e-ISSN 2320 –7876 www.ijfans.org
Vol.11, Iss.11, 2022
Research Paper **UGC CARE Listed (Group -I) Journal**

An Overview on Biometric Authentication

DR. KULDEEP PANWAR1, MR. VIPUL NEGI2, MR. SANJAY GAHTORI3

1Associate Professor, Department of Mechanical Engineering, Shivalik College of Engineering, Dehradun

2Assistant Professor, College of Pharmacy, Shivalik, Dehradun
3Assistant Professor Shivalik Institute of Professional Studies, Dehradun

Drkuldeep.panwar@sce.org.in

ABSTRACT: ***The words "bio" (life) and "matron" are the origin of the phrase "biometrics" (measurement). As a consequence, it involves measuring a user's distinctive traits in order to identify or authenticate them. By using the user's distinctive traits, such as a fingerprint scan, facial imaging, signature, or voice recognition, biometric identification verifies a user's identity to sign in to an account or get access to personal information. We currently witness a lot of cases of cybercrime, data breaches, data manipulation by unauthenticated individuals, hacking of personal accounts, and so forth since traditional password-based security techniques are hackable. In order to address these security concerns, a more secure system is necessary. Biometric authentication technology offers a different approach that cannot be circumvented because it uses software to identify or validate the user by comparing the data being fed with digital images of the user's distinctive characteristics. This information can't be copied or hacked, therefore it increases identification accuracy.***

KEYWORDS: Authentication, Biometric Authentication,Biometrics, Iris, Retina.

1. INTRODUCTION

The user's identification is confirmed if they have previously registered or if their data is already stored in the system software. The user is verified and given access to or a sign-in in this situation when the user's input data is compared to previously provide input data, such as a physiological or behavioural feature. When a user registers for the first time and is not previously logged in, their personal data is entered into the software and saved for later access [1]–[4]. In the following respects, this technique is more trustworthy than a standard PIN or any other identity- or document-based system:

- No identification card is required, and no passwords or login-ids must be remembered.
- The individual in question must be present at the specified time and location; the system has a one-to-one interface, making it more secure.
- Identification systems based on biometric authentication may be divided into two categories:
  a. Behavioral characteristics
  b. Physiological characteristic

The categorization of Biometric Traits is shown in Figure 1.

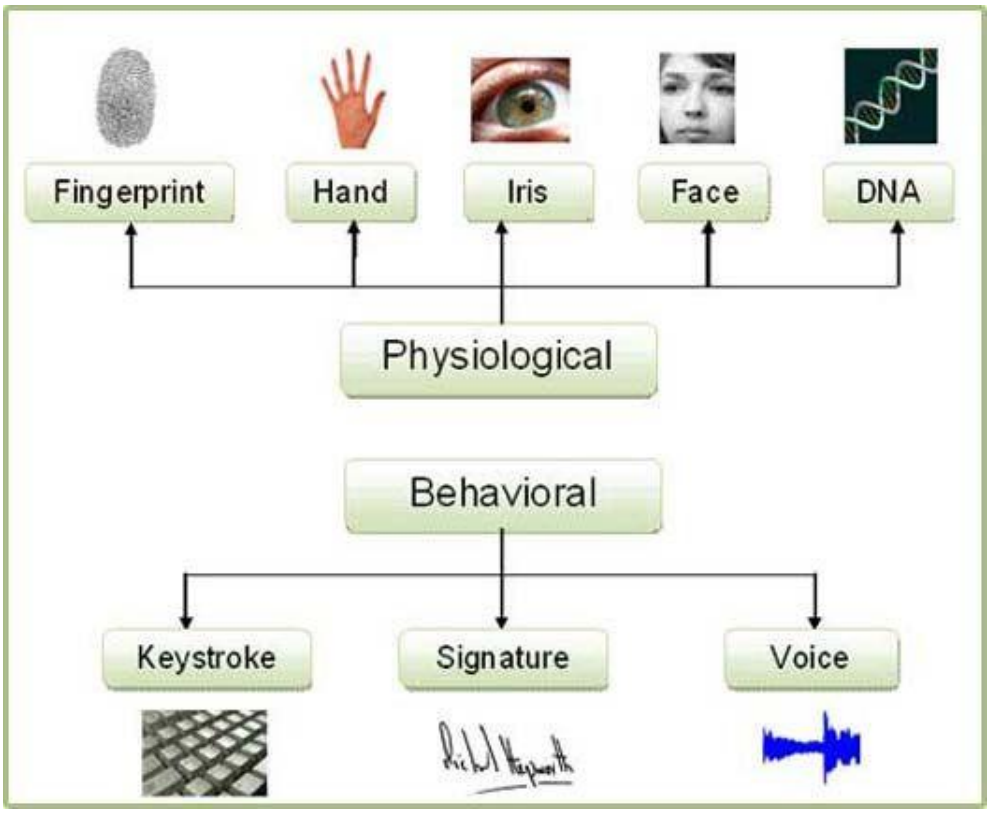

Figure 1: Illustrates the classification of Biometric Traits[5]

1.1. Fingerprints Identification:

It is the most often utilized biometric feature. The digital imaging of fingerprints is done using this technique. It examines the human finger's friction ridge skin imprint. The sensor detects the distinctive curves and bifurcations of a finger's skin. Palm scanning is the same way.

Scanningof Eye:

There are two methods for eye recognition:

- *Retina Scanning:*

The user must gaze into a gadget that uses lasers to scan his retina. The gadget examines the user's blood vascular arrangement. A person's blood vessel structure is unique. It is challenging because the user must fix a spot while the laser analyzes his eye.

- *Scanning of Iris:*

In contrast to retinal scanning, the individual does not need to be near the instrument. A camera is used to do the imaging in this case. A video-based imaging technology is used to acquire the iris patterns. The gadget analyzes the picture it has acquired. The picture includes 266 distinct spots, each of which is based on iris characteristics such as furrows and rings. The iris remains constant throughout one's life. There is no need to update the picture on a regular basis.

1.2. Recognitionof Face:

A high-resolution basic camera or a web camera is utilized for facial recognition. In visible light, facial recognition gets characteristics from the center part of the face picture. These features remain constant throughout time. Hairs, facial expressions, and other superficial characteristics are ignored. The representation is compared to the database, and if they match, the user is verified.

1.3. Imaging of Handprints:

The image of a user's hand is scanned in this technique. Digital signal processing techniques are used to extract and store characteristics such as the distance between fingers, the length of digits, and the length of the hand. Templates have been created. These templates are used to verify the features. Optical scanners are used to scan hand geometry[6]–[8].

1.4. Recognition of palm prints:

For recognition, features such as minutiae, ridges, principal lines, folds, orientation, and vein geometry are extracted. Vein geometry differs from one person to the next. The hand is put on the screen for identification, and the veins are scanned with infrared light. It takes a picture of your hand and extracts a vein pattern, which is a bright and dark pattern. Infrared light is absorbed by the veins of the hand, resulting in a darker pattern. The gadget saves a template of this biological pattern. Transducer converts this picture to a digital image for matching and comparing purposes.

1.5. Analysis of DNA:

In most criminal instances, this kind of verification is utilized. For confirmation, the user's DNA is obtained in the form of tissue, hair, blood, and nails. It takes time to analyze DNA. Although DNA is a unique trait, a hair or a nail may be taken.

1.6. Verification by voice:

When using voice verification, the user is required to utter a word or a secret code. His voice characteristics are evaluated, both physiologically and otherwise. The voice recognition process is different from the verification process. However, the selection method is more of a one to one or one too many operation. In the verification step, a sample of speaking style pattern is kept and compared to the speech of the same individual. The verification system has been trained to distinguish the voice of a certain speaker.

1.7. Scanning Signatures:

It is a dynamic analysis of the shape, size, speed, and pressure of the user's hand as they sign the document, among other factors. A signature can be copied, but the traits shown while signing cannot.

1.8. Keystroke:

It is essentially the manner in which the key is pressed. The time spent pressing the key, the time spent releasing it, and the sound produced when pressing and releasing it are all quantifiable characteristics. The method of Biometric operation is shown in Figure 2.

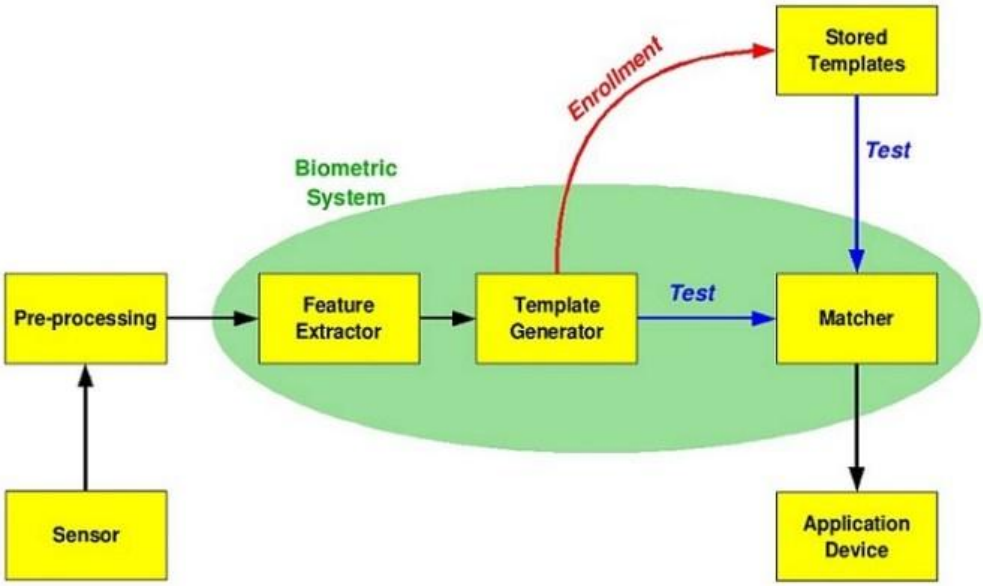

Figure 2: Illustrates the mechanism of Biometric operation[9]

Advantages:

- There is no need to memorize passwords or login IDs.
- A better way to save time and resources.
- Only authorized users have access to personal information or accounts.
- There will be no need to carry any approved papers.

Disadvantages:

- For physically challenged individuals, several of these techniques are restrictive.
- Changes in the quantity of light entering the eye as a result of pupil constriction may cause system errors.
- DNA analysis takes time, and retina scanning necessitates the purchase of an expensive equipment.
- With time and age, certain features of the face or palm may alter.

2. LITERARTURE REVIEW

A.Alhayajneh et al. discussed about Biometric authentication and verification[10].A network of wirelessly connected sensing and actuating devices is known as a Wireless Body Area Network (WBAN). WBANs that are used to disperse medication and gather biometric data are regarded as components of a Cyber Physical System (CPS). WBANs present the concept of utilizing biometric readings as a method for authentication, with the goal of maintaining user security and privacy. The different methods have all been well researched. This article aims to examine and assess the most widely used biometric authentication methods in terms of accuracy, cost, and

implementation practicality. We propose a number of authentication methods that take into account a variety of biometric characteristics.

Simon Fong et al. discussed a hand motion biometric authentication paradigm [2].The author introduces a novel hand biometric authentication method based on measurements of the user's stationary hand motion during hand sign language. Hand motions may be tracked sequentially using a cheap video camera. These hand signals could be coupled to other contextual information that might be used in biometric identification. A signer may encode a biometric password using a sequence of hand signals, such as I l, o, v, e, and u, rather than typing in the password "iloveu," which is relatively vulnerable over a communication network. Then, naturally fuzzy properties of the hand gesture photographs are extracted, allowing a classification model to assess if the signer is who he claimed to be by observing the form and posture of his hands while making those signs.

In sign language, it is believed that, similar to how different hand shape compositions do, everyone has a few modest yet distinctive behavioural qualities. In order to identify hand signs, numerous popular machine learning methods are integrated with simple and effective image processing techniques including intensity profiling, colour histograms, and dimensionality analysis. Computer simulation is used to examine the efficacy of this novel biometric authentication model, which has a recognition accuracy of up to 93.75 percent.

3. DISCUSSION

Biometrics is a term that refers to biological measures or physical traits that may be used to identify people. It is utilized in systems that employ fingerprints for identification, such as national identity cards and health insurance schemes. Biometrics, such as iris recognition, is sometimes used in this area. Fingerprint scanners and facial recognition, which are widely used on contemporary gadgets, are examples of biometric technology that are usually regarded the safest way of protecting accounts and devices. Biometric technology has a number of drawbacks, including costs, data breaches, tracking, and data. The author covers biometric technologies, kinds, and biometric characteristics in this article. Biometric technology has a promising future since it can be used for verification and authentication.

4. CONCLUSION

The words "bio" (life) and "matron" are the origin of the phrase "biometrics" (measurement). As a consequence, it involves measuring a user's distinctive traits in order to identify or authenticate them. By using the user's distinctive traits, such as a fingerprint scan, facial imaging, signature, or voice recognition, biometric identification verifies a user's identity to sign in to an account or get access to personal information. The biometric system may be used for identification verification, security purposes, and attendance tracking, among other things, and it may have many more applications in the future. The existing systems will be improved and changed to provide a secure, error-free system. For an effective security system, accuracy levels must be improved. The need must be taken into account while selecting a method. Scientific research is being carried out in the biometrics field for future applications and development.

REFERENCES:

[1] E. Pagnin and A. Mitrokotsa, “Privacy-Preserving Biometric Authentication: Challenges and Directions,” *Security and*

Communication Networks. 2017.

[2] S. Fong, Y. Zhuang, I. Fister, and I. Fister, "A biometric authentication model using hand gesture images," *Biomed. Eng. Online*, 2013.

[3] K. Zhou and J. Ren, "PassBio: Privacy-preserving user-centric biometric authentication," *IEEE Trans. Inf. Forensics Secur.*, 2018.

[4] A. Wójtowicz and K. Joachimiak, "Model for adaptable context-based biometric authentication for mobile devices," *Pers. Ubiquitous Comput.*, 2016.

[5] "bdf21422d36ae0508340866877c33051." .

[6] J. J. Kim and S. P. Hong, "Design of a secure biometric authentication framework using PKI and FIDO in fintech environments," *Int. J. Secur. its Appl.*, 2016.

[7] A. C. Weaver, "Biometric authentication," *Computer (Long. Beach. Calif).*, 2006.

[8] C. H. Lin, J. C. Liu, and K. Y. Lee, "On neural networks for biometric authentication based on keystroke dynamics," *Sensors Mater.*, 2018.

[9] "Biometric-authentication-process." .

[10] A. Alhayajneh, A. N. Baccarini, G. M. Weiss, T. Hayajneh, and A. Farajidavar, "Biometric authentication and verification for medical cyber physical systems," *Electron.*, 2018.