Choice based

Biometric Technologies and Security

1. Explain why biometrics is Considered more secure than traditional passwords and give simple examples to support your Explanation.

Biometrics is considered more secure than traditional passwords because they are based on who you are, not what you know

Here's the simple breakdown for you

1) Hard to Guess or steal.

Passwords Can be guessed, stolen, leaked or shared But Biometrics cannot be guessed so easily because they are unique to each person.

Example:

- Someone Can guess your passwords linke "Meghu13" or steal it from a note.
- But they cannot steal your fingerprint or Exact fact structure easily

) Always with you

you may forget a pass, but you can't forget your fingerPrint or face.

Example: If you forget your Password, you get get locked out

3) Difficult to ~~[illegible]~~ Duplicate

Creating fake password is easy Creating a fake fingePrint or iris is extremely difficult needs specials tools

) Differentiate between biometric verification and identification

Biometric verification: The system checks if you are the right person. you say who you are -> The system confirms it

Eample: you unlock your Phone with fingerPrint

Phone checks: "Is this my fingerPrint

Biometric identification: The system tries to find out who you are. you don't say your name -> The system searches the database to identify you

3) Explain why the False Non-match Rate (FNMR) is important in Evaluating the

why FNMR is important in BioMetric System

FNMR tell how often the System fails to recognize the right person.

why is this important?

Because a good biometric System should let real user in without trouble.

Simple Example:

4) Describe how a finger Print image is acquires, Explaining each basic Step involved

How a finger Print image is captured:

1. Finger Placement - You place your finger on a scanner Surface

2. Ligh or electrical Signal - The device Shines light or Sends an electrical Signal to read the ridges

3. Ridge detection: • Ridges reflect light or criate Strong Signals.

   • Valleys absorb light or give weak Signals.

4. Sensor Converts it to digital - The scanner turns these signals into a digital image.

5. Image cleaning - The system removes noise, enhances clarity, and sharpens the ridges.

6. Final fingerprint image - A clean fingerprint Pattern is produced and saved for use

2) Explain One major weakness of fingerPrint biometrics and describe how it affects user authentication

One major weakness:

Fingerprint biometrics Can be spoofed

How it affects authentication:

If someone uses a fake fingerPrint made from gel, silicone, or a copied Print they might unlock the device or system without Permission, reducing security.

3) why do layered biometric system improve security ? Explain with a suitable Example.

Layered biometric system use more than one biometric This makes security stronger because even if one biometric is fooled, the other one still protects the system.

Example:

Your phone asks for finger Print + face unlock. Even if someone copies your fingerprint, they still can't get in without your face. So the system becomes much harder to hack.

7. Explain the role of minutiae points in fingerprint matching and describe how they help in identifying a person.

Role of minutiae points:

minutiae points are the tiny special details in a fingerPrints like where a ridge ends or splits. These points are unique for every Person

How they help identify a Person:

The system compares the location and pattern of these minutiae points in the scanned fingerprint with the stored fingerprint.

If enough Points match, the system says it is the same Person.

8. Explain how failure to Enroll affects the overall Performance of a biometric System and give possible reasons for these failures.

How FTE affects Performance:

Failure to Enroll (FTE) means the system cannot capture or register a user's biometric during enrollment. This reduces the system's overall Performance because some cannot use the biometric system at all, making it less reliable and less convinient.

Reasons for FTE:

- Poor quality fingerprints
- Dry or wet fingers.
- Sensor Problems or low-quality scanners
- user not placing finger correctly
- Environmental issues

9) Compare any two fingerprint recognition algorithm and explain how they differ in their working.

1. Minutiae - based Algorithm

How it works:

- looks at small details.
- Compares the Position and direction

9. Pattern-based Algorithm

How it works:

- Looks at the overall pattern of the fingerprint
- Compares the global structure, not tiny details.

Key idea:

matches fingerprint based on overall shape and flow.

10. How fingerprint features are extracted:

1. Clean the image - The system removes noise and makes the ridges clearer.
- Find the ridges and valleys - it identifies the dark ridges and light spaces.
- Detect Minutia points - The ~~po~~ system finds important features like
  - ridge endings.
  - bifurcations (splits)
- Convert them ~~it~~ into data - Their positions and directions are turned into digital points

1. Evaluate the reliability of biometric systems using different accuracy metrics and Explain why they are needed.

important accuracy metrics:

1. False Match rate (FMR)
   - How often the system accepts the wrong Person, Low FMR = more secure.
2. False non-Match Rate (FNMR)
   - How often the system rejects the Correct Person.
   - Low FNMR = more use friendly.
3. Failure to Enroll (FTE)
   - How often the System cannot register a user's biometric.
   - Low FTE = more reliable.
4. Equal Error rate (EER)
   - Point where FMR and FNMR are equal
   - Lower EER = better overall accuracy.

12. Analyze why fingerprint recognition system may fail in real world environments and provide suitable examples.

Reasons and examples:

1. Dirty, wet or oily fingers.
   - Example: After eating oily foods, the scanner can't read ridges properly
2. Dry or cracked skin.
   - Example: In winter, dry fingers may not produce a clear print.
3. Damaged fingerprints:
   - Example: A worker with cuts or burns on fingers may fail to authenticate.
4. Dirty or scratched sensors:
   - Example: A phone fingerprint scanner with dust or scratches gives error.
5. Environmental conditions:
   - Example: Humiditity or rain can make the sensor misread the fingerprint

13. Justify the need for layered biometric solutions

Layered biometric solutions are needed in high security areas because one biometric alone is not enough to stop advanced attacks.

Pratical reasons:

1. Harder to spoof.
   - even if someone fakes a fingerprint they still need face or iris to get in.
2. Stronger identity Proof.
   - Two or more biometrics confirms the Person more accurately, reducing mistakes
3. Protection against sensor failure.
   - If the fingerprint scanner fails, the system can still use face or iris
4. Stop insider attacks.
   - Employees cannot simply share Passwords, they must Pass multiple biometric checks.

4. How the false Match rate (FMR) affects the security of a biometric system and explain its real-world impact.

:. False Match Rate tells how often a biometric system accepts the wrong Person.

How FMR affects security

- A high FMR means the system can be fooled easily.
- unauthorised people might get access because the system thinks they are real users.

Real-world impact:

- A stranger might unlock someone's phe if the fingerPrint scanner wrongly matches.
- In a high security lab, a high FMR could let an unauthorised Person enter a restricted area.

Propose a simple improvement that can increase the accuracy of fingerPrint.

Improvements ~~them~~:

use enhanced image Processing

How it helps:

- Remove noise, blur, and smudges.
- Makes ridges and valleys clearer.
- allow the system to extract minutiae Points more accurately.
- Leads to better matching and fewer mistakes

27/11