BIRZEIT UNIVERSITY

Faculty of Engineering and Technology

Computer Science Department

COMP432 – COMPUTER SECURITY

Authentication using Biometric

	Students Name	Students Number
1	Yousef Sharbi	1202057
2	Mahmoud Duhaidi	1200340
3	Anas Karakra	1200467

Abstract:

Authentication using biometric technologies is automated methods of verifying or recognizing the identity of a living person, based on physiological (unchangeable) or behavioral, which offers a convenient and secure way to verify a user's identity using their unique biometric, and this topic has gained Increasingly popular due to the need for secure and user-friendly authentication methods. However, it faces limitations such as privacy concerns, spoofing attacks, and high implementation costs. Potential solutions include advanced encryption, multimodal biometric systems, and continuous authentication techniques.

Introduction:

Cybersecurity technologies designed to protects information of networks, devices, programs, and data from unauthorized access, disclosure, damage, attack.

Biometric authentication is a subset of cybersecurity focusing on verifying identities through biological like physiological (finger print) or behavioral (gait), which this method offers higher security compared to traditional authentication like password.

- ## Key Aspects and Relevance:

1. **Uniqueness**: Biometrics are unique to individuals, making them difficult to stole, which prevent unauthorized access.

2. **Convenience**: Biometrics eliminate the need to remember passwords.

3. **Security**: Enhanced security through multi-factor authentication combining biometrics with other methods (phone-based banking: PIN, voice).

Background:

Biometric authentication systems rely on unique biological characteristics like fingerprints, iris scans, or facial recognition. These systems capture the user's biometric data, create a digital template, and store it securely. During authentication, the system compares the newly captured biometric data with the stored template.

Key Concepts and Technologies:

- **Fingerprint Recognition**: Analyzes unique patterns on fingertips.
- **Iris Recognition**: Identifies individuals based on iris patterns.
- **Facial Recognition**: Matches facial features with a stored template.
- **Voice Recognition**: Compares voice characteristics for verification.

Research Papers:

Paper Title	Authors	Year	Key Points	Our Opinion
Liveness Detection in Iris Recognition Systems	Ma et al	2018	Discusses methods to prevent iris spoofing attacks	best for enhancing iris recognition security.
A Survey of Gait Recognition Techniques	Zhang et al	2019	Reviews various gait recognition techniques	good approach for behavioral biometric authentication.

Motivation and Research Questions:

- Motivated Points to Search in This Area:

  1. Need for more secure authentication methods.

  2. Biometric authentication offers convenience and security advantages, which improve user experience.

  3. Need to address limitations and explore potential solutions.

- Main Questions:

  1. What are the current limitations of biometric authentication?

  2. How can biometric systems be improved to enhance security?

  3. What are the Potential solutions of biometric authentication?

Threats and Risks:

Spoofing Attacks: Fake biometric used to gain unauthorized access, and these threats can be detected by Implementing liveness detection techniques.

Privacy Issues: Unauthorized use or leakage of biometric data, and these threats can be detected by regularly updating biometric templates.

False Positives/Negatives: Incorrectly granting or denying access, and these threats can be detected by monitoring for unusual access patterns.

Non-Repudiation: Difficulty in proving someone didn't perform an action, and these threats can be detected by Implementing robust liveness detection techniques and continuous monitoring for unusual access patterns.

Countermeasures and Best Practices:

- Multimodal Biometric Authentication: Combining multiple biometric factors (fingerprint + iris scan) for authentication.

- Robust Template Protection: Using encryption techniques to secure biometric templates.

- User Education: Informing users about proper use and risks.

- Liveness Detection: Verifying user presence during authentication.

- Regular Audits: Conducting regular security audits of biometric systems.

Future Trends and Challenges:

- Emerging Biometrics: Integration of gait analysis, voice recognition, and others.
- Continuous Authentication: Verifying user identity throughout a session using behavioral biometrics (key stroke, mouse movement).
- Regulation and Standardization: Developing clear regulations for data collection, storage, and use.
- User Acceptance: Balancing security with user convenience and privacy concerns.
- AI and Machine Learning: Improving accuracy and reducing false positives/negatives.
- Wearable Biometrics: Integrating biometric sensors into wearable devices.

Conclusion:

Biometric authentication offers a secure and convenient solution for user identification, However, addressing limitations like spoofing attacks and privacy concerns is crucial. By implementing countermeasures and embracing future trends, Biometric authentication can be an important part of a strong cybersecurity system.

References:

- Ma et al, "Liveness Detection in Iris Recognition Systems," 2018.
- Zhang et al, "A Survey of Gait Recognition Techniques," 2019.