposed to unique threats like computer viruses and software attacks. The
software tokens are also vulnerable to man-in-the-middle attacks, or simple phishing attacks. For resolving the problems of phishing attacks, the one-time password is provided and supplied to the genuine website in a timely manner.

Benefits of Software tokens:

i) there is no physical token to carry

ii) they do not contain batteries that will run out

iii) they are cheaper than hardware tokens.

Drawbacks of Software tokens:

i) Requires user training

i) Needs a controlled environment for deployment

ii) If any problem occurs then it needs to be reinstalled or configured.

iii) Needs a proper protected environment

1.2.3 Using Biometrics

Something that you “are” - like iris, fingerprints, voice, face, etc.

The biometric identification is used for authenticating a person to identify the individuals or to provide access rights to the correct authenticated person. There are two types of biometric identifiers:

a) Behavioural

b) Physiological
a) Behavioural: In this type of biometric identification, we read the person’s behavioural traits. Or in other words, the traits are related to the pattern of a person’s behaviour like his speed of typing or his voice.

b) Physiological: In this type of biometric identification, we read the person’s shape of body. For example the finger prints, hand geometry, palm prints, iris recognition, face recognition etc.

Properties of the biometrics system are as mentioned below:

i) The high-security systems and sites can be accesses in a secured way.

ii) As the biometric factors are specific to the problems of users, non-repudiation problem can be solved.

iii) Various authentication methods can be used like fingerprint, iris or retina scanner

iv) Compromising is difficult.

Now, once a person is authenticated and allowed to enter into the organization, he also can access the records of the organization. When the records were maintained on the manual basis, there was a security guard outside the data storage space/ room, which first authenticated the user and then allowed to enter the room and this person, had some authority to view some documents and not to view some others.
1.3 Authorization

A process that helps in determining the levels of entrance an employee should have to the protected assets of any organization. For example, DBMS can be designed giving various access rights to the authenticated users so that some have the ability to retrieve information but cannot change the data and some have rights to make changes as well. Various views of databases are generated and some levels are created. Different levels have access to different views.

Some employees can just read the database some can update and read the database, and some can update, read and execute various procedures and triggers.

These kinds of rights are possible only if we can give proper authorization to the proper employees. Different employees will have different authorizations. This can be differentiated if we give different username and password to the different employees.

In case of giving password protection again the same problems will be faced like eavesdropping and exchange of password as a result exchange of authorities.

Another approach was use of swipe card which can also have the various problems like buddy punching, theft, unauthorised access etc. So, again we boil down to the biometrics. It will be the best possible option which will be well secured and easily applicable.

Authorization systems provide answers to the questions:

- Is the authenticated user authorized to access resource R1?
- Is the authenticated user authorized to perform operation O?
- Is the authenticated user authorized to perform operation O on resource R1?

Authentication and authorization are closely connected methods. There is a dependency of the authorization systems authentication systems so that the identity of the users is proved and the unauthorised users are prevented from gaining access to the secured resources.
1.4 Information Security in organizations

The today’s organizations major concern is how to manage their data and resources so that data security is maintained. Information is one of the most important resources for business and organizations and its management is a key challenge. That is why data security is very important in the organizations. The need for controlling and protecting information is because of its value. This information helps in good decision making by the higher levels managements (Marschak 1968).

The organizations must be able to handle and administer the information in a secured and safe manner. "Prior to the introduction of computers in the corporate world, business would store its information in locking file cabinets. This is now on the computer system for easy access and use by authorized users. The value of that information to a company has not changed since it was taken out of the file cabinets and put on the computer system therefore the security concerns for that information should not have changed" (Hendershot 1993). The data security is very important to the organizations, if it is not taken care of, the organizational data can be vulnerable to threats.

The various types of threats that can be possible on our data are:

1. Theft. If the intangible assets like data and software are taken away from the organization without permission.

   This can be done by the employees of the organization or the security guards or some person who has personal rivalry with the organization or the management.

2. Fraud. If the assets of organizations are taken away keeping all the records look as they were.

   The person who does this is very smart in his work. He will do the fraud in such a way that all the records looks as if no change has occurred. Everything remains consistent and normal.
3. Malicious Damage. Throwing malicious codes on the organizational systems.

This is actually done by some notorious people who have some issues with the organization. They can be a current employee or some ex-employee. Any type of malicious code can be used like – virus, worms, trapdoors or zombies.

4. Incompetence and Mistakes. Users do mistakes due to carelessness or unawareness.

Proper training of the system is not given to the employees and that creates a lot of problems. The users do a number of mistakes. These mistakes can be caused due to either unawareness or they are careless and are not serious enough to understand the problems that can be faced by the organizations.

5. Accidents and Disasters. Data loss due to accidents or natural disasters.

The organizational data can be lost due to some kind of accidents like there can be something like a short circuit and this causes fire and as a result all the data is lost. Also there can be some natural disaster. Like there can be floods or earthquakes and as a result the complete organizational data can be lost.

Out of the above mentioned threats, the first three threats: Theft, Fraud and Malicious Damage can be done by either unauthorized entry in organization and unauthorised access of the data. The organizations need to put a proper check on the entry and exit of the employees and need to authenticate them to access the particular data and use it or access it. If proper authentication is done then the above threats can be taken care of in a much better manner.

The use of biometrics can be the best solution to all the above problems. Access control solutions are a key component of physical security systems, and companies (particularly those that deal in sensitive data and other material) are always trying to find ways to improve identity authentication. Biometrics solutions that utilize fingerprint, iris scan, or facial recognition data for that authentication, used to be a niche technology offered in
high-end private sector and government applications. Research firm TechNavio expects the global biometrics market to reach more than $9B by 2014, driven by both physical and cyber security concerns. So we can very well understand the growing need of biometric systems in the organizations. Let us now understand the complete process that is required in biometrics.

1.5 Biometrics Processes

The biometric processes can be understood in order to secure the organizational data. Once the people are able to understand the biometric processes, they will be able to secure their organizational data from various problems. The biometric processes can be briefed in the following manner:

It is actually a four step process which when followed in a proper manner, security and discipline of the organization can be improved to a large extent.

Enrol: The first step is to enrol an employee also called as an Enrolment process. In this process, we take a number of measurements from the employee’s body parts and accordingly create templates. Once a template is formed, it is stored in the database. This database will contain all the templates with respect to the individual employees.

This process of creating the template is called as Scanning.

In scanning, the respective body part is scanned and measured. Multiple scanning is done and processed and the best output is generated. It is stored as of template. This is the method of generating the template and storing it in the database for further use.

The process described above is the process used to form a proper database of all the employees. Once it is formed, we have the data ready with us. Now whenever an employee wants to enter the organization or any secured place, a process is followed and it is checked whether this employee is allowed to enter the desired place or not. This is called Verification.
**Verification:** This is the daily process which could be done to check whether the person entering the organization is actually the same person as he says he is. For this purpose, a sample of required body part is taken and a temporary template is formed. Once this is done, this temporary template T1 is matched with the pre stored template TP. If it matches, the person is verified and thus allowed to enter into the organization. Biometric verification uses the person’s ID and physiological and behavioural aspects of the person for his authentication. The identity of the person is already declared by him either using user name-password or a smart card. Biometrics works for completing the authentication process. Database is used to keep the record of all the valid identifications of the employees as a primary key and the corresponding templates of the employee. Then a comparison is done between the previously stored templates and the actual biometrics. The result of this process is either accept or reject of the templates.

**Identification:** Biometric identification is completely based up on body parts. The identification and authentication both are served by biometrics. The database used here contains enrolled templates. These templates are then compared with the provided biometric details. If the match is found then authentication is complete and then the employee is allowed to enter the restricted area.

A biometric identification can operate either in +ve identification mode or -ve identification mode.

Positive identification: If the read biometric is there in the database and there is a single match to positively identify that person then it is called as positive identification.

Negative identification: In this case reverse is done. It checks if the provided template is not in the database. If it is not there in the database then the user is allowed to enter the restricted area.
**Enrolment**: Enrolment means entering the employee’s biometrics in the biometric system. This is also of two types:

Positive enrolment: This results in a database containing biometric templates of the employees. These are used for employees’ identification or verification.

Negative enrolment: contains the records of the blacklisted employees.

**Matching**: Biometric matching means the comparing the template of the enrolled person’s known biometric data from the database with the templates read at the time of identification or verification. The match cannot be 100% but a degree of likeness is calculated and if this degree is good then the match is accepted.
The complete process of Biometrics has been explained and understood that is will be beneficial for the security purposes and the management purposes. But the question is that Is this new Technology really required for the organization? Will this new technology gain profits for our organization? Will this added cost for implementation of this new technology be bearable?
1.6 Practicality of Biometrics

Roger Clarke proposed measures needed for a biometric system to be usable. Some to mention are the system or the biometrics devices should be:

- **Universality**: this means that all the people who would be using this system should possess that trait. For example, every person will have finger or for that matter iris so that fingerprint recognition or iris recognition can be done.

- **Uniqueness**: This means that the trait should be unique to the individuals so that they can be distinguished from one another.

- **Permanence**: This property refers to the variation of the trait over time. The one with good permanence will always be a better option.

- **Indispensable**: This property refers to the necessity of the trait and authenticity of that trait. If the trait is not found, access rights will not be provided.

- **Collectable**: This property refers to the convenience in collecting the traits from the human body. It should not be such that we are not able to collect the traits; in that case the authenticity check will not be able to be applied.

- **Storable**: this property refers to the storage of the traits. It should not be such that we face n number of problems in storing the traits that we have collected. The storage of the traits should be very easy and comfortable.

- **Measureable**: This means that the traits should be easily collectable and it refers to the property that the ease with which the trait can be measured or acquired.
• Performance: this is the details of the technology used, whether it is accurate, speedy and robust as far as its performance is concerned.

• Acceptability: This is whether people will be accepting this technology and whether the employees are ready to get their biometric traits captured and measured and assessed.

• Circumvention: This relates to property of any biometric trait to be imitated using a substitute or artefact. This is the measurement of ease with which this can be done.

• Exclusive: This property refers to the exclusiveness of the system for a particular organization. It should not be common for all the places it is installed.

• Precise and Simple: This refers to the property that the system that we are referring to should be very précised and very simple. It should not need any technical know how to operate the system. Any layman can work on it with ease and proficiency.

• Should not incur undue cost to the organization: This property says that this new system should not cost the organization too high. The cost benefit analysis should be done and we should check of incurring break even at earliest.

• Convenient to use and acceptable by the employees as well as the organizations: This is the most important point which says that the employees of the organization who are going to use this system should accept it readily and easily then only it can be a benefit to the organization.
1.7 Various Biometrics Approaches

There can be various approaches used for the biometric identification and verifications:

Types of Biometrics

1) DNA Matching

In this type of biometrics, a segment of a person’s DNA is taken and then, his identification is done on the basis of the same.

Figure 1.2: Figure showing the DNA Matching
Ear

This is a type of visual Biometrics in which the individual is identified using his ear's shape.

Figure 1.3: Figure showing the Ear Biometrics
Eyes - Iris Recognition

This is the type of visual Biometrics in which an individual is identified on the basis of the features found in their iris.

![Iris Recognition Biometrics Process](image)

**Figure 1.4:** Figure showing the Iris Recognition Biometrics
Eyes - Retina Recognition

In this type of visual Biometrics, the recognition is done using the patterns of veins at the back of the eye.

Figure 1.5: Figure showing the Retina Recognition Biometrics
Face Recognition

In this type of visual Biometrics, the individual’s identity is analysed on the basis of their facial features or patterns.

Figure 1.6: Figure showing the Face Recognition Biometrics
Fingerprint Recognition

In this type of visual Biometrics, in order to identify an individual, the ridges and valleys (minutiae) found on the human finger’s surface tips are measured.

Figure 1.7: Figure showing the Fingerprint Recognition Biometrics
Finger Geometry Recognition

In this type of visual/spatial Biometrics, the identity of the user is determined using 3D finger geometry.

Figure 1.8: Figure showing the Finger Geometry Biometrics
Gait Analysis

This is the type of behavioural Biometrics. Gait analysis is the systematic study of human motion. In this the eyes and the brain of observers are used. This process is improved by the measurement of body movements, body mechanics, and the muscle activities.

The main purpose of this type of analysis is to measure, map, and take care of the individuals with conditions which affect individuals walking ability. This method is also used by sportsmen, coaches etc. so that the athletes run more efficiently and also help to identify posture-related or movement-related problems in people with injuries. This comes under sports biomechanics.

Figure 1.9: Figure showing the Gait Biometrics
Hand Geometry Recognition

This is the type of visual/spatial Biometrics in which the hand’s geometric features (the lengths of fingers, width of the hand, etc.) help in the identification of any individual.

Figure 1.10: Figure showing the Hand Geometry Recognition Biometrics
Odour

It is also termed as Olfactory Biometrics. In this method, observer uses the odour of an individual to determine his/her identity. The work is still in progress on this and researchers are working on this technology so as to authenticate the individual in any place.

Figure 1.11: Figure showing the Odour Biometrics
Signature Recognition

This approach can be termed as visual/behavioural Biometrics. In this approach we are using the handwriting and in particular the person’s signature as a tool of authentication of any individual. The digital handwritten signature authentication is basically of two types:

a) Static: In the static authentication approach, the two scanned signatures are compared visually. There can also be a comparison done between the scanned signature and an ink signature. Comparison of the two signatures is done using advances algorithms.

b) Dynamic. The dynamic approach is more popularly used. In this case, the X,Y,T and P Coordinates of the signer are also captured along with the ceremony data using the sign device. This captured data can later be used as a digital forensic examination tool in the court. It can also be used to create a biometric template for authenticating dynamic signatures.

![Signature Recognition Diagram](image)

Figure 1.12: Figure showing the Signature Biometrics
Typing Recognition

It is the type of behavioural Biometrics. In this case, the unique characteristic of a person’s typing is used in order to establish his/her identity.

This keystroke dynamics based authentication helps to verify the user on the basis of their typing pattern. For this, a resemblance of a typing sample of user regardless of the text typed is found out, the key event timing is extracted from key features and along with that, the Latency, Dwell time, Key interval, Up to up, Flight time and standard are measure in the form of FAR, FRR and ER are measured.

Figure 1.13: Figure showing the typing Biometrics
Vein Recognition

In this type of recognition, vein pattern can be used to identify the individuals.

The finger vein recognition is used for authenticating the individuals, using the pattern-recognition techniques. The images of vein patterns of the human finger which are beneath the surface of the skin are used. In this, the vascular pattern in an individual's finger is matched with the previously stored data. This technology is currently used in the time and attendance tracking, automobile security, credit card authentication, computer and network authentication, end point security and ATMs etc.

The individual has to insert their finger into a device containing an infrared LED (light-emitting diode) light and a monochrome CCD (charge-coupled device) camera. The RBC (haemoglobin) of the blood absorbs the infrared LED light. With this light, the vein system appear as a dark pattern of lines. The camera then records the image, digitize it, certify it and send to the database of registered images. For authentication purposes, a comparison is done between the scanned finger and the pre stored data. This whole process takes less than 2sec time.

Blood vessel patterns are considered as they are unique to each individual. It is almost impossible to forge the blood vessel patterns as they are located beneath the skin's surface. The fingerprints based biometric systems can easily be fooled with a dummy finger fitted with a copied fingerprint; similarly, the voice and facial characteristic-based systems can also be forged by recordings and high-resolution images. But it is really difficult to forge the finger vein ID system as authentication using this method is done only of a living person.
Voice / Speaker Recognition

The speaker recognition can have two types of applications:

**Voice - Speaker Verification / Authentication**

This comes under the auditory Biometrics. In this type of biometrics, in order to authenticate the employee or to provide some kind of access control, voice is used.

The speaker is verified using voice. To authenticate a user as what he says is done using his voice, which is used to verify his claim. In this approach, a one to one match is done. This means one speaker's voice is matched to one template. This method is generally used as a "gatekeeper" to provide access to a secure system (e.g.: telephone banking).
We can work on such systems only with the knowledge and cooperation of the user. For example, presenting a student’s admit card during the exams is a verification process - the invigilator compares the person’s face to the picture in the admit card.

**Voice - Speaker Identification**

This type of authentication comes under the auditory Biometrics. In this type of biometrics, the unknown speaker’s identity is tried to be determined or in other words, identified.

The process of speaker identification can be described as a one to many matches. In this the acquired voice is compared against N number of pre-stored templates. This approach of authentication can easily be implemented without the knowledge of the user. It can be used to identify any talkers in a discussion, etc. The best example can be a CBI agent comparing an assailant’s sketch with a database of previously documented criminals in order to find the nearest match.
<table>
<thead>
<tr>
<th>Method</th>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
</table>
| Finger print Verification | • High Reliability  
                         | • Robust  
                         | • Highly Distinctive  
                         | • Proven Accuracy  
                         | • Advanced Technology  
                         | • User Convenience  
                         | • Uniqueness  
                         | • Stable over time |
|                      |                                          | • Injury can affect  
                         | • Dry skin can cause difficulties  
                         | • Poor environment |
| Hand Geometry        | • Small Template  
                         | • Unaffected by skin condition                    | • Size of Scanner  
                         | • Injury can affect  
                         | • Low Distinctiveness |
| Face Recognition     | • Efficient Process  
                         | • High Acceptance                                 | • Face change over time  
                         | • Can be manipulated by surgery  
                         | • Cannot be distinguish between twins  
                         | • Religious or Cultural inhibitions  
                         | • Poor environment |
| Iris Scanning        | • Uniqueness  
                         | • Robust  
                         | • Highly Distinctive  
                         | • Complex Processor  
                         | • High Cost  
                         | • Poor environment  
                         | • Relatively new technology  
                         | • Affected with diabetes |
| Voice Recognition    | • High level of user acceptance  
                         | • High Acceptance  
                         | • Low training requirement                       | • Voice and language change over time  
                         | • Easy to manipulate  
                         | • Low Accuracy  
                         | • Poor environment  
                         | • Flu or Throat infection |
| Signature Recognition| • High user acceptance  
                         | • Low training requirement                       | • Unstable over time  
                         | • Changes over time  
                         | • Low distinctiveness |
1.8 Properties of Biometric System

Looking at the requirements defined above, the research scholar feels that the biometric systems should have the following properties:

- **Accuracy:** This is the most important property of any biometric system. If it is not accurate it is of no use to the organization. A biometric system must be accurate.

- **Speed:** The biometric system should have a very good speed. There should be no delays and time wastages in the complete process. The system should not take a lot of time in collecting the templates, storing, comparing and in giving the results.

- **Scalability:** Biometric verification systems should be more scalable than biometric identification systems as one to-one matching is needed

- **Strong exception handling:** A biometric system should handle exceptions in a very strong way. Exception handling is the place where it would be the biggest test for any biometric system. If the system is able to handle the exception properly, this means we win.

- **Cost:** Biometric System should be cost effective to the organization. Before implementing any new system, the organizations always does a cost and benefit analysis and check whether this new system is suitable for the organization or not. If we will get the break even early or not. So all these kinds of checks should be applied and it should be thoroughly verified that the new system is not putting a lot of extra cost to the organization.

- **Privacy:** The biometric systems should be able to maintain privacy of the organizational data and employees’ personal data. All the information should not be disclosed to each employee. There should be various views or levels of abstraction.
1.9 Is Biometric Attendance Verification and Biometric data security correct for the Organizations?

There can be various factors which can help us determine whether the verification of attendance and data security is required for organization or not. It can be a three step procedure:

Step I: It is determined if the biometrics system is required in the organization.

Step II: The possible Return on Investment (ROI) is considered. It is checked in details, if the organization is going to gain anything after investing in the installation of this new system and that too in how much time. That means when will be the breakeven for this new installation.

Step III: It is confirmed, if organizational environment is physically suitable for biometric security system, and that employees are ready to accept this change and the latest technology.

STEP I) Evaluate the need for authentication or identification. The first thing that comes to anyone’s mind is what kind of organization needs Biometric systems?

Generally, two types of organizations need the use of biometric systems:

i) Organization where employees plays with the incoming and outgoing time. That is the place where problems like buddy punching is existing.

ii) Organizations where there is a need for controlling people’s access at various areas of the building due to security concerns.

The organizations where the hourly workers are not there or where data security is not required do not need biometric system.
STEP 2) Consider the cost/benefit ratio. If an organization needs biometric system, the cost has to be considered. For some organizations, installation can be costlier compared to thefts.

The days of time clocks and handwritten timecards are over. Now the employees time transactions can be recorded in better, smarter, easier way and secure their data in a better way. With the new technologies for tracking time of the employees and the data collection devices, organizations can

- Control labor costs
- Minimize compliance
- Improve workforce productivity

STEP III): Is the biometric technology compatible with the organizations work environment?

The readings of the devices need to be very accurate. The working environment should be supportive for the biometric sensors, and then only employees’ biometric characteristics can be read properly.

Like an environment with lot of humidity and dirt cannot be suitable for finger reader or a noisy environment cannot be suitable for the voice data system. The proper functioning of the biometric devices, full co-operation from the employees is equally required.

We should accept this fact that in all the places where biometric systems are installed, some employees will not be able to use it. It is always suggested that the system should have an alternate communication methods like PIN.

Be sensitive to employees concerns. Whenever an organization has to implement a change, employees’ readiness and concerns need to be taken into consideration. This is the reason why, when biometric system is implemented, it is important to address the privacy concerns of the employees.

The employees should be convinced that no misuse of their templates will be done. The templates would be used only for authentication within the organization.
Also, it should be made clear to the employee that with the use of this system, their privacy will be enhanced.

For implementation of Biometric System, the management has to convince the employees that there will be no health impacts. Some antibacterial materials are also being developed for the biometric system.

Basically biometric processes are used in the organizations purely for two major purposes:

a) Attendance of the Employees to put a check on their productivity.

b) Security of all type of Employees data. (Personal or Professional)

### 1.10 Organizational Development

**Organization development (OD)** can be defined as an effort to increase an organization’s importance and feasibility. OD has also been defined as the readiness of the organizations and the employees to meet change. Thus a systemic strategy of gaining knowledge and maturity with intend to change the structure of the organization for the absorption of new technologies changing openings is OD.

Organizational Development (OD) provides designed, smooth processing, leadership-driven, across the association’s services in order to increase the efficiency, effectiveness and the organization’s health. Trained helpers assist in the organizational change, labour force planning, continuous improvement of the quality, and the conflicts resolution through self-assessment, organization diagnosis, proper planning and feedback processes. The important parts of any healthy organization includes open communication, trustworthiness amongst employees, employee’s involvement, and a proper decision-making. These services help to manage and link training, budgetary resources, and organizational structure with a path forward.

For the development of the organization, it is basically needed that the employees working in the organization should maintain the integrity and the security of the organization. If the employees are not coming to the organization in their stipulated time and they are not attending the organization with regularity then it may hamper the development of the organization. Even the problem of security is aggravated in this case as employees’ use
Biometric Processes Vis-a-Vis Organizational Development
Potentials

fraudulent means like buddy punching or false signature which leads to the breach of
security and integrity.

1.11 How Employees with Poor Attendance Affect the Workplace

Habitually absent employees become a burden on the company and the rest of the staff.
They actually become a financial burden due to a drop in productivity caused by their
absence and the cost of bringing in a temporary replacement. Also the extra work handed
to other staff members can impact employees’ morale. If we are able to identify the impact
of employees with poor attendance in the workplace we will be able to encourage
developing and enforcing strict guidelines.

Continuity

The frequent absence of the employees from the job prevent a work group from
developing productive continuity. Rather than having every employee doing his job during
regular work hours, the team must adjust to certain employees not being at their stations.
The constant flow of temporary replacements due to employee absenteeism makes it
extremely difficult for a manager and staff to determine the skill set of an absent
employee, and how that employee fits into the work flow of the group.

Diminished Performance

The other employees’ performance can get affected by the employees who are allowed to
continue with a large number of absences without any apparent penalty from management.
The employees see the concessions the employer is making to retain chronically absent
employees, and the others feel they also can exploit the system. It creates a cycle that leads
to low productivity, poor employee morale and a high turnover rate.
Growth

An employee is recruited looking at their academic background and industry working expertise. These things help them to learn and perform duties required by the organization for growth. The employer expects the employee to develop professionally as the organization grows. When that employee has poor attendance, it becomes difficult for them to become experienced in their area of work and offers no value addition to the company in order to achieve their growth objectives.

Conflict

Those staff members who are requested to cover for employees with poor attendance in due course start to have hard feelings about the chronic absenteeism. In course of time, this frustration can result in open conflict between staff members. The tension created by pending confrontation, or in the wake of past conflicts, an uncomfortable work environment is created which in turn causes slow productivity and excessive turnover.

The management of attendance in any organization is very crucial. The non-attendance cost is not just the direct payment of money and profits but also the indirect costs of recruitment, setting up, re-training, loss in the output, reduced morals, etc. Generally, the indirect cost goes beyond the direct cost of absence.

The management of attendance supports in profits, productivity and morale of the employees of the organizations.
1.12 Definition of Absenteeism

Absenteeism can be defined as the absence of employees from work in their defined or stipulated time. Employees away from work on approved leaves will not be included.

Voluntary absence from the work place without any valid reason. Absenteeism means either habitual avoidance of work, or wilful absence as in a strike action. Absenteeism does not include involuntary or occasional absence because of any valid causes/reasons which are beyond one's control, such as accidents or sickness, heavy rains or earthquakes etc.

1.13 Causes of Absenteeism

The causes of absenteeism can be:

- Accidents
- Illness or physical unfitness
- Stress
- Poor leadership
- Lack of job satisfaction
- Boredom
- Personal problems
- Heavy workloads
- transportation problems
Some major factors that can be the cause of absenteeism in the organization are as described below:

**Attitude of the employee**

The main cause of absenteeism at the workplace is the attitude of the employee towards his work and the workplace. The attitude of the employee will clarify the level of commitment the employee has towards their work. An employee with good work attitude will not take unnecessary leaves and such employees generally plan their leaves well in advance so that proper delegation of duties can be arranged before they go for it. On the other hand, the employee with poor work attitude will always misuse leaves entitlements and can even have disciplinary and integrity issues.

**Number of years served with the organization**

Many surveys have been done on this matter and it is clearly found that the longer the employee is associated with the organization, the lesser unplanned leaves he will take. There can be some exceptional cases. The most likely reason for this can be that the organizations would have thrown away those employees who have indulged in absenteeism much before.

Also, the seniority plays an important role. The more senior employees are less likely to log in many missing workdays. So, we can understand that usually the junior employees and the new hires tend to take more unplanned leaves as compared to the old employees.
Work Pressure

If in any organization, the work pressure goes up, it can be clearly seen that the absenteeism rate also goes up tremendously. Many a times, in order to avoid stressful situations, like difficult meetings, coincidently report in “sick “or having “family commitments” on that day. It is the best way to take the day off in order not to face such pressures.

Relationship with Superiors

The absenteeism also depends upon the working relationships in the office. If the HOD are putting too much pressure on their staff or the managers are demanding beyond what is expected from their subordinates then automatically the absenteeism will rise. In the surveys, a large number of employees say “poor relationship with superiors” as the main reason for staying away from work.

Job Satisfaction

The major pulling factor for people to seek employment is job satisfaction other than the salary. This can be the reason of people changing jobs or work environment. Some employees prefer doing the same thing over and over again and will not seek new responsibilities, while others find it boring to perform monotonous functions. But in both cases, absenteeism will occur when their level of satisfaction is lower than what they would accept in their daily work. It is very important to track absenteeism and to be kept under control. For doing this, the employers need to address employees need. There should be mutual respect between the employee and employer so as to have a workable solution.
1.14 Cost of Absenteeism

Absenteeism may have repercussions, like:

The organizational productivity gets decreased as:

- employees need to carry extra load of work, or helping the new or substitute staff
- employees need to guide and orient new or substitute workers
- This affects confidence and services of the employee.

The organizational cost increases as:

- Organization has to pay extra for replacement workers

The organizational administrative cost also increases as:

- Assignment of work to the replacement employees and reassignment of workload to the existing employees
- time is required to sustain and control employee absence
1.15 Absenteeism Problem:
Many organizations allocate 3% of their labour budget for absenteeism based on an average of eight (8) working days missed per employee annually.

Fashion in Absenteeism

Many surveys are done on the trends of absenteeism and following generalization of absenteeism were found:

- Increase in the pay reduces absenteeism and attrition rate.
- With the growth of organizations, employee absenteeism increases
- Women absenteeism is higher
- Single employees absenteeism rate is higher than married employees
- Younger employees absenteeism rate is higher than older employees
- Duration of absenteeism older employees is higher than younger employees

1.16 Understanding Absenteeism

The absenteeism in the organizations badly affects its productivity and efficiency. The organization incurs extra cost due to the same. The absenteeism control methods need to be developed such that organizational trust is maintained. It is seen that traditional methods of absenteeism control are no more effective. It is difficult to create a fair procedure for the absenteeism.

Every employee who is away from work has valid reasons for absenteeism.

To control absenteeism, employees’ physical and emotional needs should be addressed. A greater percentage of absenteeism can be controlled through that.
1.17 Purpose of Attendance Management

Attendance management system is required to build up a readiness of the workforce to be present in the organization on a regular basis. Also it is beneficial to them in appealing their peers to show their sincere presence in the organization regularly. This can be done by:

1. Dealing with the employees excessive absenteeism fairly
2. addressing the employees needs
3. conversing the organizational goals

The organizations management needs to make managers and supervisors aware of the attendance management and the organization’s working culture.

1. Workers should be a part of organizational goal. It will motivate them to be regular in attendance.
2. The employee motivation increases if their job seems meaningful to them. The attendance automatically increases.
3. Peer employees put pressure to the absent employees so that their work load reduces.
4. Recognition of active and regular employee helps improve the attendance.
5. Supportive and understanding supervisor increases the employee regularity as he can discuss the on job problems openly with him.
6. Regular employees are happy with their jobs and get opportunities for promotion and upgrading. This leads them to feel confident and have a very good workplace relationship.
Commitment to Attendance
The attendance management program can be made successful in the work place if there is a two-way communication between the employees and the management. Attendance is the responsibility of every employee of the organization.

A good attendance is expected from the employees as they are been paid. It is an obligation for them to be present in the organizations on a regular basis. All the levels of management should be communicated about the expectations. If the organizational attendance expectations are known to the employees tries to fulfil them.

Software can be used for tracking and keeping the attendance records. They can help organizations register and track employee attendance and it can be integrated with existing payroll and human resource systems. The major parts of such system are:

**Employee:** whose attendance has to be recorded either manually through timekeeper or automatically through special hardware device such as card reader or biometrics.

**Timekeeper:** the employee responsible for recording employee's attendance manually.

**Administrator:** who can manipulate employee information or designation information.

Previously the work procedures in many organizations were done by paperwork, which caused many faults and inaccuracy, and this made gap between the manager or administrator and employee and customer (Harold, 2000). After the revolution and the growth of the technology, the dependence on computers has become a base factor for any successful business, by the spread of the computer applications and the wide usage of these application by the organizations, many innovative ideas rise to find flexible systems that were developed to provide better results and can be used by many organizations.

If employee monitoring is done in an effective manner by using the latest technology, then the above problem can be solved up to a large extent. For example, the Time-Attendance System(TAS). The latest software can help organization for registering and tracking employee attendance. They help in eliminating paperwork and saves employees’ time calculation, validation, and re-keying payroll information.
As a result, employee working hours can be accurately tracked, which is important for organizations, with exceptions such as lateness, absence, overtime and others can be accurately tracked and reported.

1.18 OBJECTIVES

India is a developing country and with India, the various organizations are also growing and developing. In the last few years, with the tremendous growth of the organizations, the work of the organizations have also increased and it cannot be thoroughly managed single handed. So, there is a need of division of work.

With this need, the organizational structure was redefined and redesigned. The complete work was divided in to various divisions or departments. Previously, people in the organization worked to achieve the pre-defined goal and now, each division work in the interrelationship for the predefined goal. Every division has its own goal with set of rules to achieve that goal and with that in collaboration with other division; the ultimate objective of the organization is achieved.

In short, each division has its own head of the department, its own data and its own rules. Each division wants to share some data with the other division and want to secure some from sharing with other departments. This can be possible only if we allow the specific people to have rights to enter into the secured area.

For this restriction in entry and usage of data many alternatives were proposed and used, e.g. initially authentication was done using signature of the employee but the trespassers started copying the signature and entering into the system.

So, the concept of identity card was introduced which was readily accepted by the people and was working without flaws. But then the trace passers found out the way to breach this security concept also. They either stole the identity card or even used it for proxy entry.
After such kind of misuse of identity cards, some electronic swipe cards were provided which were to be swiped to enter into the restricted area. Thus, the concept of swipe cards is put in to use.

This concept faces various problems. Employees give their swipe cards to others to put their attendance or to enter into the restricted areas (buddy punching). So now there is a tremendous need of a new concept which is specific to each person.

The concept of “WHO YOU ARE”!

This concept is called BIOMETRICS.

Biometrics is the most secured way of authenticating any person. It is done by using the body parts of the human. The identity card and PIN can be stolen but we cannot steal the body parts of any human. This concept can be very easily taken forward to the growth of organizations. If we are able to keep a proper check on the employees attendance and secure organizational data in a proper efficient manner then automatic growth can be seen.

The research scholar aims to highlight the following objectives:

1) In-depth analysis of the past security system.

2) How the security system in the present scenario is?

3) What is the present security system and what are the demands.

4) What type of the security system exists in the international market?

5) Analysis of the above mentioned 4 objectives.

6) How can we overcome these drawbacks and what is the new proposed system.

7) Cost-benefit analysis of the proposed system.
1.19 HYPOTHESIS

A research hypothesis is a kind of assumption which can also be called as a statement of expectation or some kind of prediction done by the research scholar which he test with the research work or study. Before framing the research hypothesis, the research scholar should be able to identify his area of interest. For this, the RS needs to read books, articles, cases, etc so that he gets the required knowledge and details of the topic.

Now, this information gained about the topic helps the RS in formulating the Research questions. When we state the research question in one sentence, it becomes the research hypothesis, which is also called as the “thesis statement.”

The relationship between variables used in the hypothesis needs to be predicted. Once it is done, then the hypothesis is proved using the remedial details gained during the research process. This approach helps in creating a greater understanding of the topic or a better conclusion.

The formulation of hypothesis can be done using following points:

1. The topic should be read and understood by the RS properly before taking the final decision. They should check that they have a sufficient amount of published material on the selected topic and it can be worked upon by the RS.

2. A research hypothesis is beyond any topic. It actually works on two variables related to each other. What you propose to “prove” through the research is called as a hypothesis. The research results in a conclusion, a theory, or an understanding that can be applicable or useful in the real world.

3. Judgmental words should not be used in the hypothesis. The judgments based on emotions are not appropriate to be hypothesis. In order to get unbiased response RS should try to be more objective.
4. The hypothesis should have questions that are not limited by law only. RS needs to conduct a literature review of 2 or 3 disciplines only. To choose a hypothesis, the best way is to have some familiarity levels with the most relevant discipline within the topic limits.

5. The terms used in the hypothesis should be defined and understood clearly. There should be no assumptions and generalizations of reader’s knowledge towards the technical terms.

6. The research scholar should keep in mind that the hypothesis can change over time with progress in the research work.

Before going forward with the topic or modification, the research scholar should take the guide’s approval.

The hypothesis can be presented as :

• a one-sentence hypothesis or

• a research question
In the light of the above cited objectives and the background or preamble, the research scholar has setup the following Hypotheses for the present study:

**Hypothesis 1:** People are resistant to technological change in the security system of the organization.

**Hypothesis 2:** Lack of proper security system results in organizationally important information hacked and misused.

**Hypothesis 3:** A proper approach for implementing the security system in any organization increases the data security.

**Hypothesis 4:** Indian organizations’ perspectives and mentality towards working hours is casual.

**Hypothesis 5:** Proper identification system reduces absenteeism

**Hypothesis 6:** Avoidance of Absenteeism increases efficiency and productivity.

The research scholar, considering the above hypotheses, wants to do the research work on the above mentioned topic so that the proposed security system strikes the market with a big bang.
1.20 RESEARCH METHODOLOGY

Organizations are growing with the same pace as of India’s development. These organizations need to follow some rules and methods to maintain the security in all the departments so that the important information is not hacked. The access is provided only to the authentic people.

With change in technology, the way of providing security to the data of the organization or any process of the organization has really become very cumbersome and tough. It is to be found out how new ways can provide security to avoid breach on the existing system.

Ten years ago, there were different methods of providing security and following the organizational rules. But now, with the growth of the Indian organizations and changes in the method of their working, the need to identify some new ways of providing security is required which cannot be breached very easily.

As India is a developing country, all the organizations are also developing and growing rapidly to compete with the international organizations.

Data collection: A process conducted by the research scholar in order to prepare and collect data is called as data collection. The data collection is done to get the required information for keeping records, for decision making on important issues, or for passing information to others. In order to provide information about a specific topic, the research scholar collects the data.
Interviews

In Quantitative research, the interviews are considered to be more structured as compared to the Qualitative research. In a structured interview, the RS is has to asks a specific set of questions which are generally predefined.

Face-to-face interview is a type of interview in which the research scholar talks to the interviewee in the face to face method. This type of interview enables the RS to set up a good rapport with the participants and helps the RS to gain their cooperation. If the interviewee gives vague answers to the interviewer and as a result he can seek the follow-up information.
Telephone interviews- This type of interview are fast and cheap and the researcher can contact any person who has a telephone. Geographical distances have no value. The disadvantage of this approach is that the response rate is low as compared to the face-to-face interview but higher than the questionnaire sent through mail.

Computer Assisted Personal Interviewing (CAPI): This is a type of personal interview in which the questionnaires are replaced by the direct entry of the information into the database by the laptop or hand-held computer brought by the interviewer. By using this approach, the time is saved. It involves data processing and saves RS from carrying around hundreds of questionnaires. It is an expensive approach and needs the interviewer to have a technical knowhow.

Questionnaires

Paper-pencil-questionnaires: This approach is used to send the details to be filled up by a large number of people and saves the time and money of the researcher. The respondents are truthful in responding to the questionnaires regarding controversial issues in particular due to the fact that their responses are anonymous. The major drawback is that majority of the people who receive questionnaires are not interested in filling up the forms and return them and those who do might not be representative of the originally selected sample.
Web based questionnaires: The latest technology used by the researchers in today’s time is the use of Internet based research. In this technology, the e-mails are received on which the end user would click on an address and reach to the secured web-site to fill the questionnaire. It is a quicker and less detailed way of getting the questionnaires filled. The main disadvantage of this method is that the people who are not tech savvy or do not own a computer cannot fill up the questionnaires. Also there is a possibility that the research scholars do not get the proper responses as people are in a great hurry to complete it and so might not give correct and accurate responses.

1) Primary data:

The prime focus is on the primary data. It is collected through information of various companies/organizations visited.

Companies visited are:

a) TCS (IT)

b) Reliance broadcast network ltd (Media)

c) Atharva Institute of Management Studies (Educational Institute)

d) Spencers (Retail)

e) Oracle(IT)

f) Bank of Maharashtra (Finance)

The research scholar has also used interview and questionnaire methods.

The data collection always follows a plan. This plan follows the activities like:

1. Pre collection activity — what data is to be collected, what methods would be used etc.

2. Collection — collecting data from various sources

3. Present Findings — sorting out the data and presenting the findings.
The main data collection methods used by the researcher in the research are:

**Questionnaires** - are the forms filled and returned by the respondents. This is an inexpensive method and is used where literacy rates are high and respondents are of cooperative nature. Questionnaires can be handed personally or sent by mails. They can then be collected after the defined time or can be returned by post. This method can be used for the entire population or sampled respondents.

In the questionnaire method, respondents should fill the form themselves. The types of respondents should be literate. It should be prepared in the major languages of the target group. The research scholar has considered English language in her research.

The questionnaire should be:

1. Short
2. Simple
3. Clear
4. Proper target respondents
5. questions

The type of questions in the questionnaire is open-ended as well as closes ended questions.

**Interviews** – The researcher conducted interviews with the respondent. Taking interviews is more expensive as compared to questionnaires. Benefits of interviews:

6. better for complex questions
7. better for cases where literary rate is low
8. better for cases where cooperation is less

The research scholar conducted structured interviews using survey forms and open interviews. The notes were taken which were interpreted for the future analysis.
**Direct observations** – The research scholar also made visit to the organizations for the direct observations and noted the observations which was later used for the analysis.

**Open-ended interviews** - The research scholar also took some open ended interviews.

**Focus groups** - The research scholar also discussed with the group of 5-10 respondents whose opinions were considered during the analysis.

**Telephonic Interview** - The researcher also covered the data gathering through the telephonic interviews. This method was used with the people who have a very less time and could not be contacted for any reason. This is a cheaper and a faster method which is very flexible.

The research scholar has also performed various types of surveys like:

**Pilot Survey**: In this the research scholar identified few companies and distributed the questionnaire and checked whether a proper result can be expected from such kind of respondents and organizations or not.

**Field Survey**: Once the pilot survey was conducted and type of respondents was identified, then the researcher actually distributed the questionnaire to the respondents and got 250 surveys filled by a variety of people from various organizations.

**Experience Survey**: The research scholar identified some key respondents and conducted one to one interview and tried to analyse their responses.

**Peer Discussion**: Research Scholar also conducted a peer discussion with the colleagues and the same level of respondents of her field so as to discuss upon the outline of the study and tried to take their feedback.

**Brain Storming**: The research scholar brainstormed with the various respondents using schedule method and identified the way to reach towards the objective.
2) **Secondary data and the Sources:**

Collection of secondary data: sources- various libraries, News paper articles, white papers, internet, journals, telephonic talk and support from the guide. The research scholar has visited:

a) British Council Library
b) J Gate Research Journal
c) Proquest E-Journal
d) Citeseer

Internet is the biggest source which has been adequately used.

Research scholar has conducted regular meetings with the guide and meetings with the heads of various organizations and scholars in concerned field to collect the data.

1.21 **SCOPE**

The research scholar cannot do the research without setting the limits. Some boundaries need to be set. These boundaries can be on the basis of geography, demography, age group, income group or number of organizations.

The research scholar defined her scope to Mumbai city. All the companies of Mumbai city of different sectors like Information Technology, Finance, Education, Media etc. Were visited and it was observed how they are being affected by the security system.

Another boundary was the number of companies or organizations that the research scholar visited. The researcher visited only 5-6 companies mentioned in the methodology, so that proper study and proper comparative outputs can be shown.
1.22 UTILITY

The research scholar feels that her study would be useful in the growth and development of the organization. This work will help in increasing the employee satisfaction and ultimately in the development of India.

1) The working of various organizations will be more systematic and secured.
2) The employee information and details will be safe and cannot be hacked.
3) The employees will no more be able to play with the rules and regulations of the organization.
4) With proper security system, the organization will grow and ultimately, growth of India will be seen.
5) Indian organizations would be in position to compete with the international organizations as far as security is concerned.

1.23 LIMITATIONS:

1) Time boundedness: As there is a limited time, it will be major limitations during the research work.
2) Geographic limitations: The study has been particularly limited to the companies in Mumbai only. As Mumbai is a hub and it has got most of the companies and MNC here, we can limit our search to Mumbai only.
3) The third limitation was the way organization’s employee reacted to the questionnaire and interviews taken by the research scholar.
4) One of the considerations would be the time lag between preparation, supply and the receipt of the feedbacks from the respondents.