BRAINWARE UNIVERSITY

Term End Examination 2023-2024
Programme – M.Sc.(ANCS)-2022
Course Name – Biometric Security
Course Code - MNCS304B
(Semester III)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) Select the reason why combining biometric authentication with OTPs is considered a strong security practice.

a) It prevents the need for biometric enrollment.
b) It ensures that users don't need to remember passwords.
c) It speeds up the authentication process.
d) It adds two distinct and independent layers of verification.

(ii) Test the reason why OTPs are effective for security in biometric authentication.

a) OTPs are permanent codes linked to the user\'s biometric data
b) OTPs are time-sensitive and valid only for a short duration
c) OTPs can be used across multiple authentication sessions
d) OTPs are stored on the user\'s device for easy access

(iii) In a biometric 2FA system with OTPs, test the step comes after successful biometric authentication.

a) User account creation
b) One-Time Password generation
c) Capturing additional biometric data
d) User identity verification through email

(iv) Predict that the biometric security with OTPs that helps to mitigate the risk of data breaches.

a) It encrypts biometric data during transmission
b) It prevents unauthorized access through biometric cloning
c) It allows unlimited login attempts with OTPs
d) It stores biometric data in public databases

(v) Decide the strength of signature-scan technology.

a) Resistance to imposters
b) Requirement for specialized devices
c) Inconsistent signatures
d) Limited applications

(vi) Recognize the reason for selecting a biometric system.

a) Accuracy
b) Acceptability
c) Cost effectiveness
d) All of the above

(vii) Memorize FNMR in biometric system.

a) False Non-Matrix Rate
b) False Not-Matrix Rate
c) False Non-Manipulative Rate
d) None of the above

(viii) Recognize FMR In Biometric system.

a) False Multipication Rate
b) False Match Rate
c) Failure-to-Match Rate
d) None of the above

(ix) In Eigenfaces, select the vast majority of faces can be reconstructed by locating distinctive features from approximately _____

a) 75-100
b) 100-125
c) 100-150
d) 75-150

(x) In kiosk system, identify accurate distance for scanning is _____

a) 1-2 feet
b) 2-3 feet
c) 3-4 feet
d) None of the above

(xi) Identify biometrics is used for _____ a person.

a) authenticating
b) authorizing
c) a and b
d) None of the above

(xii) Which one of the following is not finger-scan technology? Identify the correct one.

a) Optical technology
b) Silicon technology
c) Radio-wave technology
d) Ultrasound technology

(xiii) Predict applications of biometric security.

a) Mobile access and authentication
b) accessing building
c) banking
d) All of the above

(xiv) The comparison between biometric templates is rendered as _____ Choose the correct one.

a) score
b) confidence level
c) a and b
d) None of the above

(xv) A user's template will be incorrectly judged to be a match for a different user's template, which is discovered from_____

a) False Non-Match Rate
b) False Match Rate
c) Failure-to-Enroll Rate
d) None of the above

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Define the advantages of voice scanning. (3)
3. Define a unique characteristic of a keystroke scan (3)
4. Summarize what Identity Verification Capabilities Should Your System Have? (3)
5. Judge fingerprint scans a widely adopted biometric authentication method (3)
6. How does a retina scan contribute to biometric security? Prepare (3)

OR

Explain about voice scan (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Evaluate the strengths of facial recognition technology and its versatility in applications, despite certain weaknesses. (5)
8. Estimate the strengths of iris recognition technology, particularly its high accuracy and stability of characteristics over time. (5)
9. Summarize the limitations and challenges associated with iris recognition, and how do these affect its deployment in various applications? (5)
10. Define the working principal of finger-scan technology. (5)
11. Describe the features of a finger in detail. (5)

12. Judge the potential future growth areas for iris recognition technology and its current applications, such as in physical access and network security. (5)

OR

Justify the concept of Two-Factor Authentication (2FA) in detail. Discuss its significance in enhancing security and provide examples of where it is commonly used. (5)

****