## 2) Identification, Authentication & Operational Security

**2.1 Username and Password:** The first security is that when user log on to the computer and asked for to enter username and password. The first step is called as identification. You announce who you are. The second step is called as authentication. Once you entered user name and password, a computer will check all the entries and try to authenticate, and only login will succeed.

- Managing password: Hackers have dozens of tools at their disposal for cracking passwords, such as those based on words in a dictionary can be cracked in the matter of seconds. Passwords are meant to be secret shared between the user and the system authenticating the user. To authenticate a remote user when user has not got a password, some issues need to be considered:
  - Do not give password to the caller but call back an authorised phone number from your files.
  - Call back someone else.
  - Send passwords that are valid only for a single login request so that the user has to change immidiately to a password no known by the sender.
  - Send mail with courier with personal delivery.
  - Request confirmation on a different channel to activate the user account.

- Choosing password :- Password selection is very important for the authorised user. This is because the password is the way the computer verifies that someone logging in with your account is really you.

What not to do when choosing a password:

⇒ Do not choose a password based upon your personal data.

⇒ Do not choose a password that is your a word, name of a TV show, keyboard sequence.

⇒ Do not choose a password that is a simple transformation of a word, such as putting punctuation marks at beginning and end, writing letter "l" as "1", writing a word backwards.

⇒ Do not choose passwords less than 8 characters long or that are made up of solely of numbers or letters. Use letters of different cases and use mixture of alphabets, digits and symbols.

Best methods for choosing password:

⇒ Eight characters of password should be the absolute minimum length.

⇒ Create a phrase or series of letters that is seemingly random but are easy to remember. For example: I have two kids: Jack and Jill.

⇒ Add numbers to the base word to make it more secure. For example: Woodstack 3652 etc.

⇒ Use punctuation and symbols to complicate it further. For example: Woodstack#3562 etc.

⇒ Create complexity with uppercase and lowercase letters. For example: WooDStack#3562 etc.

2.2 Role of people in security:- The heart of any security system is people. This is particularly true in computer security, which deals mainly with technological controls that can usually by passed by human intervention. People are considered the weakest link in the security chain. Awareness of the risks and available safeguards is the first line of defence for security of computer system.

## Password selection :-

The following are the guidelines for selection of password

1) Make your password as long as possible.
2) Use as many different characters as possible.
3) Do not use personal information
4) Do not use words listed in standard dictionary.
5) Do not use password that is same as your account number.
6) Do not use password that are easy to spot while typing.
7) Change your password on regular basis.
8) Never write down password.
9) Never share password with anyone.

— (Some key words your password should not include are listed in textbook. Refer textbook for details.)

## Password selection strategies :

There are four basic techniques are in use to reduce guessable passwords while allowing the user to select a password which is memory.

1. User education
2. Computer generated password
3. Reactive password checking
4. Proactive password checking.

### (1) User education :-

* Tell the importance of hard to guess passwords to the users and providing guidelines for selecting strong password.
* Many users may ignore the guidelines which may not be the good judgement of what is strong password.

② Computer generated password :-

* Computer generated passwords also have some problems. If the passwords are reasonably random in nature, users will not be able to remember it.
* Even though password is pronounceable, the user may have difficulty in remembering it.

③ Reactive password checking :-

* In this scheme, the system periodically runs its own password cracker program to find out guessable passwords.
* If the system finds any such password, the system cancels it and notifies the user.
* This method have number of drawbacks - because a strong minded opponent who is able to steal a password file can dedicate full CPU time to the task for hours or even days.

④ Proactive password checking :-

* It is the most promising approach to improved password security. In this scheme, a user is allowed to select his/her own password.
* However at the time of selection, the system checks the password if the password is allowable then allow or reject it.
* The trick with a proactive password checker is to strike a balance between acceptability and strength of the user.
* If the system continuously rejects many passwords, then users will complain that it is very hard to select a password.

Following are the two possible approaches to proactive password checking :-

- All passwords must be 8 characters long.
- In the password, there should be at least one uppercase, lowercase, numeric digits, and punctuation marks.

Piggybacking :- Piggy backing refers to access of a wireless internet connection by bringing one's own laptop computer within the range of another's wireless connection, and using that service without the suscriber's explicit permission or knowledge. In security, piggybacking refers to when a person tags along with another person, who is authorised to gain entry into a restricted area, or pass a certain checkpoint.

The reasons for piggybacking can be one of the following:

- Avoid paying a required access fee.
- Gaining access to an area completely disallowed to the piggy backer.
- To avoid the hassle of signing in, presenting identification, or being involved in an interaction with the staff, even if the person has right to access.
- A person may have forgotten or lost his/her access key, passcard token, or finds the access procedure inconvenient.

Shoulder surfing :- In computer security, shoulder surfing refers to the direct observation techniques, such as looking over someone's shoulder, to get information. It is particularly effective in crowded places because it is relatively easy to observe someone as they:

- fill out a form
- enter your PIN at an ATM or POS machine
- use calling card at a public pay phone
- enter passwords at a cyber cafe, public and university libraries, or airport kiosks
- enter a code for rented locker in public place such as swimming pool or airport.

- Dumpster Diving :- Dumpster diving is a method by which attacker searches for important system information by diving into the dump. The search is carried out in paper waste, electronic waste such as old HDD, floppy and CD media recycle and trash bins on the systems. Attackers tries to extract passwords, system configuration, network configuration, user lists from this method and gain access to these important system details.

  To prevent dumpster divers, all papers and print-outs should be shredded in cross-cut shredder before being recycled, all storage media must be erased, and all staff is educated about the danger of untracked trash.

- Installing unauthorised Software / Hardware :-

  Unauthorised Software Installation :- Installation unauthorised software programs such as games to play during break time, signature files for email, weather programs, etc. on your computer at work may seem harmless or even beneficial. However software from unauthorised sources can create following problems :

  - Free ware or low cost softwares can contain viruses that can be spread to other computers on the network.
  - It can crash your system and send unwanted messages on the network.
  - It can contain spyware, that can be used for capturing data and information you type and send it to marketers or criminals.
  - Downloading unauthorised software can be anything but harmless and therefore shall be avoided.

  Installing unauthorised hardware :-

  By Insider :- The insider plants unauthorised hardware to sniff the network and to leak the information.

  By outsiders :- Outsiders such as service personnels of the supplies and third party vendors to gain unauthorised access into system or network.

- Access by Non-employee :- Providing access for non-employees is a challenge in all regards. The best practices associated for providing access to non employees are listed below
  - Username identification =>
  - Enable on-demand
  - Time Limited Account
  - Permission Lockdown
  - Isolated networks or domains

  (Refer textbook for details)

- Security Awareness :- Security awareness and training are critical at all stages and levels of information security. For example, upper management needs to learn about the institutional risks; users must be taught how to defend themselves against malicious code; system and network administrators require training to help them maintain and improve the security of systems they oversee.

  Companies face threats to their employees, systems, operations, and information every day. These threats include computer viruses, network attacks, fraud, industrial espionage and even natural disasters

- Individual User Responsibility :- Users who are not aware of computer security aspects of the system, compromise the security by :
  1. Executing programs from unknown source
  2. Opening documents from unknown source.
  3. Exposing password or not protecting them.
  4. Accessing computer networks executing the programs remotely without the knowledge of their source
  5. Opening e-mails and their attachments from untrusted origin

⑥ Downloading plugging and active-X controls.
Hence, it is the responsibility of the user to be aware about information security and avoid the above points.

□ security policies :- Security policy can be defined as rules that regulate how an organisation manages and protects its information and computing resources. The objectives of security policy are :

- Improve information security
- Avoid misuse
- Control Information Browsing
- Prevent Penetration
- Prevent Computer viruses
- Prevent Fraud
- To minimize the effect of component faliure.

In security policies, following considerations are required to be undertaken :

① Security policy document : The security policy document is required with recording comprehensively various rules and guidelines that include the roles required to authorize the user.

② Identification : The subjects or users of the system should be positively and uniquely identified.

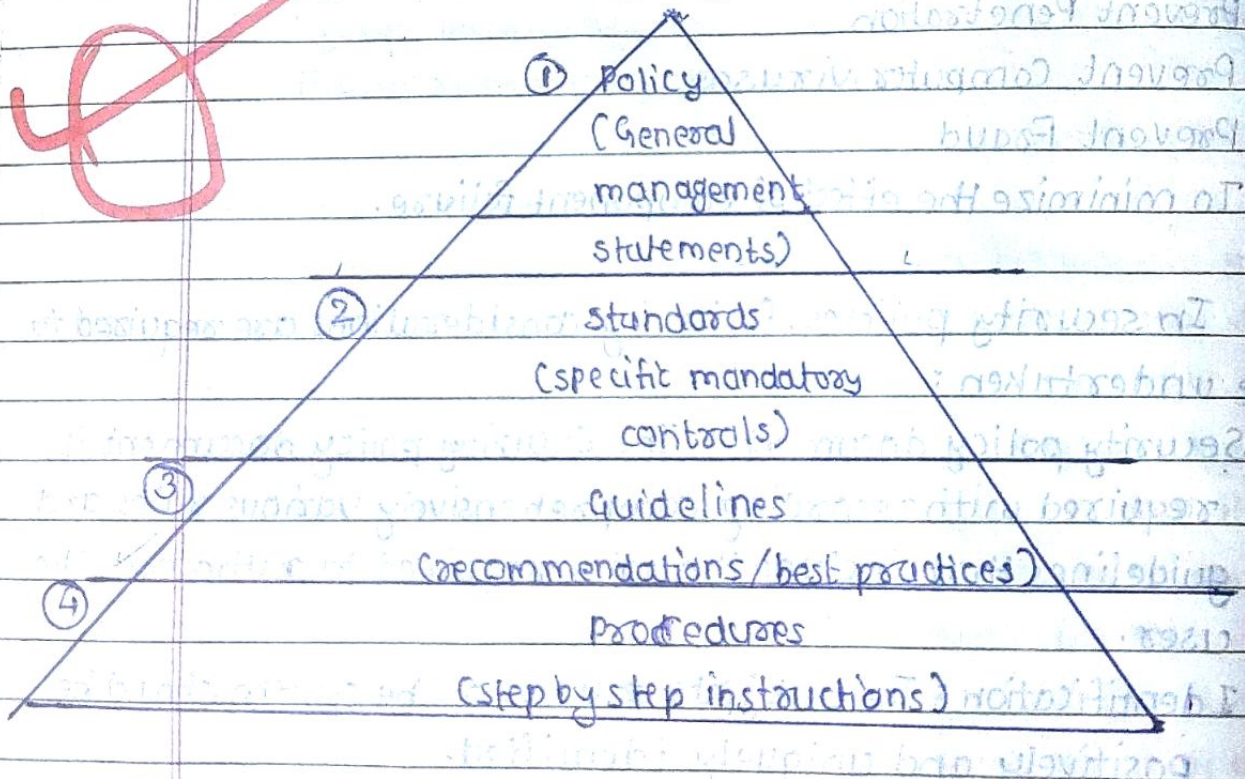
③ Marking : The object or resources should be marked either physically or logically that provide information on the level of sensetivity of the objects and previlages required for the subject to use that object.

④ Accountability : The system should be able to identify or trace events which user is doing what? When? And from where? In case of problem, an audit should be able to reveal the cause of problem.

⑤ Assurance :- The security policy is prepared systems related to marking, identification and accountability are implemented and running and the security status of the system is proper. These all things are needed to assured compulsorily.

⑥ Continuous upgrades :- The system secured today is not as secured as tomorrow since many new types of methods of attack are invented. Therefore continuous upgrades are necessary.

What are policies, standards, Guidelines and procedures for information security?




① Policies :- An information security policy consists of high level statements relating to the protection of information across the business and should be produced by senior management.

(2) Standards:- standards consists of specific low level mandatory controls that help enforce and support the information security policy.

(3) Guidelines:- Guidelines consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place.

(4) Procedures:- Procedures consist of step by step instruction to assist workers in implementing various policies, standards and guidelines.

Example: Access to Company Information is Restricted

* Policy:- Access to company information systems is restricted to authorised users only.
* Standards:- Users are required to have a unique userID and a confidiential password.
* Guidelines:- Passwords should be five to eight alphanumeric characters.
* Procedures:- UserID and password requests must contain a signature of the authorised information owner. Approval signatures shall be verified against a company authorized signatures reference manuals.

2.3 Access Controls: Access control is the ability to permit or deny the use of particular resources by particular entity. Access control mechanisms can be used in managing physical resources, logical resources or digital resources. For example, a private text document on a computer, which only certain users should be able to read.

Page No. 50
Date

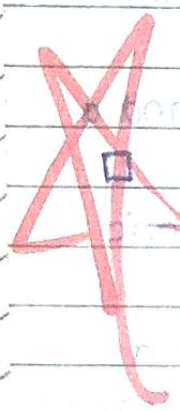
Access control techniques:

- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role ~~based access~~ based access control (RBAC)

Discretionary access control (DAC):- DAC is a type of access control in which user has complete control over all the programs it owns and executes, and also determine the permissions other users have those files and programs. DAC is an access policy determined by an owner of an object. The owner decides who is allowed to access the object and what previlages they have.

Two important concepts in DAC are:

- File and data ownership
- Access rights and permissions



Mandatory access control (MAC):- MAC is a type of access control in which only the administrator manages to access controls. The administrator defines usage and access policy, which cannot be modified or changed by the users, and the policy, will indicate who has the access to which programs and files. It is often placed in systems where priority is placed on confidientiality. Two methods commonly used for applying mandatory access control:

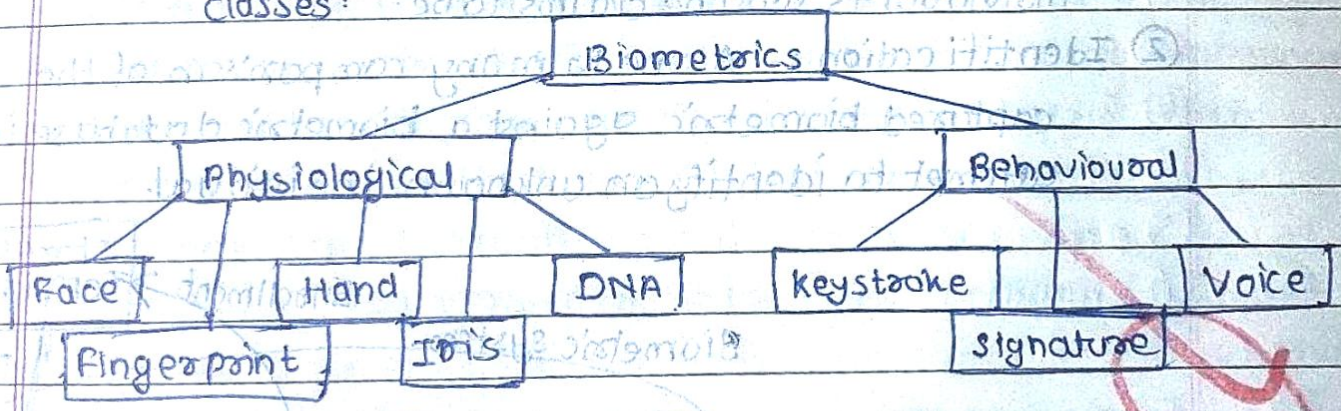
- Rule based (or label based) access control.
- Lattice based access control.

Role based access control (RBAC) :- RBAC is an policy determined by the system, not the owner. RBAC differs from DAC because in RBAC, access is controlled by the system level, outside of the user's control. Three primary rules are defined for RBAC:

- Role assignment
- Role authentication
- Transaction authorisation

2.4 Biometrics :- Biometrics refers to study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioural characteristics. Biometric identification is used on the basis of some unique physical attribute of the user that positively identifies the user.

Biometric characteristics can be divided into two main classes:




Classification of biometric characteristics

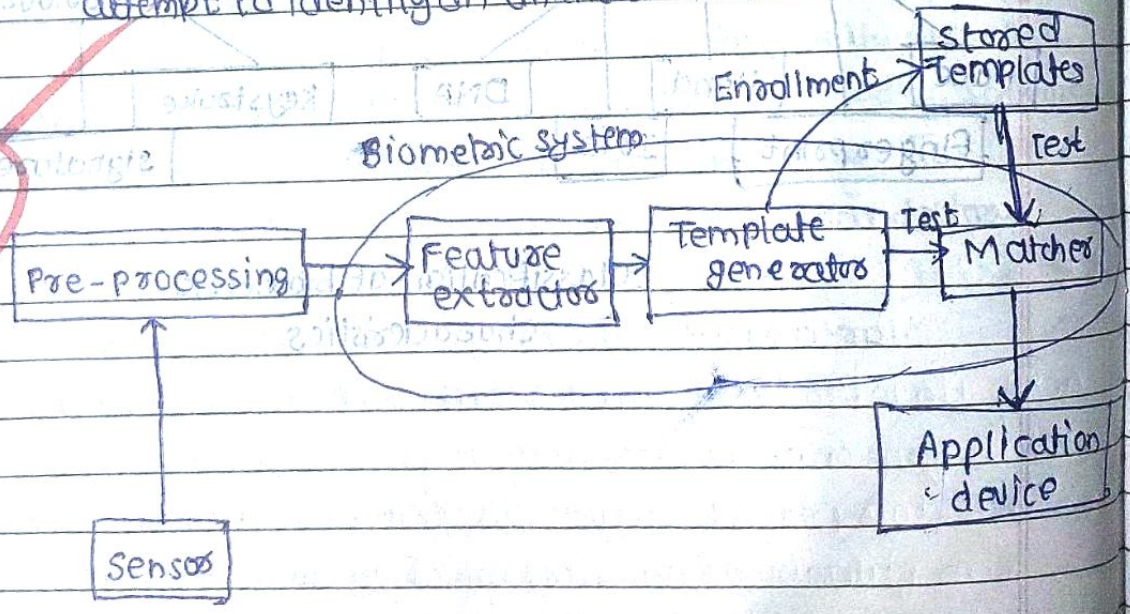
It is possible to understand, if a human characteristic can be used for biometrics in terms of following parameters:

- Universality :- Each person should have the characteristic
- Uniqueness :- is how well the biometrics seperate individuals from another
- Permanence :- measures how well a biometric resists aging and other variance over time.
- Collect ability :- ease of acquisition for measurement.
- Performance :- accuracy speed and robustness of technology used.
- Acceptability :- degree of approval of a technology.
- Circumvention :- ease of use of a substitute

A biometric system can operate in two modes:

① Verification :- A one to one comparison of a captured biometric with a stored template to verify that the individual is who he claims to be.

② Identification :- A one to many comparison of the captured biometric against a biometric database in attempt to identify an unknown individual.




Block diagram of bio-metric system

The first time an individual uses biometric is known as enrollment. During enrollment, biometric information from an individual is stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment.

① The first block (sensor) is the interface between real world and the system; it has to acquire all necessary data.

② The second block performs all necessary pre-processing: it has to remove all artifacts from the sensor, to enhance the input.

③ The third block extracts necessary features. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from a source.

④ If enrollment is being performed, the template is simply stored somewhere. If matching process is being performed, the obtained template is passed to the matcher that compares it with other existing templates.

Performance measurement parameters of Biometric System:-

The following are used as performance metrics for biometric systems:

- False accept rate or false rate match (FAR or FMR) - the probability that the system incorrectly matches the input pattern to a non-matching template in database. It measures the percent of invalid inputs which are incorrectly accepted.
- False reject rate or false non-match rate (FRR or FNMR) - the probability that a system fails to detect a match between input pattern and a matching template in database. It measures per cent of valid inputs which are incorrectly rejected

- Receiver operating characteristic or relative operating characteristics (ROC) :- The ROC plot is a visual characterisation of trade off between FAR and the FRR
- Equal error rate or crossover error rate (EER or CER): the rate at which accept and reject errors are equal.
- Failure to enroll rate (FTE or FER) - the rate at which attempts to create a template from an input is unsucessful. This is most commonly called as low quality inputs.
- Failure to capture rate (FTC) :- Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
- Template capacity :- The maximum number of sets of data which can be stored in the system.

Applications of Biometrics:

1. Biometric Time clocks or Biometric attendance systems
2. Biometric safes and Biometric locks
3. Biometric access control systems
4. Biometric systems for single logon facilities on PC.
5. Wireless Biometrics for high end security
6. Applications in identifying DNA patterns and criminals
7. Biometrics airport security services.

- Finger prints :- In this, the fingerprints of the user are matched with the database and matching is carried out using complex image processing algorithms. Fingerprint recognition or finger print authentication refers to the automated method of verifying match between two human finger prints. Finger prints are one of many forms of biometrics used to identify an individual and verify their identity.

Patterns:-

* An arch is a pattern where the ridges enter from one side of the finger, rise in the center forming an arc, and exit from the other side of the finger.
* The loop pattern where the ridges enter from one side of the finger, form a curve, and tend to exit from the same side they enter.
* In whorl pattern, ridges form circularly around a central point on the finger.

Finger print sensors:- A finger print sensor is an electronic device used to capture a digital image of a fingerprint pattern. The captured image is called as live scan. This live scan is digitally processed to create a biometric template.
Commonly used finger print sensor technologies are:

- Optical fingerprint imaging involves capturing a digital ~~impac~~ image of a print using visible light.
- Ultrasonic sensors make use of the principles of medical ultrasonography in order to create visual images of the fingerprint.
- Capacitance sensors utilize principles associated with capacitance in order to form fingerprint images.

Applications of finger prints:

- Forensic: Corpse identification, Criminal investigation, Terrorist identification, Parenthood determination, missing children, etc.
- Government: National ID card, Correctional facility, Drivers' licence, Social security, Welfare disbursement, Border control, Passport control.
- Commercial: ATM, Credit card, Personal Digital Assistant (PDA), Electronic data security, Computer login

Advantages of finger prints:

⇨ Very high accuracy
⇨ It is one of the most developed biometrics.
⇨ Easy to use
⇨ It is standardised
⇨ Higher reliability and stability

Disadvantages of finger prints:

⇨ Vulnerable to noise and distortion brought on by dirt and twists
⇨ Some people have damaged or eliminated finger prints.
⇨ For some people, it is still intrusive, because it is related to criminal identification.

☐ Hand prints:- Hand geometry biometrics is based on geometric shape of hand - size of palm, length and width of fingers, distance between knuckles, etc.
Hand geometry is a biometric that identifies user by shape of their hands. Hand geometry readers measure a user's hand along with many dimensions and compare those measurements to measurements stored in a file.

Advantages of hand prints:

⇨ Though it requires special hardware to use, it can be easily integrated into other devices or systems
⇨ It has no public attitude problems, as it is associated with authorised access.
⇨ Simple, relatively easy to use and inexpensive.
⇨ Environmental factors such as dry weather, which causes drying of skin is not an issue.
⇨ Usually considered less intrusive.

Disadvantages of hand prints:

⇒ Very expensive
⇒ Considerable size
⇒ Not ideal for growing children.
⇒ It is not unique and cannot be used in identification system.

Retina Scan Techniques: A retinal scan is a biometric technique that uses the unique patterns on the person's retina to identify them. A human retina is a thin tissue composed of neural cells that is located in the ~~posterior~~ posterior portion of the eye. Because of the complex structure of capillaries that supply retina with blood, each person's retina is unique.

A biometric identifier known as retinal scan is used to map the unique patterns of the person's retina. The blood vessels within the retina absorb light more readily than the surrounding tissues and are easily identified with appropriate lighting.

Uses of retina scan techniques:

- Retinal scanners are typically used for authentication and identification processes. This technique is utilized by several government agencies including the FBI, CIA and NASA.
- Retinal scanners are also used in medical applications. Many diseases can be detected as they have some impact on eyes.

Advantages of Retina Scan Techniques:

⇒ Low occurrance of false positives.
⇒ Very high accuracy.
⇒ Extremely low (almost 0%) false negative rates
⇒ Highly reliable as no two people have same retinal pattern
⇒ Speedy results.

Disadvantages of retina scan techniques:

⇨ Measurement accuracy can be affected by disease such as cataracts
⇨ scanning procedure is perceived by some as invasive
⇨ Not very user friendly.
⇨ High equipment costs.
⇨ Very intrusive, very expensive.

Voice patterns: In the method of voice synthesis, the voice of user is recorded and its digital signal analysis is carried out. The analysis is matched and depending upon the satisfactory match, authentication is carried out.

Speaker recognition is the computing task of validating a user's claimed identity using characteristics extracted from their voices.

Advantages of voice biometric patterns:

⇨ Ability of use existing telephone
⇨ Cheap technology
⇨ Non-intrusive
⇨ Low perceived invasiveness

Disadvantages of voice biometric patterns:

⇨ High false matching rates
⇨ Low accuracy
⇨ An illness may change person's voice.

Page No. 39
Date

- Signature and Writing Patterns:- In a signature recognition system, a person signs his or her signature on a digitalized graphics tablet or personal digital assistant. The system analyses signature dynamics such as speed, relative speed, stroke order, stroke count, and pressure.

Advantages of signature recognition:

⇒ Non intrusive
⇒ Little time of verification
⇒ Cheap technology.
⇒ Low False Acceptance Rates.

Disadvantages of signature recognition:

⇒ Individuals who do not sign their names in a consistent manner may have difficulty enrolling and verifying in signature verification

- Keystroke dynamics:- Keystroke dynamics or typing dynamics, is the detailed timing information that describes exactly when each key was pressed and when it was released as a person is tying at a computer keyboard.

Comparison of the biometric methods:

→ PTO

Page No. 60
Date

| | Iris-recognition | Retinal Scan | Finger print | Hand geometry | Voice recog | Facial recognition | Writing Signature |
|---|---|---|---|---|---|---|---|
| ① Accuracy | High | High | High | Medium-Low | Medium | Medium-Low | Low |
| ② Cost | High | High | Medium | Low | Medium | Medium | Medium |
| ③ Device Req | Camera | Camera | Scanner | Scanner | Micro phone | Camera | Optical pen, touch panel |
| | | | | | Telephone | | |
| ④ Social Acceptability | Medium-Low | Low | Medium | High | High | High | High |
| ⑤ Reliability | Very high | Very high | High | High | High | High | High |
| ⑥ Easiness of use | Average | Low | High | High | High | High | High |
| ⑦ Attacks precaution | Very high | Very high | High | High | Average | Average | Average |
| ⑧ Stability | High | High | High | Average | Average | Average | Average |
| ⑨ Acceptance | Average | Average | Average | High | High | High | Very high |
| ⑩ Identification and Authentication | Both | Both | Both | Authentication | Authentication | Both | Both |
| ⑪ Interference | Glasses | Irritations | Dirtiness injury, roughness | Arthritis, rheumatism | Noise, cold | Scratch, tense | Changable or easy signatures |
| ⑫ Use | Nuclear installation, Medical services | Nuclear installation, medical service | Police, Industrial | General | Remote access banks and database | Police, Industrial | Industrial |

THE END