iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

FROM PASSWORDS TO PRINTS: THE TRANSFORMATIVE JOURNEY OF BIOMETRICS IN DIGITAL TRANSACTIONS

Aditya Bhadouria[1], Priyanshi Nileshbhai Ghoghari[2], Heer Chirag Parikh[3], Aryan Yadav[4], Shivam Patel[5], Kiran R Dodiya[6], Akash Khunt[7], Divya Patel[8]

[1,2,3,5] M.sc Cyber Security, NSIT- IFSCS (Affiliated TO NFSU), Jetalpur, Ahmedabad, Gujarat, India
[4] M.Sc. Cybersecurity, National Forensics Science University, Ponda, Goa, India
[6.] Assistant Professor & Program Coordinator of DFIS (Cyber Security &Digital Forensics) NSIT-IFSCS Jetalpur, Ahmedabad. (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India.
[7.] Assistant Professor & Program Coordinator of Cyber Security (Cyber Security & Digital Forensics) NSIT-IFSCS Jetalpur, Ahmedabad (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India
[8.] Assistant Professor & Course Co-Ordinator of DFIS (Cyber Security & Digital Forensics) NSIT-IFSCS, Jetalpur, Ahmedabad (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India.

ABSTRACT
A person is automatically verified using biometric features derived from their biological and behavioral traits. This process is known as biometric verification. Compared to traditional systems that use a card or password, a biometric verification system can reliably distinguish between an authorized person and an imposter. People could be recognized using biometrics based on who they are rather than what they have (such as an ID card) or what they know (password). ATMs, computers, security systems, mobile phones, credit cards, and health and social services currently use biometrics. An unimodal biometric system must deal with several issues, so multimodal biometrics is the way of the future in this field. This paper will present a survey of some unimodal biometrics currently in use across various environments, those still in limited use, those still being developed, or those still in the research stage.

Keywords:
Verification, Identification, and Recognition in biometrics, unit and multi-modal biometrics.

1.INTRODUCTION

1.1 What is an Electronic Transaction?

An electronic transaction is a digital exchange of goods, services, and information between entities using computer-mediated networks, the Internet, or private networks. These transactions include buying or shopping over the Internet, banking services, access to governmental services, and other business-to-business exchanges. Transactions occur between a person and businesses, governments, and other organizations to improve procedures and accelerate fast transactions. Nowadays, Electronic transactions are one of the most fundamental parts of any modern economy worldwide, providing secure, convenient, and instantaneous services.[1].

1.2 What is biometric?

Biometric authentication, therefore, is the process through which unique physical or behavioral characteristics verify an individual's identity. Each has a uniqueness- everything from fingerprints and facial recognition to iris patterns, voice, or even behavioral patterns like typing, rhythm, or gait. These are taken, stored, and used as identification to grant or restrict access to systems, devices, or services. It links identity verification with who a person is, rather than what he knows in the form of passwords or what he possesses in the form of cards or tokens. With an ever-increasing reliance on digital transactions and secure systems, biometrics have extensively entered numerous sectors. With biometric security, the human body becomes the

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

"key" to authentication- both convenient and safe. Unlocking a smartphone, gaining entry to a secure facility, or making an electronic transaction can be easily done using biometrics to smoothly and highly reliably process the activity.[2].

1.3 What is a Biometric Scanner?

A biometric scanner is a hardware tool that captures and stores an individual's biometric data, including fingerprints, facial features, or iris patterns. Such scanners analyze the data taken compared to the available, already stored biometric templates within a secure database. Access will be granted if the scanned biometric matches the available data; otherwise, it will be denied. Biometric scanners are found in many applications- from security systems to border control, as well as consumer electronics such as smartphones and ATMs. Using biometric scanners ensures fast, efficient, and highly secure access control in personal and professional environments.[3].

1.4 Why are Biometrics Widely Used?

Biometric authentication offers many essential advantages over traditional methods of security, hence providing a preferred solution for most industries:

Practicality: Unlike passwords or security tokens that may get lost, forgotten, or stolen, biometric features are always associated with the user. Thus, access can be granted seamlessly without having to remember complicated credentials.

Security: Since biometric features are highly exclusive to individuality, they are difficult to duplicate or steal. While passwords can be hacked, and cards can be cloned or lost, biometric authentication systems offer security against impersonation or unauthorized access.

Greater Accuracy: Biometric systems can accurately and appropriately distinguish between an accepted user and an imposter. This makes biometric authentication helpful in high-security environments like government offices, banks, and other critical infrastructure locations.[4].

2 LITERATURE REVIEW:

2.1 History of Biometric System:

While the earliest accounts of biometrics date back to 500 BC in the Babylonian empire, the first record of a biometric identification system was in the 1800s in Paris, France. Alphonse Bertillon devised a method for categorizing and comparing criminals based on specific body measurements. Even though this system was far from ideal, it was the first to show that using distinctive biological traits to authenticate identity was possible. Fingerprinting emerged in the 1880s as a means of contract signature and criminal identification. A fingerprint was understood to be a representation of an individual's identity and to have legal significance.[5].

There is debate over who created fingerprint identification, but Edward Henry is given the invention credit. Biometrics grew exponentially as a research field over the next century. There were so many advances in the 1900s that it would be impossible to list them all, so here are some of the highlights from the second half of the century:

Semi-automated facial recognition methods were developed in the 1960s. These methods required administrators to analyze facial features within an image and extract usable feature points. They are much more manual than the ones we have for opening phones.

By 1969, fingerprint and facial recognition had become so common in law enforcement that the FBI allocated funds to develop automated processes. This sparked the development of more advanced biometric capture and data extraction sensors.[6].

The National Institute of Standards and Technology established a Speech group in the 1980s to study and advance the processes for speech recognition technology. These studies laid the foundation for today's voice command and recognition systems.

The idea that irises, like fingerprints, were unique to everyone was proposed in 1985, and the first iris recognition algorithm was patented in 1994. Furthermore, it was discovered that blood vessel patterns in the eyes were unique to everyone and could be used for authentication [7].

2.2 What are the stats of biometrics nowadays?

Biometric technology research has advanced rapidly in the last decade alone. Biometrics has progressed from a novelty technology to an everyday part of life. Apple added fingerprint recognition to the iPhone in 2013, ushering in the widespread acceptance of biometric authentication. Most mobile phones nowadays have biometric capabilities, and many apps use biometrics to authenticate everyday

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

functions. Biometrics is now so popular that it is used to secure electronic payments. It's becoming old-fashioned to pay with cash; the most secure way of transaction today is using biometric payment methods like Google Pay, Amazon Pay, Apple Pay, etc.[8].

NO	Key Focus	Methodologies/Technologies	Applications/Use Cases	Challenges/Limitations	Data sets
1	Soft Biometrics for Border Security	Multi-channel soft biometrics framework with sub-components, namely ApparelNet, A-Net, OneDetect, RSFS	Border control authentication, crowd monitoring, fashion world, e-learning	Intrusiveness, latency, tampering, privacy	FVG, PETA, MMV Pedestrian
2	Fingerprint Fragment Recognition	Fingerprint feature analysis Level 2 and Level 3	Fragmented fingerprint recognition in security systems	Potential for recognition from small-area fragments	-
3	KNN Algorithm in Facial Recognition	Application of KNN algorithm, feature extraction, distance metrics, optimization strategies	Security systems, identity verification, human-computer interaction.	Computational complexity, sensitivity to parameters	-
4	Unimodal Biometrics Systems	Survey of various unimodal biometric technologies in different environments	ATMs, computers, security installations, mobile phones, health services	Reliability, fraud, limitations of unimodal systems	-
5	Fraud Prevention in Insurance Using Biometrics and AI	Integration of biometric verification with AI-based risk assessment	Insurance fraud prevention	Fraud sophistication, implementation complexity	-
6	Deep Learning in Biometric Recognition	A comprehensive survey of deep learning applications in biometrics (face, fingerprint, iris, etc.)	Cellphone authentication, airport security, general biometric recognition	Model complexity, data requirements	More than 150 datasets and benchmarks
7	Fundamentals of Biometric Identification	Comparative analysis of biometric technologies, multibiometrics, and fusion	Biometric authentication systems, commercial applications	Qualitative comparison of biometric types, commercial landscape	-
8	Challenges in Biometric Systems	Overview of critical issues: recognition performance, security, bias, fairness, and privacy	General biometric recognition systems	Security attacks (spoof, adversarial, template), bias, user trust	-
9	Security and Privacy in Biometric Systems	Review of security and privacy concerns in biometrics, design of secure authentication protocols	eCommerce, banking, healthcare	Privacy issues, threat of compromised traits	-
10	Multi-factor Authentication	OTP and biometric-based multi-factor authentication	E-government services	Password vulnerabilities need for robust security	Explore unified

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

	for E-Government Services	scheme			authentication mechanisms for public services

Tabel 1: Literature Review

3 TYPES OF BIOMETRICS SYSTEMS:

1. Fingerprint

A fingerprint identification system searches for specific characteristics in the line pattern on the surface of the finger. The bifurcations, ridge endings, and islands comprising this line pattern are saved as images.[9].

2. By face

To find a match, a facial recognition system examines the position and shape of several facial features. Other times, surface characteristics like the skin are considered.[10].

3. By Iris

When an iris scan is performed, a scanner reads out the unique characteristics of an iris, which are then converted into an encrypted code. Iris scanning is an excellent security technique, especially if it is performed using infrared light.

4. By Finger Vein Pattern

In Vein pattern recognition, the veins' ending points and bifurcations in the finger are captured as an image, processed, and converted into an encrypted code. This method, combined with the fact that veins are found beneath the skin's surface rather than on its surface, makes this technique more secure than fingerprint-based identification and faster and more convenient for the user. It is a more costly method[11].

5. By Palm Vein Pattern

This method is also based on identifying distinct vein patterns. However, it is simpler and more secure because more reference points are used than in finger vein pattern recognition. Along with iris scanning, this technology, which cannot be copied (or only with extreme difficulty), is currently regarded as the best method in biometric security. Palm scanning is quick and precise, providing high user convenience.[12].

6. By Ear Shaping

Ear shape biometrics uses specialized headphones and inaudible sound waves to measure the acoustics of the ear, unlike many other biometric modalities that require special cameras to take measurements. Each earphone contains a microphone that records sound waves as they bounce off the distinct curves of the ear canal and reflect from the ear canal in various directions. A biometric template is created from a digital representation of the ear shape for future use.[13].

7. By Voice Recognition

Technology for voice recognition falls under the biological and behavioral biometric categories. The physical structure of a person's vocal tract, which includes the nose, mouth, and larynx, affects the sound. In terms of behavior, each person differs in how they speak, including their pace, tone, accent, and body language. A precise vocal signature is produced by combining information from physical and behavioral biometrics, though mismatches due to illness or other factors are possible.[14].

4 METHODOLOGY USED FOR ELECTRONIC TRANSACTION:

4.1 What do you mean by biometric payments or transactions?

A biometric transaction refers to a situation where the payer's identity is confirmed using biometric data or information, such as voice, iris, fingerprint, or facial identification. Such transactions authenticate utilizing an individual's unique biological attributes instead of PINs and passwords. This enhances security, and the chances of fraud are reduced as well. Key Biometric Transactions facts:

Security: Biometric data is a very strong way to prevent unwanted access because it is specific to one individual and cannot be easily reproduced.

Convenience: Biometrics eliminates the hassle of carrying cards or remembering complex passwords.

Common usage: Customers can pay for things using mobile phones, ATMs, or even some retail stores with face recognition or fingerprint identification facilities.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

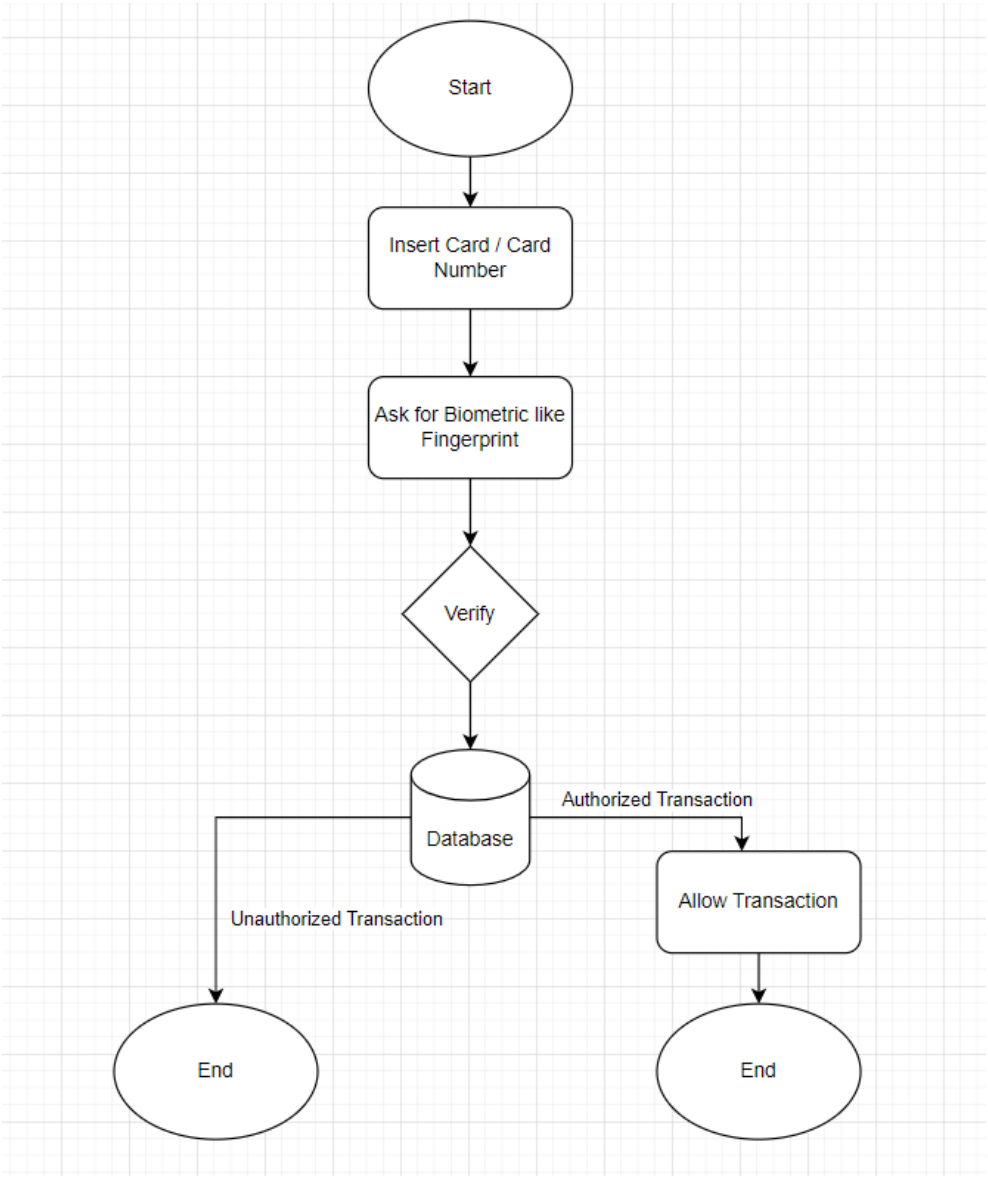

Figure 1: Flow Chart for Electronic Transaction

The flowchart of the biometric payment system includes the lifecycle or the process since its initiation. When customers insert their card or card number, they are asked to provide biometric information, such as fingerprint. The system then verifies by comparing the information with the data stored in its database. The system completes this transaction if the biometric input matches the stored data. If a mismatch or verification fails, the system labels the transaction as unauthorized, so payment is not processed. This pattern uses the security and accuracy of biometrics to allow only authorized users to continue with the transaction process. This type of Transaction is a point-of-sale (POS) technology that uses physical characteristics to identify the user and agree to allow the transaction of data/funds from their account. The most common biometric Transaction is payment done using fingerprint authentication in online payments based on finger scanning.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

5 RESULT:

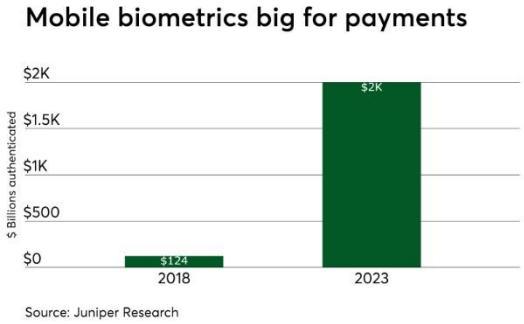

Figure 2: Increment in Biometric Payments

Figure 12 shows that biometric authentication is becoming more common for electronic transactions. The reasons cited for this growth are high security and increased payments over the web. Biometric systems rank among the safest authentication techniques, are reliable, and are proof against fraud, making them the most sought-after way to secure transactions.

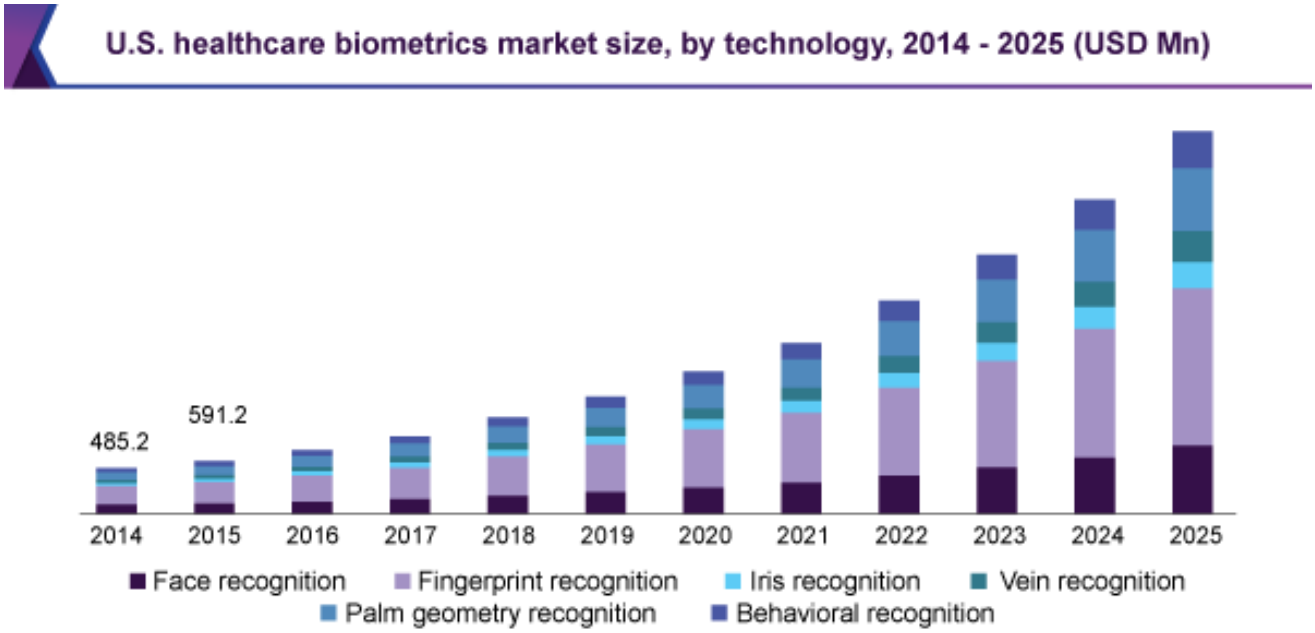

Figure 3: Incrementing of the Biometrics Technology market in Healthcare [13]

As such, from dealing only with health, Figure 13 shows how this biometric technology advances with time and becomes irreplaceable in many industries. Over time, the approach towards health care has become important through biometrics because it aids in patient security, protects patients' data, and allows easy accessibility to health care. This fast growth enables the technology to be accessed publicly; even kids use biometric systems on mobile devices to access authorization and authentication for payment. Biometric authentication has evolved to solve these security concerns better and more reliably. First, starting with fingerprint recognition, it expanded into voice authentication, iris scans, and facial recognition. Biometrics enables further toughening access with access granted based on one's unique biological or behavioral characteristics for authentication purposes. The growing use of smartphones and other mobile devices accelerated the acceptance of biometrics into electronic payments. The latest biometric authentication- anything from fingerprint scanning to Apple's Face ID on iPhones- makes providing a mobile app biometric authorization easy. Users can now safely approve a transaction by tapping a button or glancing at the device

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

screen. In the evolution of digital payment platforms, biometrics is expected to be increasingly integral to ensuring safe, easy transactions worldwide.

6. ANALYSIS:

The evolution of biometrics in electronic transactions is essential for enhancing security against increasingly sophisticated threats. Future fingerprint recognition systems should integrate vein pattern recognition alongside surface fingerprint analysis, creating a dual-layer authentication process far more resilient to spoofing. Similarly, facial recognition technology can be improved by examining the position and shape of facial features and incorporating iris and facial vein mapping. This multifactor approach adds unique identifiers that are difficult to replicate, significantly increasing the accuracy and security of the system. By embracing these advancements, we can create a more secure environment for electronic transactions, effectively mitigating the risks of identity theft and fraud.

7. CONCLUSION:

Every transaction today in such a rapidly changing technological scenario calls for much more security than ever because of sophisticated digital systems and the intricacy that goes along with cyber threats. With the increasing dependence on digital platforms and online transactions, the demand increases to increase security measures further. Biometric security systems are successful, reliable, and secure ways of authenticating users through distinct biological characteristics such as speech patterns, facial recognition, and fingerprints. Although biometric systems reportedly provide good protection today, they remain largely an under-development area with continuous research and development efforts focused on filling recently discovered or emerging weaknesses and enhancing existing capabilities. This evolving revolution will be fully brought to bear for the advanced sophisticatedness, accuracy, and integrity required in biometric technology in the future, advancing in a way that is as user-friendly as possible without compromising security or usability. They will also be more smoothly incorporated into everyday digital interactions. Thus, having been on the trajectory underway, it can be guaranteed that the electronic transactions of tomorrow will be secure enough to be safeguarded by biometric technology. Biometric authentication would thus become a staple of the digital security architecture for an extremely resilient and adaptive defense against new threats as science and technology advance. In the future, biometrics could offer unparalleled levels of security, defending our digital interactions in a world where connectivity is expanding.

REFERENCE:

[1] B. Hassan, H. H. R. Sherazi, M. Ali, and A. K. Bashir, “A multi-channel soft biometrics framework for seamless border crossings,” *EURASIP J Adv Signal Process*, vol. 2023, no. 1, pp. 1–24, Dec. 2023, doi: 10.1186/S13634-023-01026-X/TABLES/2.

[2] K. M. Kryszczuk, P. Morier, and A. Drygajlo, “Study of the distinctiveness of Level 2 and Level 3 features in fragmentary fingerprint comparison,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3087, pp. 124–133, 2004, doi: 10.1007/978-3-540-25976-3_12.

[3] “(PDF) K-Nearest Neighbours (KNN) : A Powerful Approach to Facial Recognition -Methods and Applications.” Accessed: Nov. 10, 2024. [Online]. Available: https://www.researchgate.net/publication/382947916_K-Nearest_Neighbours_KNN_A_Powerful_Approach_to_Facial_Recognition_-Methods_and_Applications

[4] “Jason – Page 2 – Securlinx.” Accessed: Nov. 10, 2024. [Online]. Available: https://securlinx.com/author/securlinxadmin/page/2/

[5] “(PDF) Biometrics Verification: a Literature Survey.” Accessed: Nov. 10, 2024. [Online]. Available: https://www.researchgate.net/publication/327667231_Biometrics_Verification_a_Literature_Survey

[6] “(PDF) Research Paper on Biometrics Security.” Accessed: Nov. 10, 2024. [Online]. Available: https://www.researchgate.net/publication/352508064_Research_Paper_on_Biometrics_Security

[7] “K-Nearest Neighbours (KNN) : A Powerful Approach to Facial Recognition - Methods and Applications.” Accessed: Nov. 10, 2024. [Online]. Available: https://www.jetir.org/view?paper=JETIR1807A61

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[8] S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, "Biometrics recognition using deep learning: a survey," *Artif Intell Rev*, vol. 56, no. 8, pp. 8647–8695, Aug. 2023, doi: 10.1007/S10462-022-10237-X.

[9] R. De Luis-García, C. Alberola-López, O. Aghzout, and J. Ruiz-Alzola, "Biometric identification systems," *Signal Processing*, vol. 83, no. 12, pp. 2539–2557, Dec. 2003, doi: 10.1016/J.SIGPRO.2003.08.001.

[10] A. K. Jain, D. Deb, and J. J. Engelsma, "Biometrics: Trust, but Verify," *IEEE Trans Biom Behav Identity Sci*, vol. 4, no. 3, pp. 303–323, May 2021, doi: 10.1109/TBIOM.2021.3115465.

[11] "5 ways biometrics are going mainstream for payments | PaymentsSource | American Banker." Accessed: Nov. 10, 2024. [Online]. Available: https://www.americanbanker.com/payments/list/5-ways-biometrics-are-going-mainstream-for-payments

[12] G. Singh, G. Bhardwaj, S. V. Singh, and V. Garg, "Biometric identification system: Security and privacy concern," *Artificial Intelligence for a Sustainable Industry 4.0*, pp. 245–264, Oct. 2021, doi: 10.1007/978-3-030-77070-9_15.

[13] "Jason – Page 2 – Securlinx." Accessed: Nov. 10, 2024. [Online]. Available: https://securlinx.com/author/securlinxadmin/page/2/

[14] M. Al Rousan and B. Intrigila, "A Comparative Analysis of Biometrics Types: Literature Review," *Journal of Computer Science*, vol. 16, no. 12, pp. 1778–1788, Dec. 2020, doi: 10.3844/JCSSP.2020.1778.1788.