National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

BIOMETRIC SECURITY

Table of CONTENTS

1. Introduction to Biometric Security
2. Fundamentals of Biometrics
3. Types of Biometric Technologies
4. Integration of Cybersecurity and Biometrics
5. Applications and Case Studies of Biometric Security
6. Challenges and Security Risks
7. Standards, Regulatory Frameworks, and Emerging Ecosystem
8. Benchmarking and Evaluation
9. Future Trends in Biometric Security
10. Conclusion
11. Appendices

Executive Summary

This comprehensive report delves into the world of biometric security, examining its origins, fundamental principles, widespread technologies, integration with cybersecurity frameworks, real-world applications, emerging trends, and the profound challenges posed by privacy, spoofing, and regulatory issues. In recent years, biometric systems—ranging from fingerprint scanners to advanced iris recognition—have transformed from niche concepts to mainstream tools used in smartphones, national ID programs, airport checkpoints, financial services, enterprise access, and beyond. By 2025, and well into the next decade, biometric solutions will likely be at the heart of "passwordless" security strategies, shaped further by artificial intelligence, decentralized computing models, and continuous user authentication paradigms. This report provides a structured exploration of these topics, offering both technical depth and executive-level perspectives for stakeholders evaluating or deploying biometric security in their organizations.

1.

Introduction

Biometric security is an authentication method which uses unique human characteristics, commonly called **“something you are”**, to verify identities. Traditionally, authentication was done using passwords or PINs, otherwise known as **“something you know.”** Later, they were supplemented with items, e.g. key fob, smart card, which were **“something you have.”** Biometrics draws on something fundamentally different, something more internal; the unique physical or behavioral feature of the individual.

In the last decade, the scope of biometric security has broadened due to the widespread use of smartphones, national identity programs in populous countries, enterprise access control, and growing attention to cybersecurity globally. By 2025, biometrics have become central to multi-factor authentication strategies, national ID initiatives, border security processes, and personal device security. But, as these initiatives and applications are being embraced quickly, there are more serious concerns that are being raised about privacy, data protection, the spoofing attack, and the ethical considerations of large biometric databases.

In the report, we address the development of biometrics, the biometric modalities (fingerprints, face, and others, but also vein scanning, and continuous behaviour), the use of biometric data in modern cybersecurity solutions, their use cases in various fields, the technical and societal problems that remain, and the future trends that will impact biometric security.

Authentication in the beginning (1960s) was text-based passwords to determine who you are. As time passed, organizations came to realize the flaws in these single factor mechanisms. Passwords can be forgotten, guessed, stolen, or shared. To strengthen knowledge-based factors (passwords) multi-factor authentication allow to add possession factors (tokens, smart cards). As smart phones started integrating fingerprint and eventually facial sensors, biometric authentication became a reality by the early 2010s, transitioning from a science fiction trope. Apple launched its Touch ID in 2013 and its Face ID in 2017, bringing the technology to the mainstream consumer and showing the industry how it could enable frictionless yet strong user authentication.

Biometrics have become part of every aspect of security throughout the world today. The notion that "you are the password" is convenient and has secured better layers of security as one's unique physical characteristics are hard to replicate, unlike a password. In addition, advanced biometric technology can address the weaknesses of previously existing technologies, such as the duplication of IDs and the theft of passwords from large databases. Biometrics isn't perfect. Just as we may spoof the test: either with an artificial fingerprint, or artificial face, some of that is easy. Much like the other tests, they do have values but so does ease of access. But they also have their own issues. How will they store our biometrics? How will they use them? These are patent issues at the very least. It's important to balance innovation and privacy as biometrics scale further.

2

Fundamentals of Biometrics

2.1 Definition

Biometrics identifies individuals based on their physiological or psychological traits, automatically, and verifies in certain circumstances. This definition points at the notion of each person having measurable and distinguishing characteristics whose values remain constant over time to make it useful for verification. Common physiological characteristics are fingerprints, iris patterns, and facial features. Common behavioral characteristics are speech, typing, walk, etc. A biometric system aims to perform two key functions.

- **Enrollment:** The first function is to enroll the biometric trait i.e. to capture the chosen physiological or behavioural trait and convert to a digital reference (also called a “template”).
- **Verification/Identification:** A biometric system does the following: .Collection of a new sample at the time of authentication and comparing that with the stored templates. This either confirms a claimed identity (one-to-one match), or tells us who is the person (one-to-many match).

2.2 Modalities – Physiological vs. Behavioral

Biometric traits generally fall into two broad categories.

- **Physiological biometrics:**

  Refers to Anatomical or biological attributes. Examples include fingerprints, palm prints, facial structure, iris and retina pattern, vein structure, hand geometry, and even DNA. Many physiological biometric traits are formed early in life (e.g. fingerprints form in the womb) and change very little during adulthood. As a result, they are seen as stable and intrinsic, personal markers of identity.

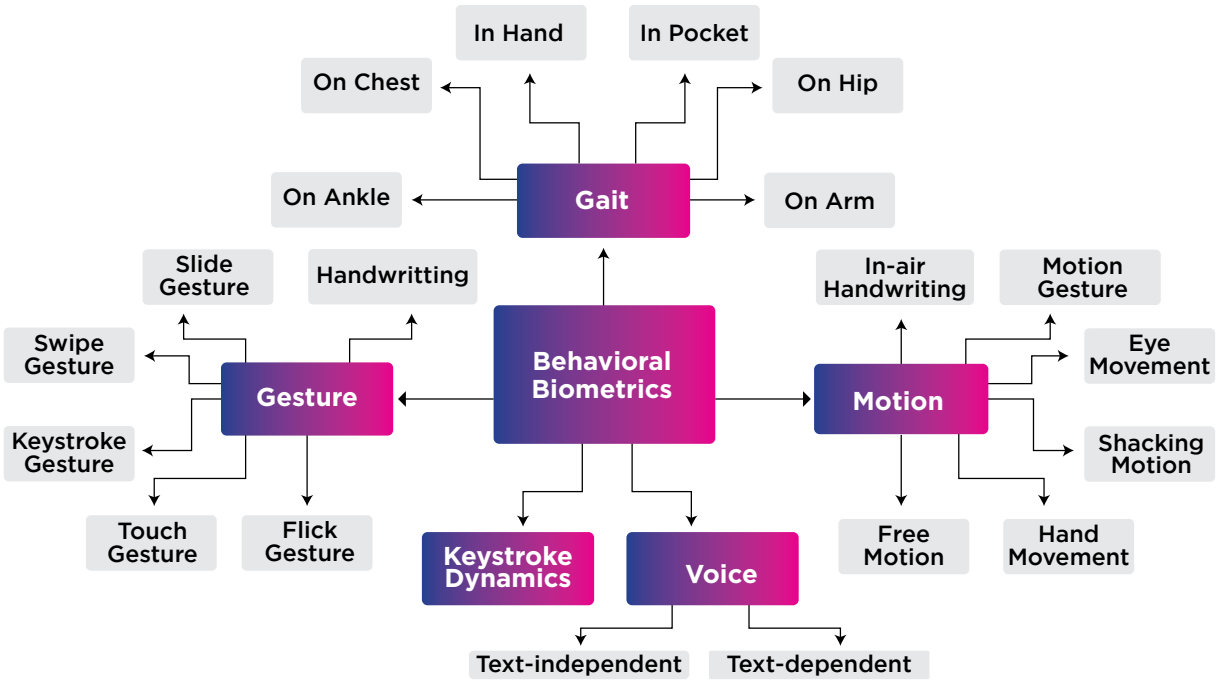
Retina (eye) scanning

Fingerprint scanning

Facial recognition

- **Behavioural biometrics:**

  These are based on the way the person acts. Such as Voice recognition, Keystroke dynamics, Gait analysis, Signature analysis. Over time and in different contexts, behavioural characteristics can vary more. A person's voice sounds different when they have a cold, and even keystroke patterns will change using a different keyboard or when the original user is stressed. Despite this, each individual has inherent behavioral consistencies that a sufficiently sophisticated system can measure and recognize. Both categories play crucial roles in modern security. The physiological characteristics of individuals often offer high uniqueness, while behavioral characteristics enable continuous and passive authentication of the user, verifying the user in real-time.



User Profiling:

Additionally, there is a concept known as user profiling, which extends beyond purely physiological or behavioral biometrics. Rather than measuring a single trait—such as a fingerprint or one's gait—user profiling amalgamates multiple contextual and behavioral signals to establish a holistic, risk-based identity assessment. This can include tracking login times, geolocation patterns, device or browser fingerprints, and typical usage flows in an application. Machine learning models build a unique "profile" of each user's normal activities, then continuously or periodically compare real-time behavior against this baseline. If the system detects unusual deviations—such as a login from an unexpected country, atypical transaction behaviors, or drastically different mouse movement patterns—it can prompt additional authentication or generate alerts for possible fraud or account takeover. While not strictly categorized as a single "biometric modality," user profiling leverages behavioral analytics at a broader level, providing an extra layer of continuous verification or passive authentication that complements the explicit physiological and behavioral biometrics described above.

Biometric Modality	Type	Contactless?	Example Applications	Strengths	Challenges
Fingerprint	Physiological	No (touch)	Phone unlock, employee attendance, forensics	High accuracy; compact sensors; widely adopted	Spoofable with molds; affected by dirt/cuts; requires touch
Facial Recognition	Physiological	Yes	Phone unlock, airport e-gates, surveillance	Contactless & user-friendly; works at a distance	Privacy concerns; needs good lighting or IR; mask reduces accuracy (mitigated by AI)
Iris Scan	Physiological	Yes (IR capture)	National IDs (Aadhaar), border control, secure access	Extremely accurate; stable over time	Requires user alignment; hardware cost; user intimidation (eye scan
Retina Scan	Physiological	No (peering into scanner)	Military access (historically	Very high accuracy	Inconvenient/intensive; rarely used now
Palm Vein	Physiological	Yes	ATM withdrawals (Japan), hospital patient ID	Internal trait (hard to fake); contactless	Requires IR device; moderate user acceptance
Voice Recognition	Behavioral	Yes (remote)	Telephone banking, smart assistants	Hands-free; works over phone; can detect stress	Spoofable by recordings/ deepfakes; impacted by Illness/noise
Keystroke Dynamics	Behavioral	Yes (passive)	Online banking fraud detection, secure computer login	No extra hardware; continuous after login	Moderate uniqueness; can be affected by mood or context
Gait Analysis	Behavioral	Yes	CCTV surveillance, smartphone continuous auth	No user action needed; works from a distance	Low distinctiveness alone; changes with injury/ clothing
Signature Dynamics	Behavioral	Semi (stylus or pen)	Document signing (banks, contracts)	Uses familiar behavior (signing)	Variability in signatures; requires special tablet
DNA Matching	Physiological	No (sample-based)	Forensic identification, paternity tests	Ultimate uniqueness (except twins)	Not real-time; privacy extreme; needs lab processing
Multi-modal (e.g., Face + Finger)	Combined	Varies	Border control (passport + finger), high-security vaults	Very high security (redundancy); flexibility if one fails	More complex UX; higher cost; requires managing multiple devices

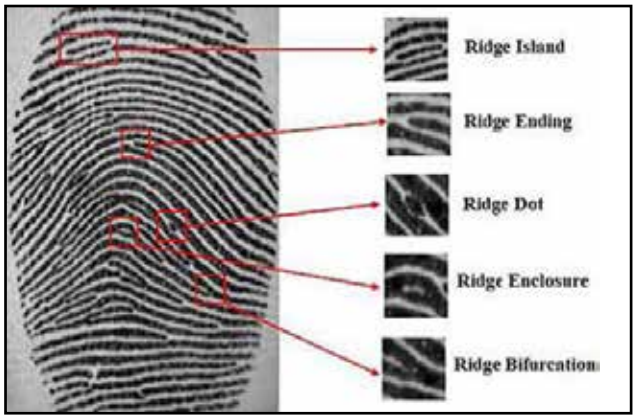
2.3 Functional Components of a Biometric System

Any biometric system typically includes several sequential processes:

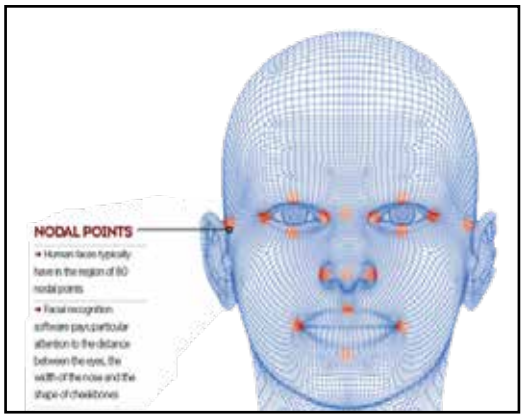
- **Enrollment:** During enrollment, the user's biometric sample is captured with specialized sensors or devices. High-quality data is essential, since the enrolled template forms the reference for all future comparisons. For instance, fingerprint enrollment involves scanning a finger multiple times to capture stable ridge patterns; face enrollment may require the user to look at a camera from different angles; iris enrollment often requires an IR-based camera.

- **Template Creation:** After capture, the system extracts key features from the raw biometric data—such as minutiae points in a fingerprint or nodal points in a face. These features are encoded into a mathematical template, typically much smaller in size than the original image or recording.

Example: Minutiae Point extraction in Finger print



Nodal Points in a face :



- **Storage:** The template is stored in a secure database or on a user's device, often encrypted. Modern approaches aim to store these templates in tamper-resistant hardware (such as a Secure Enclave on smartphones) or in specialized devices to minimize risks from data breaches.

- **Matching:** In the authentication phase, a new sample is taken (finger pressed on a scanner, face looked into a camera, etc.) and converted into a comparable template using the same feature extraction algorithm. The system computes a similarity score between the new sample and the stored template(s). If the score exceeds a threshold, a "match" is declared. Threshold values are tuned based on organizational requirements for security (reducing the false accept rate) versus usability (reducing the false reject rate).

- **Decision:** The final step decides whether to deny or grant or access based on the outcome of the match. In identification scenarios (one-to-many), the system searches across a database of enrolled templates to see if any match is sufficiently close. In verification scenarios (one-to-one), the system compares against only one claimed identity's template.

2.4 Security and Storage Considerations

Biometric systems need careful consideration for privacy and security risks. Most modern systems process data into a small non-invertable template that cannot be reused rather than saving the raw biometric data (e.g. fingerprint image). These templates are generally encrypted while being stored or sent. In the event of a compromise, a template carries less risk than an image. However, certain sophisticated attacks try to reverse-engineer the template. So, strong encryption and frequent auditing of storage methods are important. To prevent interception, secure channels (TLS) or proprietary encryption protect the template during transmission (mainly remote authentication case). Storage on a device (like smartphone storage) makes it difficult for attacks to extract templates, even if the smartphone's operating system gets compromised. To ensure the presentation of the biometric identifiers is live , some vendors offer liveness detection as an added layer of security to ensure that the presented biometric is not sourced from a static photograph or a 3D silicon dummy

2.5 Enrollment Refresh and Updates

Human characteristics inevitably change over time. Changes in physiological traits such as iris patterns may be slight and slow but an individual's fingerprints may wear off in certain professions or as one ages. The facial features may change with weight gain or loss, facial hair, aging, surgery, etc.

Behavioral attributes can shift even more dynamically. As a result, many systems of biometrics plan re-enrollment or template updates from time to time. Contemporary systems powered by artificial intelligence can perform modifications to a template stored in memory, given that the changes remain within some known limits.

3

Types of Biometric Technologies

3.1 Physiological Biometrics: Technical Overview

Physiological biometrics are based on distinct anatomical or biological attributes, typically captured through specialized sensors. They tend to be relatively stable over an adult's lifetime.

3.1.1 Fingerprint Recognition

It is one of the oldest and most pervasive biometric methods, historically used by law enforcement via Automated Fingerprint Identification Systems (AFIS), and now widely adopted in smartphones, employee time/attendance systems, and border checkpoints. Fingerprint scanners capture the valleys & ridges on a fingertip, analyzing minutiae such as ridge endings and bifurcations. Modern sensors range from capacitive to ultrasonic. Though fingerprints are recognized for their high uniqueness, some individuals (e.g., manual laborers or the elderly) can have difficulties with damaged or faint ridge patterns. Spoofing attacks are possible but combated by liveness detection.

Core Sensor Technologies

- **Optical Scanners**: Shines light on the finger and capture the reflected image of the ridges.
- **Capacitive Scanners:** Measure the difference in electrical capacitance between fingerprint ridges and valleys, frequently used in smartphones.
- **Ultrasonic Scanners:** Transmit ultrasonic pulses and record returning echoes to form an image of surface and subsurface details.

Feature Extraction

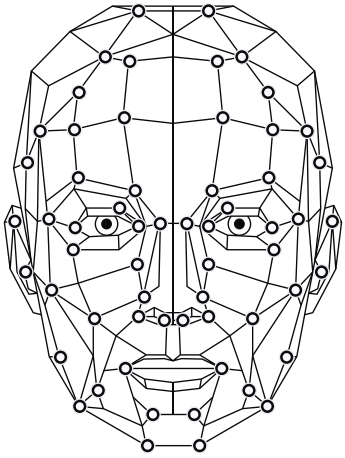
- **Pre-processing**: Enhances the fingerprint image (e.g., noise reduction, contrast adjustment).
- **Binarization and Thinning**: Converts ridges into a thin "skeleton."
- **Minutiae Detection**: Identifies ridge endings and bifurcations.
- **Template Formation**: Stores minutiae coordinates and angles as the user's enrolled reference.

Matching Algorithm

- **Minutiae-Based Matching**: Compares the positions and orientations of minutiae in the sample image with those in the enrolled template, generating a similarity score.
- **Correlation-Based Matching**: May be used in some high-end or forensic systems, comparing local regions or the entire ridge pattern for alignment.

3.1.2 Facial Recognition

Facial Recognition technology uses an image or a series of images of a person's face to identify distinct landmarks-—the distances and shapes of the eyes, nose, mouth, jawline, and others. In more advanced systems infrared mapping or three-dimensional modeling is used to reduce the chances of a simple photograph attack. Apple's Face ID is one of the most successful mainstream examples. The system uses a projected grid of infrared dots to spatially map the user's face.



This contactless technology is being widely used in airports, CCTV, and unlocking personal devices, this . However, privacy advocacy groups are alarmed by facial recognition's potential for mass surveillance.

Image Acquisition

- **Standard RGB Cameras:** Capture 2D images, widely used in smartphones and surveillance systems.
- I**nfrared/3D Sensors**: Use projected infrared dots or time-of-flight technology to build a depth map.
- **Thermal/IR**: Rely on heat signatures or near-infrared imaging, occasionally used for liveness detection.

Feature Extraction

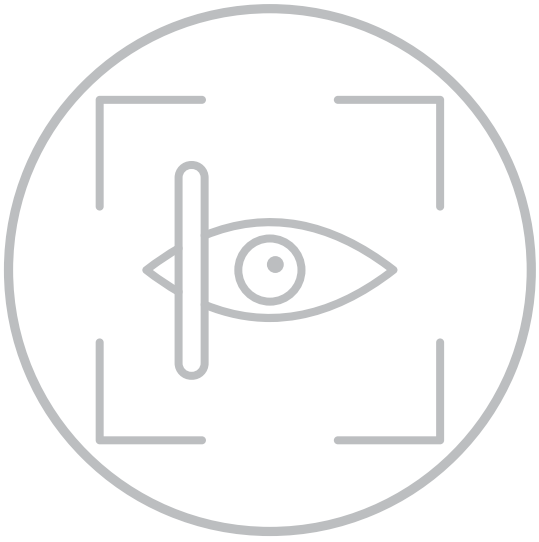
- **Face Detection**: Identifies and isolates the face region from the background.
- **Alignment**: Normalizes the face by adjusting for tilt and scaling.
- **Descriptor Computation**: Employs deep neural networks or classical algorithms (e.g., Eigenfaces) to generate a numeric "embedding" for each face.
- **Template Storage**: Saves the resulting embedding or descriptor as the user's reference.

Matching Algorithm

- **Distance Metrics:** Computes Euclidean or cosine distance between the new face embedding and the stored reference. A threshold determines whether the two faces match.
- **3D Matching**: Depth data can improve accuracy and detect static-photo attacks.

3.1.3 Iris Recognition

Iris Recognition focuses on the patterns in the colored ring around the pupil. Iris patterns are believed to be highly unique, stable over a person's lifetime, and less prone to wear than fingerprints. Iris scanners use infrared illumination to reveal detailed iris textures. Though accurate, iris recognition can be perceived as intrusive by some users and typically requires the user to position their eye carefully within a scanner's range.



Sensor Setup

Iris recognition systems typically use near-infrared illumination (700–900 nm) to emphasize unique textural patterns in the iris.

Feature Extraction

- **Segmentation**: Locates the pupil boundary and outer iris edge.
- **Normalization**: Maps the circular iris region into a rectangular coordinate system to minimize effects of pupil dilation.
- **Filtering:** Applies wavelet or Gabor filters to highlight fine iris textures.
- **Encoding**: Generates a compact binary template (often called an IrisCode).

Matching Algorithm

- **Hamming Distance**: Measures bit-level differences between the new IrisCode and the enrolled reference. A low Hamming distance indicates a strong match.

3.1.4 Vein Pattern Recognition (Palm or Finger Veins)

Vein Pattern Recognition can be performed on the palm or fingers. By shining near-infrared light, these systems capture the unique vein layout beneath the skin. Vein biometrics are generally considered more secure against spoofing because veins lie beneath the surface. Japan's banking sector popularized palm vein ATMs for added security without physical contact.

Finger Vein Authentication System Hitachi

Palm Vein Authentication System (Palm Graph) Fujitsu

Source: Hitachi, Fujitsu

Imaging Method

Near-infrared light illuminates the palm or finger; deoxygenated blood in the veins absorbs IR, creating a distinct contrast pattern.

Feature Extraction

- **Vein Skeleton**: Identifies branching and junctions of the subcutaneous vein network.
- **Template Representation**: Often records these branch points (similar to fingerprint minutiae), forming a unique "vascular map."

Matching Algorithm

- **Graph Matching**: Compares the captured vein pattern graph to the enrolled template. Differences in node positions or connections can indicate a mismatch.

3.1.5 DNA-Based Recognition

DNA-based recognition relies on analyzing an individual's genetic blueprint (deoxyribonucleic acid) to establish identity. Because DNA is nearly unique to each person (except in cases of identical twins), it offers a powerful way to differentiate individuals with a very high level of certainty. However, collecting and processing DNA typically requires specialized laboratory procedures, making it far less convenient than other biometrics like fingerprints or facial recognition. Consequently, DNA matching is mostly used in forensic investigations rather than everyday authentication scenarios.

Sample Collection

DNA is extracted from biological materials such as blood, saliva, or hair follicles. This process can be more invasive compared to methods like scanning a fingerprint or taking a photograph. Strict protocols must be followed to prevent contamination or degradation of the sample, which can introduce errors into the final DNA profile.

Analysis

After collection, the sample undergoes chemical processing in a laboratory. Common techniques include polymerase chain reaction (PCR) amplification, which multiplies specific regions of DNA, and short tandem repeat (STR) profiling, which identifies certain genetic markers unique to each individual. This laboratory-based approach typically takes several hours to days, depending on the complexity of the analysis and the number of samples being processed.

Matching

Once a DNA profile is generated, it's compared against another DNA profile (for example, from a suspect or stored reference). Similarities in the genetic markers indicate a potential match; because these markers are extremely distinctive, DNA comparisons boast very low error rates when properly conducted. However, DNA matching cannot realistically be done in real time: the need for chemical reagents and specialized equipment makes it impractical for quick identity verification at security checkpoints or consumer devices.

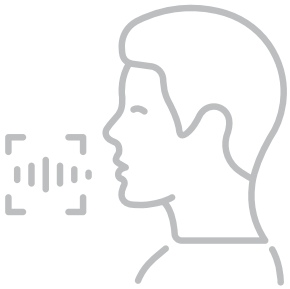
Privacy and Ethical Considerations

Storing DNA data raises significant privacy and ethical concerns. Unlike most other biometric traits, a DNA sample can reveal sensitive information about health conditions and family relationships. As a result, many jurisdictions regulate the use and retention of DNA profiles, limiting them to authorized forensic or medical purposes. The high level of accuracy and uniqueness associated with DNA therefore comes at the cost of invasive collection and stringent data protection requirements, which collectively make it a forensic identifier rather than a routine authentication tool.

3.2 Behavioral Biometrics: Technical Aspects

Behavioral biometrics rely on an individual's learned actions or patterns, which can be more variable than physiological traits but also well-suited for continuous or passive verification.

3.2.1 Voice Recognition (Speaker Identification)



Voice Recognition (speaker identification) relies on the combination of physical and learned speech characteristics. It is particularly useful for remote authentication, such as in call centers or interactive voice response (IVR) systems, but can be vulnerable to voice impersonation or advanced AI "voice cloning." Systems often include text-dependent prompts or random challenge phrases to thwart replay attacks.

Audio Capture

- Microphone Input: Can come from a phone, computer, or a headset.
- Noise Reduction: Removes background interference or echo to isolate the speaker's voice.

Feature Extraction

- **Voice Activity Detection**: Segments the speech from silence.
- **Spectral Features**: Mel-frequency cepstral coefficients (MFCCs) or neural embeddings characterize vocal timbre and pitch.
- **Template**: A feature vector capturing speaker-specific attributes.

Matching

- **Distance-Based Comparison**: Compares the new voice sample's feature vector with the stored reference, typically using a threshold to distinguish genuine from imposter samples.
- **Text-Dependent vs. Text-Independent**: Some systems require a fixed passphrase, while others accept free-form speech.

3.2.2 Keystroke Dynamics

Keystroke Dynamics measures the timing, speed, and pattern of a user's typing. It can be applied for continuous authentication in online banking or corporate systems, alerting administrators if the current typing style deviates significantly from the enrolled user profile. Though keystroke data does not require special hardware, it may exhibit higher variability under stress, using different keyboards, or in changing contexts.

Data Collection

- **Timing Metrics**: Monitors dwell time (how long each key is pressed) and flight time (gap between keystrokes).
- **Error/Recovery Patterns**: Tracks backspaces, corrections, or typical typographical errors.

Feature Extraction

- **Statistical Models**: Calculates mean and variance of keypress intervals for each user.
- **Machine Learning**: Some solutions employ supervised or unsupervised learning to handle user variability.

Matching

- **Threshold Comparison**: Evaluates how closely the current keystroke pattern aligns with the enrolled profile. If it drifts beyond acceptable limits, the system may prompt for additional authentication.

3.2.3 Gait Analysis

Gait Analysis involves identifying a person by how they walk, typically captured via video cameras or wearable sensors. Each person's skeletal structure and habitual movement patterns impart a certain uniqueness, although factors like footwear, injuries, and fatigue can introduce variations. Gait analysis is sometimes employed in surveillance contexts where other biometric data (like face) is not clearly visible.

Capture Approaches

- **Video-Based**: Camera/Surveillance cameras track a person's silhouette or joint positions over time.
- **Wearable Sensors**: Smartphones or smartwatches collect accelerometer and gyroscope data to characterize stride length or foot impact.

Feature Extraction

- **Temporal and Spatial Measurements**: Extracts cadence, step length, joint angle changes, and other motion parameters.
- **Pose Estimation**: Locates skeletal points in consecutive frames, forming a gait cycle pattern.

Matching

- **Template Comparison**: Compares the captured gait descriptors to the user's reference profile.
- **Variability Tolerance**: Systems often allow for normal changes, such as footwear or minor injuries, to avoid false rejections.

3.2.4 Haptics-Based Behavioral Biometrics

Haptics-based behavioral biometrics leverage how users interact with vibrations, touch feedback, or grip on their devices. Modern smartphones, game controllers, and certain specialized tablets use haptic engines that produce subtle vibrations or resistance, and the user's response patterns can form a unique behavioral signature.

Data Capture

Sensors embedded in devices can measure force, pressure, and accelerometer/gyroscope readings when a haptic event is triggered (such as a vibration or tactile "click" simulation). The user's reaction—grip stability, reaction time, or micro-adjustments offers potential identifiers.

Feature Extraction

- **Pressure Mapping**: Tracks how firmly the user holds or presses a device during haptic feedback.
- **Reaction Timing**: Measures delays in user response to vibrations or mechanical cues.
- **Grip Dynamics**: Monitors shifts in device orientation or force distribution over the surface area.

Matching

Live haptic interaction data is compared to the user's established profile. Systems may look at the total force curve or the temporal structure of grip changes to detect whether the same person is holding the device. This could be integrated seamlessly into continuous or low-friction authentication scenarios.

Challenges

- **Hardware Variations**: Different device models or firmware versions can produce slightly different haptic signals.
- **User Adaptation**: Users might change how they grip a device over time or under different conditions (e.g., standing vs. sitting).
- **Data Consistency**: Repeated, standardized haptic events are needed to build consistent user profiles.

3.2.4 Other Behavioral Factors

Signature Dynamics

Signature Dynamics go beyond static signature image matching by analyzing how a signature is performed in real time. Rather than merely comparing the visual result of a signature, these systems capture the speed, pressure, stroke order, and pen tilt as the user writes. Since these motion-based traits are harder to mimic precisely, signature dynamics often provide stronger security than matching a scanned image alone.

Data Capture

Digital signature pads or stylus-equipped tablets are commonly used for data collection. As the user signs, the device records a time series of positional coordinates, pen pressure levels, and sometimes angle or tilt information.

Feature Extraction

- **Temporal Metrics**: The system measures pen-lift timings and the velocity of each stroke.
- **Spatial Patterns**: It notes the sequence of strokes, including direction and curvature.
- **Pressure and Tilt**: The device tracks subtle changes in pen pressure or tilt, adding further uniqueness to the signature profile.

Matching

Signature data from an authentication attempt is compared to an enrolled reference, often using threshold-based or machine learning methods. A certain degree of flexibility is typically allowed, since genuine signatures can vary from day to day or be influenced by factors such as haste or fatigue. Systems with strict thresholds risk higher false rejections, whereas looser thresholds can elevate the risk of forgeries being accepted.

Behavioral Profiling

Overview

Behavioral Profiling is a broader approach that consolidates diverse data points—such as mouse movements, device orientation, application usage, or scrolling behaviors—to establish a holistic model of user interaction. These attributes are monitored either continuously or periodically, allowing the system to flag anomalies indicative of account takeover or insider threats.

Data Capture

Profiling solutions can capture information at various layers, including:

- **Web Sessions**: Mouse speed, click frequency, browsing patterns.
- **Mobile Apps**: Touchscreen gestures, device tilt, and grip changes.
- **System Activity**: Preferred shortcuts, time-of-day usage, typical application launch sequences.

Analysis

Sophisticated AI or machine learning algorithms build a "profile" for each user based on historically observed behaviors. When a new session deviates significantly from the established pattern—like an unusual navigation path or a drastically faster typing speed—the system can either prompt for additional authentication or alert security teams to potential fraud.

Implementation Considerations

- Continuous Authentication: Allows near real-time detection of impostors who begin acting after initial login.
- Privacy: Monitoring multiple user actions can raise privacy concerns; transparent policies and secure data handling are essential.
- Adaptive Thresholds: Behavior can vary due to location changes, new devices, or simply user mood, necessitating a careful balance between sensitivity and tolerance.

3.3 Emerging Modalities

A range of novel biometrics has been proposed or tested, particularly for niche or high-security scenarios. While many of these approaches remain in research or pilot stages, they indicate future directions for authentication technology.

3.3.1 ECG (Electrocardiogram) Heartbeat Authentication

ECG Heartbeat Authentication uses electrocardiogram signals from a wearable device (e.g., a smartwatch). Research suggests individuals have distinctive cardiac rhythms. Yet practical challenges—such as electrode contact and heart rate variability—limit widespread adoption so far.

Signal Capture

- **Electrodes**: Often placed on the wrist or embedded in specialized wearables.
- **Sampling Rate**: Typically 200–500 Hz to capture cardiac waveforms.

Feature Extraction

- **Wave Segmentation**: Detects the P, Q, R, S, and T components of the cardiac cycle.
- **Parametric Descriptors**: Measures intervals and amplitudes to form a user-specific profile.
- **Template**: Stores features such as the distances between peaks or specific wave slopes.

Matching

- **Distance-Based Comparison**: Evaluates how closely the new ECG segment aligns with the user's enrolled template.
- **Variability**: Can accommodate moderate changes in heart rate due to stress or movement by using adaptive matching thresholds.

3.3.2 EEG (Electroencephalogram) Brainwave Biometrics

- Brainwave Patterns (EEG) explore an individual's unique neural responses. While intriguing, wearing EEG headsets is not feasible in most consumer or daily security contexts, but it may be relevant for high-security or medical scenarios in the future.

Data Collection

- **EEG Headset**: Typically multiple electrodes placed on the scalp.
- **Filtering**: Removes artifacts from eye blinks and muscle movements.

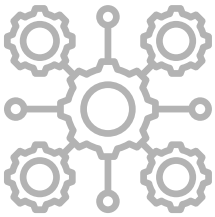
Feature Extraction

- **Frequency Bands**: Analyzes alpha, beta, gamma power levels, often using Fourier or wavelet transforms.
- **Evoked Responses**: In some protocols, users are exposed to stimuli and the system captures event-related potentials (ERPs).

Matching

- **Neural Signatures**: A vector or template representing the user's brainwave patterns.
- **Practicality**: While EEG provides unique signals, current hardware setups can be cumbersome for everyday authentication.

3.3.3 Ocular Micro-Movements



Ocular Micro-Movements measure subtle involuntary eye motions, with potential application in lie detection or advanced user identification.

High-Speed Tracking

Systems rely on cameras with frame rates of 200–500 fps to observe micro-saccades—tiny, involuntary eye movements that occur even when a person attempts to maintain a steady gaze.

Feature Extraction

- **Micro-Saccade Detection**: Identifies the magnitude, velocity, and frequency of these small motions.
- **Liveness Indicator**: Micro-saccades are difficult to replicate artificially, presenting a robust anti-spoof measure.

Matching

- **Statistical Profile**: Compares the micro-movement pattern to the user's enrolled baseline.
- **Deployment**: Mostly experimental, with potential integration in VR/AR headsets or high-security systems requiring strong liveness checks.

3.3.4 Ear Canal Echo / Acoustic Biometrics

- Ear Canal Shape has been tested in prototypes of earbud-based authentication systems, where the shape of a person's ear canal affects the sound reflections captured by the earbud's microphone.

Sensor Mechanism

Earbuds or in-ear devices emit audio signals and record the resulting echoes within the ear canal.

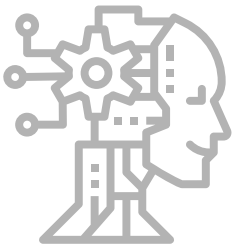
Feature Extraction

- **Frequency Response**: The system measures how different frequencies are absorbed or reflected by the canal's shape.
- **Template**: A curve or impulse response capturing the canal's unique acoustic profile.

Matching

- **Correlation-Based**: Compares the live echo pattern against the enrolled reference, often employing noise-cancellation algorithms.
- **Feasibility**: Offers potential for passive, continuous checks if earbud usage is routine.

3.3.5 Potential Future BCIs



Brain-computer interfaces (BCIs) link a person's nervous system directly to external devices, allowing control or communication through unique neural signals. In advanced approaches like electrocorticography (ECoG), electrodes placed on the brain's surface capture highly detailed data—revealing intricate "brain signatures" that could, in theory, enable identity verification. However, these techniques remain mostly limited to medical or research use because they involve surgical implantation and carry significant complexity and risk.

Sensor Setup

- **Invasive Electrodes**: ECoG arrays rest on the cortical surface, offering clearer signals than standard scalp EEG.
- **Clinical Procedures**: Such installations are typically limited to neurosurgical patients for therapeutic or research reasons, rather than general biometric deployments.

Feature Extraction

BCI algorithms parse brainwave recordings across frequency ranges (delta, theta, alpha, beta, gamma) or event-related potentials (ERPs). Because ECoG data has higher spatial and temporal resolution than scalp EEG, it can capture finer neural activity patterns. Researchers then use techniques like Fourier transforms, wavelet decomposition, or machine learning classifiers to distinguish individuals.

Matching and Practical Considerations

When attempting biometric authentication, the system compares a newly recorded brain signal to an enrolled neural profile. Although early experiments show promising accuracy, real-world applications are constrained by the inherent invasiveness and medical risks of surgical implants. Most BCI research focuses on assisting patients with motor or communication impairments rather than general authentication use cases.

While these emerging biometrics—ECG, EEG, ocular micro-movements, and ear canal echoes—are less commonly deployed in mass-market applications, they demonstrate innovative ways to tackle limitations of older methods (e.g., spoofing, environmental constraints). Some modalities offer robust liveness detection or passive, continuous authentication. Others pose user comfort or cost barriers that must be resolved before widespread adoption becomes feasible.

3.4 Multi-Modal Biometric Systems

Single-modality biometric solutions such as fingerprint-only or face-only perform very well under the ideal conditions but have limitations as well. Some users cannot always easily provide reliable fingerprints (e.g., manual laborers with worn ridges), while others might sometimes have difficulty with a face-only biometric in poor lighting or masked. An assailant who can fake a fingerprint or facial scan is a major threat. To address these issues, many organisations are now adopting multi-modal biometric systems to ensure effective identity verification.

Using additional traits (such as fingerprint + iris, or face + voice) reduces accuracy failure rates and counterfeiting and increases ease of use. Multi-modal architectures, especially when coupled with continuous authentication, are considered best practice for critical security environments, despite being more complex and sometimes expensive than single-modality architectures. As biometric hardware continues to become cheaper and the fusion algorithms driven by AI continue to get better multi-modal systems will likely move from niche or high-assurance applications to more commercial use.

Improved Accuracy and Reduced Spoofing.

In a single authentication transaction, the requirement of more than a single biometric "proof" means lower error rates – both FAR (false accepts) and FRR (false rejects). If the score produced by one kind (for instance, a partial fingerprint contact) is not strong enough to make a decision, the second kind can decide whether to confirm or deny the identity. An attacker who spoofs one modality must similarly deal with additional layers of security. This duplication makes sure it is stronger against advanced presentation attacks like silicone fingerprints or hyper–realistic face masks.

Enhanced Inclusivity and Resilience.

Multi-modal systems ease accessibility issues, as they offer backup solutions when a specific modality cannot be used or is not reliable. An individual with faded fingerprints may confirm their identity using their iris. If a person with a mask or makeup is unable to be identified with facial recognition, the system can default to fingerprint or voice. Moreover, environmental factors that block one modality (e.g., glare affecting face scans) may not block another (an IR-based iris scan or a palm-vein sensor). This robustness makes multi-modal installations particularly suited to large deployments where user characteristics and environmental conditions differ greatly.

Adaptive and Configurable Workflows.

High-tech multi-modal systems can allow for context-based configuration. Nonetheless, an organization may allow a single biometric check under normal conditions (e.g. fingerprint to unlock the phone) but require both fingerprint and iris for a high-risk move (e.g. accessing an encrypted corporate database). In certain deployments, the user may be asked one after another, where if the first face image scan is indecisive, the biometric system will ask for a second (e.g. iris) or a voice scan. Adaptive ways keep security strong yet don't hassle genuine users.

System Complexity and Cost Considerations.

Multi-modal systems are more complex because of this.

The cost of hardware: Getting input from each modality requires dependable sensors and integration.

Using a software method to fuse the data can help combine the match scores together using a fusion algorithm which is decision based or score based. However, this data will add to the computing and development burden.

Users need to enroll in more than one modality, and this might lengthen enrolment procedures and need careful user guidance.

Because these factors can increase implementation and maintenance costs, multi-modal authentication is most often found in high-assurance environments (border control, military bases, national ID, sensitive corporate facilities).

Multi-Modal Fusion Techniques

Usually one of two ways to combine the results is adopted by multi-modal systems.

Score Level Fusion: Occurs after the score is computed for each modality, whereby a "fusion engine" combines the scores into one final accept/reject decision (weighted sums, averages, custom AI models, etc.).

Decision-level fusion: Happens when each modality gives an accept/reject and the system applies rules such as "if at least two of three modalities accept, grant access."

A more complex type is feature-level fusion, where extracted features from different modalities are fused before the matching process. While this can provide great accuracy improvements, it requires sophisticated AI pipelines and extra compute.

Continuous Authentication with Multi-Modal Approaches.

Continuous authentication means the idea of one-time multi-modal checking is made continuous and ongoing in the background. An enterprise workstation may check the user with fingerprint + facial recognition at login, then deploy continuous facial recognition via webcam or may analyze the keyboard usage behaviour. If the user is assumed to have left and another person took their place, the continuous system detects a mismatch and can lock the system.

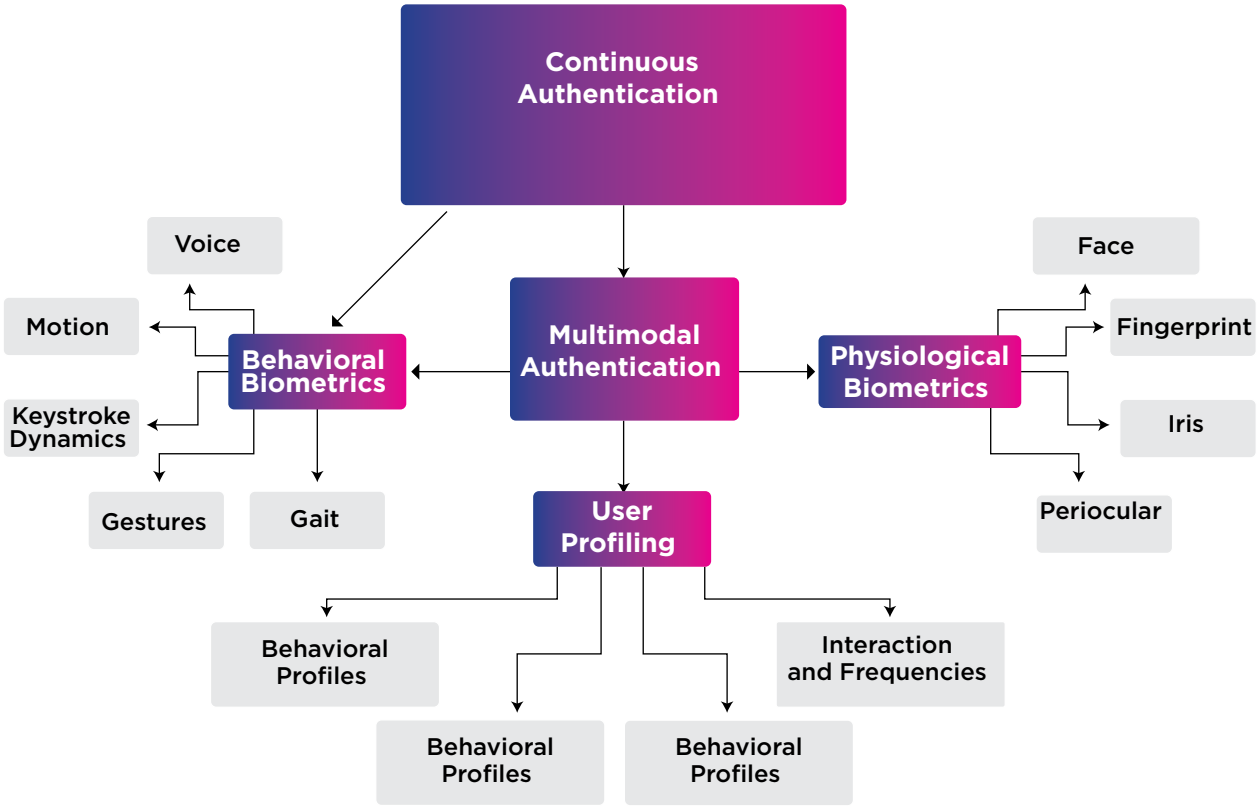
Combining two-factor authentication or multi-modal at entry point and continuous tracking of behavior or physiology ensures organizations a guarantee of identity.

Real-World Use Cases and Examples.

National ID Programs: India's Aadhaar utilizes fingerprint and iris to manage deduplication for more than one billion citizens.

Enterprise data centers: DC's are facilities that need double confirmation (e.g. fingerprint + iris) for securing essential infrastructure at every entry.

Air Travel: Proposed biometric corridors for air travel will rely on the simultaneous use of face + iris, resulting in low error rates even for passengers wearing masks, glasses, and hats and reducing congestion of passengers.



Reference : https://www.researchgate.net/publication/338789512_Sensor-based_Continuous_Authentication_of_Smartphones'_Users_Using_Behavioral_Biometrics_A_Survey

4

Integration of Cybersecurity and Biometrics

4.1 Multi-Factor Authentication (MFA) with Biometrics

Contemporary cybersecurity emphasizes MFA, which typically requires users to present at least two types of credentials drawn from different categories: something you know (password/PIN), something you have (token/smartphone), and something you are (biometric). Biometrics thus serve as the "inherence" factor. This layered approach significantly reduces unauthorized access. Even if an attacker acquires a user's password, they cannot pass the biometric step unless they also replicate that person's physical trait in real time—a far more challenging prospect.

Many smartphone-based MFA solutions simplify the user experience by leveraging the phone's built-in biometric sensor. After successfully scanning a fingerprint or face, a cryptographic challenge can be signed locally without revealing biometric data to external servers. This approach enhances both convenience and security.

4.2 Biometrics and Tokens/Smart Cards

Hardware tokens have evolved beyond simple key fobs to incorporate embedded fingerprint sensors. For example, certain payment cards allow cardholders to enroll their

fingerprint on the card itself, so each transaction can only be performed when the rightful owner touches the sensor. This innovation merges “something you have” (the card) and “something you are” (the fingerprint) into a single device. Similarly, government-issued electronic identity documents may store biometric templates on a chip, which are matched locally to confirm that the cardholder is genuinely the individual named on the card.

4.3 AI-Driven Enhancements

Artificial intelligence plays a pivotal role in advancing biometric systems. Deep learning techniques have significantly improved the accuracy of face, voice, and fingerprint matching, enabling reliable identification even under suboptimal lighting, noise, or partial occlusions. AI is also central to liveness detection, where sophisticated neural networks detect subtle cues indicating a real, living sample. These might include tiny involuntary facial muscle movements, blood flow under the skin, or micro-tremors in a voice. At the same time, attackers also use AI to generate highly convincing fake faces, voices, and fingerprints, leading to a constant AI vs. AI cat-and-mouse dynamic.

4.4 Behavioral Biometrics in Cybersecurity

In addition to physical traits, many organizations deploy behavioral analytics for continuous verification. Once a user logs in, the system continuously monitors behavioral signals such as typing rhythm, mouse usage patterns, or phone movement data. If the behavior diverges significantly from the known baseline, an alert may be triggered or further reauthentication steps required. This strategy helps catch session hijacking attacks where an intruder gains access to an unlocked device or a valid session token. Financial institutions credit such behavioral systems with significant reductions in online fraud, since malicious users operating remotely often exhibit distinctly different interaction patterns.

4.5 Biometric Encryption and Blockchain

Biometric encryption transforms a user's biometric data into cryptographic keys or tokens, so the raw trait is never exposed. If an attacker steals the encrypted key, they cannot easily reconstruct the underlying fingerprint or iris. Cancelable biometrics also fall under this category. In parallel, blockchain-based decentralized identity frameworks are gaining momentum. Under these schemes, users control their own biometric data, stored locally or on a secured personal device, while only zero-knowledge proofs or hashed attestations are placed on a distributed ledger. The ledger validates that a user is unique or meets certain criteria without revealing sensitive personal information.

4.6 Secure Device Biometrics (FIDO2 Standards)

Industry coalitions like the FIDO (Fast Identity Online) Alliance have introduced standards—FIDO2 and WebAuthn—that enable passwordless authentication on websites using local device biometrics. When a user registers for a service, the device generates a public-private key pair, with the private key safeguarded by a secure element. The user's fingerprint or face unlocks that private key locally. During login, the site receives a signed assertion proving the user has the correct private key, but the biometric data never leaves the device. By 2025, many major web services and operating systems (Windows, Android, iOS) support passwordless flows, illustrating how biometrics and cybersecurity are deeply intertwined.

5

Applications and Case Studies of Biometric Security

5.1 National ID Programs

Large-scale biometric ID programs are a pivotal example of biometrics in action. India's Aadhaar is the world's largest biometric identity project, enrolling over 1.38 billion residents through fingerprints, iris scans, and a photograph. Aadhaar aims to eliminate ghost beneficiaries and ease service delivery. Citizens can authenticate themselves at points of service (banks, ration shops) by scanning their fingerprint or iris, which is matched with the stored Aadhaar record in real time.

Other nations have similarly embarked on biometric ID or voter registration drives, including Pakistan's NADRA database, Nigeria's biometric ID programs, and various African countries implementing fingerprint-based voter systems. These projects underscore the power of biometrics to prevent identity duplication and expand citizen access to social benefits. Yet they also highlight issues of data privacy, potential governmental surveillance, and ensuring inclusive systems for those whose biometrics are challenging to capture.

5.2 Financial Sector (Payment Authentication and Fraud Detection)

Financial institutions have rapidly embraced biometrics for both security and customer convenience. In mobile banking, users can log into apps simply by scanning a fingerprint or face, building on the phone's hardware-level security. This approach mitigates the risks of stolen passwords or SIM-based attacks. Call centers in the banking sector have rolled out voice recognition to authenticate customers, reducing the reliance on cumbersome knowledge-based security questions. HSBC's Voice ID in the UK serves as a prominent example, reportedly cutting phone fraud by at least 50%.

Payment authentication methods also incorporate biometrics, such as fingerprint-based contactless cards or palm-vein-based ATM withdrawals in Japan. India's Aadhaar Enabled Payment System (AePS) allows micro-ATMs to authenticate transactions by matching a user's fingerprint to their Aadhaar-linked bank account. Behavioral analytics are further deployed behind the scenes to detect fraudulent sessions—if a user's typing or mouse movement does not match their normal pattern, the transaction may be flagged or blocked.

5.3 Airport and Travel Security

Airports worldwide, seeking greater efficiency and security, have introduced biometric-based check-in, security, and boarding procedures. In the United States, certain airlines and airports have started using facial recognition for "biometric boarding," matching live face images against government databases. Meanwhile, India's DigiYatra initiative aims for a seamless facial recognition journey: passengers enroll their face and flight details in an app and, upon arrival at the airport, cameras confirm their identity at entry gates, security checkpoints, and boarding gates, eliminating constant ID checks. Although such systems offer greater speed and contactless convenience—especially relevant in post-COVID times—they also raise privacy questions regarding data retention and surveillance.

5.4 Enterprise Security

Enterprises frequently deploy biometric solutions to secure access to offices and confidential data. Physical access control might involve fingerprint or facial scanners installed at turnstiles or on locked doors. Biometric time and attendance systems reduce payroll fraud and "buddy punching." Logical access solutions (such as Windows Hello for Business) let employees securely log into corporate devices or sensitive applications using facial recognition or fingerprint. High-security facilities like data centers often employ multi-modal biometric checks (e.g., badge plus fingerprint plus iris) to ensure only authorized personnel cross certain thresholds.

During the pandemic, concerns arose over shared fingerprint scanners, prompting some organizations to adopt facial recognition or mobile app-based check-ins. The legal environment in certain jurisdictions (for example, Illinois' BIPA) requires explicit user consent and short data retention periods, driving the need for privacy-aware biometric deployments.

5.5 Healthcare

Healthcare has its own unique needs for patient identification and data protection. Biometric solutions can ensure that the correct patient record is retrieved, preventing errors such as mismatched patient files or prescription mix-ups. Hospitals may use fingerprint or palm-vein scanners to verify patient identity at registration or pharmacy points. Some facilities also implement biometric access controls for medication cabinets, linking a fingerprint scan to an electronic record of which nurse accessed which drug.

In low-resource settings, biometrics have proven invaluable for tracking immunizations or maternal healthcare visits, ensuring continuity of care. Telehealth solutions during and after COVID-19 sometimes incorporate face or voice verification to confirm patient or provider identity for remote consultations or e-prescriptions. However, healthcare data is subject to stringent privacy regulations (like HIPAA in the US), demanding strong safeguards around stored biometric data.

5.6 Wearables and Consumer Technology

The consumer electronics space has arguably done the most to normalize biometrics in everyday life. Smartphones and tablets almost universally include built-in biometric unlock features, such as Apple's Touch ID and Face ID or Android's face unlock and fingerprint sensors. These systems leverage dedicated secure hardware enclaves to store templates locally. The convenience is so compelling that many users who once left their phones unlocked now lock them because the biometric unlock is quick and easy.

Smartwatches and other wearables may employ heart rate or ECG-based approaches to confirm that the device is on the owner's wrist, though practical mainstream adoption beyond simple passcode locks has been limited so far. Voice assistants like Amazon Alexa or Google Home can recognize different voices in the same household, providing personalized responses or restricting certain actions to the recognized account holder.

Some car manufacturers have integrated biometrics (e.g., fingerprint ignition or in-cabin face recognition) to personalize driver profiles or add a theft deterrent. As IoT devices

multiply in the home, it is not a stretch to imagine front doors or personal computers that automatically recognize household members by face, voice, or gait, ushering in a more frictionless authentication experience.

5.7 Post-COVID Era Contactless Technology

The COVID-19 pandemic accelerated demand for contactless biometrics. Organizations that once relied on fingerprint timeclocks switched to facial recognition or mobile-based systems to minimize physical contact. Airports, border checkpoints, and events expanded trials of face or iris recognition to reduce queues and physical document exchanges. Facial recognition algorithms were updated to handle mask detection or partial face visibility, though not always at the same level of accuracy as pre-pandemic conditions.

In parallel, the growth of remote services—telehealth, remote onboarding of bank accounts, online proctoring for exams—necessitated easy yet secure identity checks. This led to more widespread use of "selfie + ID" apps, where facial recognition and liveness detection confirm that the applicant is the same person shown on the photo ID. While highly convenient, such approaches must address potential spoofs via deepfake videos or manipulated documents.

6

Challenges and Security Risks

6.1 Vulnerabilities and Spoofing Attacks

Despite their advantages, biometric systems remain vulnerable to sophisticated spoofing. Attackers have demonstrated the ability to lift latent fingerprints from everyday objects, mold them in silicone or gelatin, and fool lesser fingerprint sensors. Simple facial recognition implementations can sometimes be tricked by a photograph or video played on a phone, though modern systems include liveness checks. Voice recognition can be compromised by high-quality recordings or AI voice generators. Deepfake technologies pose a looming threat, with advanced systems able to simulate a person's face or voice in real time. These risks underscore the need for robust anti-spoofing mechanisms at both the hardware and software layers.

6.2 Privacy Concerns

Biometric data is uniquely sensitive. Unlike passwords, a person's facial structure, fingerprints, or iris patterns cannot be "reset" if compromised. Large biometric databases present prime targets for criminals and state-level cyberattacks. If stolen, biometric data could theoretically be used to impersonate individuals across multiple systems. Furthermore, there is significant potential for "function

creep," where data collected for one purpose (such as unlocking a phone) is later used for government surveillance or commercial profiling without proper user consent. Legislation, such as the EU's General Data Protection Regulation (GDPR) and Illinois' Biometric Information Privacy Act (BIPA), aims to restrict how organizations collect, store, and use biometric data. Yet, compliance and enforcement remain inconsistent globally.

6.3 Impact of Aging, Injuries, and Environmental Factors

Biometric reliability can degrade over time. Facial recognition may fail if a user grows or shaves a beard, or if they frequently wear a mask in pandemic-era conditions. Fingerprints can become hard to read for individuals with certain health conditions or labor-intensive jobs that wear down the ridges. Voice changes with illness, background noise, or even emotional stress. Environmental factors such as dim lighting or extreme bright conditions can hinder camera-based systems. Systems must provide backup methods, such as a fallback password or PIN, and may need periodic re-enrollment to remain effective.

6.4 Security of Biometric Hardware

Biometric hardware can be a weak link if sensors are poorly designed or installed. Attackers might replace a sensor with a malicious reader that captures raw data. Thus, many vendors use anti-tamper sensors, secure communication channels from the sensor to the main system, and secure enclaves that handle template creation and storage. System integrators must also be cautious with device deployment, ensuring physical security and routine firmware updates to patch potential vulnerabilities.

6.5 Societal Acceptance and Revocability

Some users remain uncomfortable providing biometric data to employers, governments, or private companies. Data leaks or revelations of misuse quickly erode public trust. Whereas traditional credentials (passwords, tokens) can be revoked, biometric revocation is inherently complex—an individual cannot simply change their fingerprint if it is compromised. Researchers have proposed "cancelable biometrics," where data is mathematically transformed, allowing a new transformation if a template is exposed. However, these remain niche in actual implementation. Societal acceptance depends heavily on transparency, consent, data minimization, and a demonstration of tangible benefits (such as faster processes or stronger fraud prevention).

7

Standards, Regulatory Frameworks, and Emerging Ecosystem

Biometric security systems, once isolated technical solutions, are now subject to complex global standards and strict regulatory mandates. This shift reflects biometrics' transition from niche authentication tools to critical infrastructures underpinning financial services, healthcare, government identity programs, and national security. In this section, we delve into the technical specifications, compliance landscapes, and emerging ecosystem shaping the future of biometric deployments.

7.1 Global Biometric Standards

The technical landscape of biometric security is increasingly defined by robust global standards, aimed at ensuring interoperability, enhancing spoof-resistance, and safeguarding sensitive biometric data throughout its lifecycle. Key standards shaping the field include:

7.1.1. ISO/IEC 19794 Series – Biometric Data Formats

The ISO/IEC 19794 family standardizes how biometric data should be structured and transmitted. It covers multiple

modalities including fingerprints (Part 2), facial images (Part 5), iris images (Part 6), and vascular patterns (Part 9). A critical example is ISO/IEC 19794-2, which defines the minutiae template format for fingerprint recognition. This template captures ridge endings and bifurcations in a compact, vendor-neutral way, allowing fingerprint systems from different manufacturers to exchange and match data accurately. Without such standards, interoperability across borders (e.g., biometric e-passports) or across systems (e.g., police databases) would be practically impossible.

Moreover, the ISO/IEC 19794 standards emphasize quality metrics — for instance, specifying minimum resolutions for fingerprint images or normalization procedures for face image acquisition — which directly impacts matching accuracy in real-world deployments.

7.1.2 ISO/IEC 30107 – Biometric Presentation Attack Detection (PAD)

Spoofing attacks such as using a fake fingerprint mold, a printed photograph, or an AI-cloned voice — represent one of the greatest vulnerabilities in biometric systems. ISO/IEC 30107 directly addresses this by introducing a technical framework for Presentation Attack Detection (PAD).

Part 1 defines the terminology and concepts, Part 2 outlines evaluation methodology, and Part 3 (ISO/IEC 30107-3) specifies rigorous test protocols for assessing system resilience against attacks. Modern biometric deployments (especially in financial services or border security) increasingly demand PAD compliance certification, where systems must not only detect live traits (like subtle finger perspiration or micro-blinks) but also resist high-fidelity forgeries under laboratory conditions.

Conformance to ISO/IEC 30107 ensures that biometric systems go beyond simple matching and actively verify the authenticity of the presented trait.

7.1.3 FIDO Alliance – Fast Identity Online (FIDO2 and WebAuthn)

The FIDO Alliance addresses a different weakness in traditional authentication — reliance on passwords, which are easily stolen or guessed. FIDO2 and WebAuthn standards allow users to authenticate securely using their device's built-in biometric sensors (e.g., fingerprint readers, face scanners) without transmitting biometric templates to servers.

Instead, the authentication flow works as follows:

- Upon device enrollment, a public-private key pair is generated.
- The private key is stored securely (e.g., in a Trusted Platform Module or Secure Enclave) and is unlocked locally via biometric authentication.
- During login, the device signs a challenge using the private key. The server verifies the signature using the public key — without ever seeing the user's fingerprint or face.

This architecture inherently adopts a zero-trust approach — assuming that external networks may be compromised and safeguarding user credentials at the device level. FIDO2 has now been adopted by major operating systems (Windows Hello, Android, iOS) and leading web browsers, setting the stage for passwordless authentication to become a mainstream reality.

7.1.4 NIST SP 800-63B – Digital Identity Guidelines

The NIST SP 800-63B document, issued by the US National Institute of Standards and Technology, sets definitive recommendations for digital identity proofing and authentication. It recognizes biometrics as a valid "inherence" factor but cautions that biometrics must never be the sole authentication factor for high-assurance levels.

NIST mandates that:

- Biometric samples must be captured via liveness detection techniques.
- All biometric match scores must cross threshold values designed to minimize both False Accept Rate (FAR) and False Reject Rate (FRR) based on the sensitivity of the system.
- Matching must occur in a restricted and secured environment, and biometric unlocks must always be coupled with another authentication factor (like device possession or knowledge-based PINs) when securing sensitive operations.

NIST also highlights that if a biometric is compromised, it cannot be changed like a password, necessitating strong template protection (e.g., encryption, cancelable biometrics).

Together, these standards promote critical best practices in biometric system design:

- Secure template management (ISO 19794, FIDO2)
- Liveness detection and spoof resistance (ISO 30107, NIST)

- Encryption of data in transit and at rest (FIDO2, NIST)
- Multi-modal biometric integration to reduce spoofing risks and enhance inclusivity.

Without adherence to such standards, biometric deployments risk being either insecure or non-interoperable — defeating the very trust users place in identity technologies.

7.2 India-Specific Regulatory Developments

India has emerged as a global pioneer in large-scale biometric applications. Accordingly, the regulatory and standards landscape is evolving rapidly to govern the responsible use of biometrics.

7.2.1 Aadhaar and UIDAI Regulations

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 established the framework for India's biometric identity infrastructure. Key technical mandates include:

- Mandatory liveness detection during biometric capture.
- Encryption at the source: All biometric data must be encrypted immediately after capture and before transmission.
- STQC Certification: Biometric capture devices must pass stringent security and performance standards under the Standardization Testing and Quality Certification (STQC) framework.

UIDAI's Technical Specifications also prohibit the storage of biometric images by authentication service providers, limiting exposure of raw data and enforcing a template-based matching architecture.

7.2.2. RBI's Push Toward Behavioral Biometrics

While the Reserve Bank of India (RBI) has not made behavioral biometrics mandatory, its Digital Payment Security Controls guidelines (2021) encourage banks and payment operators to move beyond static credentials. Key recommendations include:

- Implementing risk-based and context-aware authentication.
- Deploying continuous authentication mechanisms, such as keystroke dynamics and device interaction monitoring.

Banks are increasingly adopting behavioral biometric profiling to track unique session behaviors and flag anomalous activities in real-time — an evolution implicitly encouraged by the RBI's emphasis on adaptive security measures.

7.2.3 Digital Personal Data Protection Act (DPDP) 2023

India's Digital Personal Data Protection (DPDP) Act, 2023 formally classifies biometric data as "sensitive personal data," invoking strict obligations:

- Prior explicit consent is mandatory before biometric collection.
- Entities must ensure purpose limitation and data minimization.
- Organizations must adopt technical safeguards like encryption, access control, and regular vulnerability assessments for biometric repositories.
- Breaches involving biometric identifiers must be reported to the Data Protection Board of India promptly, under prescribed timelines.

Thus, while biometrics promise enhanced security, Indian law now equally stresses safeguarding biometric rights through enforceable accountability.

7.3 Global Regulatory Landscape for Biometrics

Outside India, many regulatory frameworks treat biometrics with heightened sensitivity, recognizing the irreversible nature of these identifiers if compromised.

- GDPR (General Data Protection Regulation - EU): Under GDPR, biometric data processed for the purpose of uniquely identifying a person is considered "special category data," subject to heightened processing restrictions. Explicit consent, transparency, and impact assessments (DPIAs) are mandatory.
- BIPA (Biometric Information Privacy Act - Illinois, USA): One of the world's strictest biometric privacy laws, BIPA mandates:
    - Prior written consent before biometric capture.
    - Clear disclosure of data use and storage practices.
    - A defined data retention schedule and secure destruction policies.
- California Consumer Privacy Act (CCPA): Extends individual rights to access, correct, or delete biometric data, treating it as a form of personal information.
- Emerging AI and Biometric Regulations (EU AI Act): The draft European AI Act proposes restricting real-time remote biometric identification in public spaces, highlighting a broader trend of cautious oversight over biometric surveillance technologies.

Globally, regulators emphasize consent, transparency, security, and accountability as foundational principles when deploying biometrics in public or private settings.

7.4 Future Directions in Biometric Regulation and Standards

Looking ahead, several trends are poised to shape the intersection of biometrics and regulation:

- Decentralized Biometrics and Self-Sovereign Identity: Solutions where biometric templates are securely stored on personal devices, combined with blockchain-based proofs (such as zero-knowledge attestations), will likely proliferate, reducing centralized risks.

- Algorithmic Fairness and Transparency: Regulators may soon require vendors to disclose the demographic performance of biometric systems, addressing concerns over racial, gender, or age-related biases.
- Mandatory Anti-Spoofing Certification: Financial and government deployments may demand compliance with ISO 30107-3 PAD benchmarks to resist advanced spoofing attacks.
- Cross-Border Interoperability Standards: As global mobility grows, interoperable biometric systems (e.g., standardized iris templates or FIDO-certified devices) will become critical, particularly for e-passports, international border management, and multinational corporations.
- Integrated AI and Biometric Audits: Future audits may assess not just raw biometric data handling, but also how AI-driven biometric matchers behave under adversarial conditions, ensuring that AI-enhanced biometrics remain accountable, explainable, and robust.

In essence, the future regulatory environment for biometrics is likely to mirror the dual demands of innovation acceleration and rights preservation, requiring technologists to embed security, fairness, and transparency into the very DNA of biometric systems.

8

Evaluation & Benchmarking— How We Prove Biometrics Are Trustworthy

Before any maker rolls out a biometric system, they have to answer four practical questions:

1. **Security**: "How many impostors can sneak through?"
2. **Convenience**: "How often will real users get blocked?"
3. **Spoof-proofing**: "Can fake fingerprints or deep-fakes fool it?"
4. **Fairness**: "Does it work equally well for every age, skin tone, or accent?"

Organised testing & benchmarking turns those questions into hard numbers that any engineer or regulator can check.

8.1 Core Error Metrics:

1. False-Accept Rate (FAR) — "Letting the Wrong Person In"

Imagine 1000 strangers all try the same fingerprint reader: If 2 of them fool the reader and get inside, the FAR is 2 ÷ 1000 = 0.2 %.

A low FAR means the lock is hard to trick.

2. **False-Reject Rate (FRR)** — ***"Locking the Right Person Out"***

   Now picture the genuine owner touching the reader 1000 times: If it refuses her 5 times, the FRR is 5 ÷ 1000 = 0.5 %.

   A low FRR keeps day-to-day life friction-free.

Key point: tightening security (lower FAR) usually nudges FRR up, and vice versa.

3. **Equal-Error Rate (EER)** — ***"One-Number Snapshot"***

   If you slowly turn the reader's "strictness knob," there is one setting where FAR and FRR become equal.

   That number is the EER. Lower EER = better overall design.

4. **ROC Curve** — ***"The Tuning Dial"***

   Engineers plot FAR on the horizontal axis and True Accept Rate (= 1 – FRR) on the vertical axis.

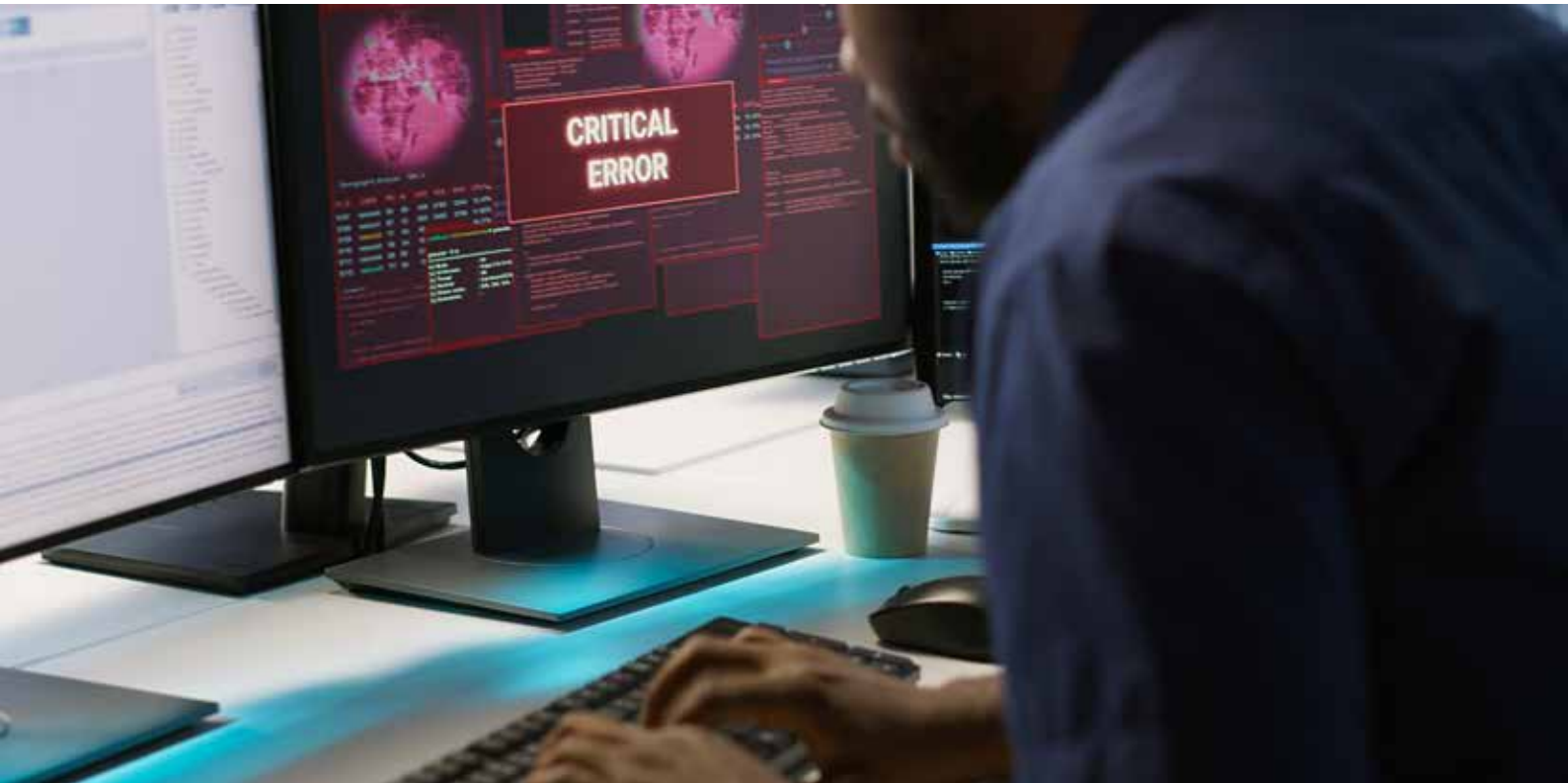
   The resulting Receiver-Operating Characteristic curve shows every possible trade-off point.

   A steep curve that hugs the top-left corner is the signature of a high-quality algorithm.

8.2 Liveness & Anti-Spoof Scores

A face matcher can be 100 % accurate and still be useless if an attacker can wave a glossy photo—or a deep-fake video—at the camera and walk right in.

To plug that hole, modern systems add a Presentation-Attack Detection (PAD) layer: tiny algorithms (or hardware tricks) that confirm the fingerprint, face, or voice in front of the sensor is coming from a live human, right now, not from a printed copy or recorded audio.



ISO 30107—the global scorecard for spoof resistance:

The ISO 30107 standard formalizes how vendors must measure and report their anti-spoof strength.

It introduces two companion error rates:

1. **APCER — Attack-Presentation Classification Error Rate**

   The percentage of fake or spoof samples that the system mistakenly classifies as genuine.

   (How often a spoof succeeds)

   Example:

   A certification lab presents 500 silicone fingerprint moulds to the sensor.

   8 of those moulds are accepted as real.

$$\text{APCER} = \frac{8 \text{ successful spoofs}}{500 \text{ spoof attempts}} \times 100\% = 1.6\%$$

An APCER of 1.6 % means roughly 1–2 spoof fingers in every 100 could breach the system. High-security deployments (e.g., payments, passport e-gates) typically require APCER well below 0.5 %.

2. **BPCER — Bona-Fide Presentation Classification Error Rate:**

   The percentage of live, bona-fide presentations that the anti-spoof layer wrongly labels as fake.

   (How often a real user is treated as a spoof)

   Example

   The same lab now tests 1000 genuine users.

   25 of them are falsely rejected and asked to try again.

$$\text{BPCER} = \frac{25 \text{ false rejections}}{1\,000 \text{ live attempts}} \times 100 = 2.5\%$$

A BPCER of 2.5 % means 1 in 40 legitimate users will suffer a frustrating "spoof suspected—please retry" message. For customer-facing systems, organisations aim for BPCER under 1 % to keep user experience smooth.

8.3 Independent "Score-Keepers":

To avoid marketing spin, most governments and large buyers rely on public, repeatable test beds:

- **NIST FRVT – Face Recognition Vendor Test (millions of portrait & "selfie" photos).**

  Run continuously by the U.S. National Institute of Standards and Technology (NIST), FRVT is the de facto league table for face recognition. Vendors submit their algorithms; NIST tests them on millions of images ranging from passport-style portraits to uncontrolled "selfies" and CCTV stills. Results are published for four tracks—1:1 verification, 1:N identification, masked-face performance, and demographic bias. Scores include False-Match Rate (FMR), False-Non-Match Rate (FNMR), and elapsed CPU/GPU time, so buyers can see both accuracy and speed.

- **NIST IREX – Iris Exchange**

  IREX does for iris recognition what FRVT does for faces. Recent rounds evaluate PAD (Presentation-Attack Detection) as well as classic matching. Algorithms face high-resolution near-infrared images, lower-quality consumer shots, and deliberate spoof artefacts such as printed contact lenses. Output metrics—Equal-Error Rate, ROC curves, and APCER/BPCER—tell regulators how an iris engine copes under both clean and adversarial conditions.

- **NIST MINEX III – Minutiae Interoperability Exchange**

  MINEX III focuses on fingerprints, but not on raw image matching; it checks template interoperability. The test forces a vendor's "feature extractor" to create ANSI/INCITS 378-compliant templates and then asks another vendor's "matcher" to read them. By mixing-and-matching thousands of fingerprint pairs, NIST measures both minutiae-quality and cross-vendor compatibility essential for large AFIS or law-enforcement databases where hardware and software come from different suppliers.

- **LivDet – Liveness Detection**

  LivDet is an academic, open-data contest held every 1–2 years for spoof detection in fingerprints (and more recently, faces). University labs build large sets of "live" vs "fake" prints or photos using latex, gelatin, 2-D/3-D masks, or screens. Competitors run their PAD algorithms on these datasets while organisers track Accuracy, APCER, and BPCER. Because everything is peer-reviewed and code can be audited, LivDet acts as a public reality-check on anti-spoof claims.

These labs publish ranking tables every few months; vendors cannot cherry-pick results.

8.4 Fairness & Demographic Tests

Recent studies showed some face algorithms perform worse on darker skin tones or certain age bands.

Modern evaluations therefore break down FAR/FRR by gender, age, and ethnicity.

The latest NIST FRVT reports include these demographic slices so buyers can spot bias before deployment.

9

Future Trends in Biometric Security

9.1 AI and Machine Learning in Biometrics

Deep learning has already improved biometric accuracy (especially in face and voice), but its full potential is yet to be realized. Future systems will employ AI for adaptive template updates, calibrating to normal changes like aging or facial hair. AI-based liveness detection will become increasingly sophisticated, analyzing micro-expression, blood oxygenation patterns, or minute skin reflections. Meanwhile, generative adversarial networks (GANs) will spur more realistic spoofs, ensuring an ongoing arms race. Expect next-generation biometric solutions to incorporate AI not just in matching but also in orchestrating multi-factor and multi-modal checks in real-time, dynamically adjusting thresholds based on perceived risk.

9.2 Decentralized Biometric Systems (Blockchain-Based)

As concerns about centralized "honeypot" databases grow, decentralized identity models using blockchain or distributed ledgers will likely gain traction. In these systems, a user's biometric data stays on their personal device or in a secure personal vault, while verifiers consult a ledger for cryptographic attestations, ensuring uniqueness without storing raw data. Projects like Worldcoin have already sparked debate by scanning irises to create global "proof-of-personhood," though critics worry about privacy. By

2025 and beyond, a range of decentralized identity providers may emerge, offering new paradigms in how we prove identity without central authorities holding all biometrics.

9.3 Continuous and Passive Authentication

Traditional authentication checks identity only at login or entry points, leaving sessions vulnerable to hijacking. The future is trending toward ongoing background checks of user presence via camera snapshots, microphone cues, or usage behaviors. A device might use the front camera to confirm the same face remains in front of the screen, or sense the user's unique manner of scrolling. Such continuous or passive authentication can be integrated seamlessly, but it raises concerns about constant surveillance of a user's environment. Organizations adopting these methods need strong privacy controls and clear user consent mechanisms.

9.4 Biometrics in the Metaverse and Web3

As virtual reality (VR), augmented reality (AR), and broader concepts of the Metaverse evolve, user identity becomes more critical. VR headsets with inward-facing cameras can capture iris or face data to log users in. In AR glasses, eye tracking can identify or authenticate the wearer. Web3 platforms, anchored in decentralized infrastructure, may require robust proofs of personhood to mitigate bots or fraudulent accounts. Biometrics could ensure that each avatar or user is a unique human, though how this data is stored and protected remains a subject of intense debate. Enhanced authentication in virtual economies might also rely on biometric hardware wallets or gestures that only the legitimate owner can perform accurately.

9.5 Enhanced Privacy Techniques

Privacy-by-design principles continue to mature, with advanced methods like fully homomorphic encryption (FHE) potentially allowing biometric matching on encrypted data. Federated learning may enable AI algorithms to train on local biometric data across millions of devices without sending raw data to a central server. Regulators worldwide are likely to demand clearer transparency and user control over biometric usage. This interplay of technology and regulation will define which innovative privacy safeguards become standardized.

9.6 New Modalities and Fusion

Emerging modalities such as ECG-based authentication or brainwave-based systems may see expanded research and limited specialized use by 2030. More immediately, multi-modal fusion will become the norm in high-security contexts. Organizations may require fingerprint plus face or face plus voice for certain transactions, each validated by robust liveness checks. With computing power cheaper and AI more advanced, fusing these signals in real-time will be feasible without significant user inconvenience, enhancing both accuracy and resistance to spoofing.

9.7 Regulations and Ethical Biometrics

Regulations will shape biometrics significantly. The EU's proposed AI Act and updated eIDAS frameworks, for instance, could restrict real-time remote biometric identification by law enforcement. Various countries have introduced or strengthened data protection laws, many categorizing biometric data as "sensitive" with strict usage rules. Companies deploying biometric surveillance or broad-based face recognition may face bans or severe limitations. Ethical concerns around demographic biases, such as facial recognition struggling with certain skin tones or ages, have led to algorithmic fairness mandates. Vendors must address these biases through more diverse training data and transparent performance reporting.

Conclusion

Biometric security has made significant strides from niche technology to a daily reality for billions of people worldwide. Its evolution was driven by the limitations of passwords and token-based systems, the advent of powerful mobile processors, and the growing desire for convenient yet robust identity verification. From a single touch unlocking a smartphone to advanced airports and border checks that rely on facial recognition, biometrics now underpins critical infrastructure in finance, healthcare, public services, and beyond.

In examining its benefits, we see how biometrics improves security, reduces fraud, and offers user-friendly access to services that once required multiple steps or physical tokens. National ID programs demonstrate that, at scale, biometrics can transform service delivery and inclusion. Enterprises find biometrics useful not only for physical access but also for continuous monitoring of privileged users. Healthcare settings rely on it to ensure patient safety and data integrity. Consumers enjoy frictionless device unlock and personalized experiences.

Nevertheless, biometrics is no panacea. Spoofing remains a formidable challenge, particularly with the advent of AI-driven deepfakes. Privacy and data governance issues loom large, since a stolen biometric cannot be replaced like a password. Systems must incorporate rigorous protections, robust encryption, and legal frameworks that preserve human rights and dignity. Moreover, broad acceptance relies on addressing ethical questions around potential demographic biases and the fear of pervasive surveillance.

Looking to the future, we anticipate deeper integration of AI for anti-spoofing and adaptive matching, increased adoption of decentralized and privacy-preserving architectures, continuous authentication that quietly confirms the legitimate user throughout a session, and expansions into the Metaverse and other virtual realms. As technology evolves, the crux of biometric security will remain the same: bridging our physical identity to the digital world in a way that is both trustworthy and respectful of individual autonomy. Achieving that balance is the collective responsibility of technologists, businesses, governments, and civil society.

11

Appendices

Abbreviations

- **AFIS** – Automated Fingerprint Identification System
- **AI** – Artificial Intelligence
- **AR** – Augmented Reality
- **BCI** – Brain-Computer Interface
- **BIPA** – Biometric Information Privacy Act
- **DNA** – Deoxyribonucleic Acid
- **ECG** – Electrocardiogram
- **ECoG** – Electrocorticography
- **EEG** – Electroencephalogram
- **FAR** – False Accept Rate
- **FHE** – Fully Homomorphic Encryption
- **FIDO** – Fast IDentity Online
- **FRR** – False Reject Rate
- **GAN** – Generative Adversarial Network
- **GDPR** – General Data Protection Regulation
- **IR** – Infrared
- **MFCC** – Mel-Frequency Cepstral Coefficients
- **MFA** – Multi-Factor Authentication
- **OTP** – One-Time Password
- **PCA** – Principal Component Analysis

- **PCR** – Polymerase Chain Reaction
- **PIN** – Personal Identification Number
- **STQC** – Standardization Testing & Quality Certification
- **STR** – Short Tandem Repeats
- **VR** – Virtual Reality
- **WebAuthn** – Web Authentication (part of the FIDO2 standard)

Glossary of Key Terms:

- **Adaptive Authentication**: A security approach that dynamically adjusts authentication requirements based on context or risk factors (e.g., requiring additional biometrics if a login attempt seems suspicious).
- **AFIS (Automated Fingerprint Identification System)**: A large-scale fingerprint database system used mainly by law enforcement to store, compare, and match fingerprints. Modern AFIS can rapidly search millions of records to identify individuals.
- **AI (Artificial Intelligence)**: Techniques and algorithms enabling machines to perform tasks typically requiring human intelligence (e.g., learning from data, pattern recognition). AI significantly enhances biometric matching accuracy, liveness detection, and adaptive authentication.
- **AR (Augmented Reality)**: Technology that overlays virtual elements onto the real world, often via headsets or smartphone cameras. In biometric contexts, AR devices may incorporate eye-tracking or face scans for authentication in mixed-reality environments.
- **BCI (Brain-Computer Interface)**: A direct pathway between the human nervous system and external devices, often involving electrodes to detect and interpret brain signals. Invasive methods like ECoG offer high-fidelity data but remain limited to specialized medical or research uses.
- **Behavioral Biometrics**: Biometrics based on how an individual performs certain actions—typing rhythm, gait, voice patterns, or haptics—rather than purely physical traits. Useful for continuous or passive authentication, but often sensitive to context or user stress.
- **Behavioral Profiling**: A broader approach that aggregates diverse data points (e.g., mouse movements, application usage) into a holistic user profile. Systems continuously compare new behaviors against the profile to detect anomalies indicative of fraud or account takeover.
- **Biometric Encryption**: A security practice transforming raw biometric data (e.g., fingerprint images) into cryptographic keys, ensuring the original trait is never directly stored or transmitted.

- **BIPA (Biometric Information Privacy Act)**: A U.S. state law (Illinois) governing biometric data collection, use, retention, and disposal. Requires explicit, informed consent and allows individuals to sue for violations, thereby influencing how businesses handle biometrics.
- **Cancelable Biometrics**: A method applying a non-invertible transform to a biometric trait (e.g., a fingerprint template), allowing it to be "reset" if compromised—akin to changing a password.
- **Continuous Authentication**: An authentication model that checks user identity throughout a session rather than a one-time login event. Often relies on behavioral biometrics (e.g., keystroke dynamics, mouse usage) to detect intruders who take over an already unlocked session.
- **Correlation-Based Matching**: A technique in fingerprint or image comparison that directly compares and aligns local or global image regions rather than focusing on distinct feature points like minutiae.
- **Deepfakes**: AI-generated synthetic media—photos, videos, or voices—designed to mimic a real person. They pose a major threat to biometric systems reliant on face or voice recognition without robust anti-spoofing measures.
- **DNA (Deoxyribonucleic Acid)**: The genetic blueprint of living organisms. While exceptionally accurate in distinguishing individuals, DNA analysis is impractical for everyday authentication due to lab-based processing, privacy concerns, and slow turnaround times.
- **ECoG (Electrocorticography)**: An invasive BCI technique placing electrodes directly on the brain's surface to record neural signals at high resolution. It provides detailed data for research or medical applications, but its invasiveness limits common biometric usage.
- **ECG (Electrocardiogram)**: A measure of the heart's electrical activity. In biometrics, ECG-based methods extract distinct waveforms (P, Q, R, S, T peaks) to create user-specific templates for wearable-based authentication.
- **EEG (Electroencephalogram)**: A non-invasive recording of brain activity via scalp electrodes. EEG biometrics are often confined to experimental or high-security contexts due to variability and the complexity of wearing headsets regularly.
- **Enrollment**: The process of capturing a user's biometric data (e.g., scanning a fingerprint, recording facial features) and creating an initial reference template that future authentication attempts compare against.
- **FAR (False Accept Rate)**: The likelihood that a biometric system incorrectly authenticates an imposter as a legitimate user. Lower FAR means higher security against unauthorized access.
- **FHE (Fully Homomorphic Encryption)**: A form of encryption allowing computations on encrypted data without decryption. In biometrics, it promises privacy-preserving matching (though still in research or early adoption stages).

- **FIDO (Fast IDentity Online)**: An industry alliance developing open standards (e.g., FIDO2, WebAuthn) for passwordless authentication. FIDO protocols allow devices to authenticate users locally via biometrics without sending raw data to servers.
- **FRR (False Reject Rate)**: The likelihood that a biometric system fails to recognize a legitimate user. A lower FRR means fewer legitimate users are inconvenienced.
- **GAN (Generative Adversarial Network)**: A type of AI model capable of producing highly realistic synthetic data (images, videos, or audio), raising the stakes for biometric spoofing and necessitating advanced liveness detection.
- **GDPR (General Data Protection Regulation)**: An EU regulation imposing strict data privacy and protection requirements on entities handling personal data, including biometric identifiers. Non-compliance risks significant penalties.
- **IR (Infrared)**: Light waves outside the visible range, used in various biometric sensors (e.g., iris recognition, palm vein) for imaging in low-light or contactless applications.
- **MFCC (Mel-Frequency Cepstral Coefficients)**: A common set of acoustic features representing how humans perceive sound frequencies, widely used in speaker identification systems.
- **MFA (Multi-Factor Authentication)**: A security model that requires multiple independent factors—something you know, have, or are—so that compromising one factor alone (e.g., a password) won't grant unauthorized access.
- **Minutiae**: Characteristic points in fingerprint ridges—bifurcations (forks) and endings—that form the basis of most fingerprint-based authentication.
- **Multi-Modal Biometrics**: Systems using two or more biometric modalities (e.g., fingerprint + face, or face + iris). They enhance accuracy, reduce spoof risk, and increase flexibility for users who struggle with a single modality.
- **Normalization**: The process of scaling or aligning biometric data into a standardized form (e.g., unwrapping an iris from circular to rectangular) to facilitate consistent feature extraction and comparison.
- **OTP (One-Time Password)**: A single-use code generated for a specific login session or transaction, commonly used alongside biometrics in layered security to reduce the risk of credential compromise.
- **PCA (Principal Component Analysis)**: A statistical technique for reducing dimensionality, often used in older facial recognition (Eigenfaces) or to simplify EEG signal data.
- **PCR (Polymerase Chain Reaction)**: A laboratory method of amplifying DNA segments, core to forensic DNA matching. Due to chemical steps and the need for specialized equipment, it's impractical for real-time identity checks.

- **PIN (Personal Identification Number)**: A numeric code used for authentication (e.g., ATM withdrawal). While not a biometric factor, PINs frequently combine with biometrics for multi-factor security.
- **Score-Level Fusion** A multi-modal approach merging numeric similarity scores from various biometrics (e.g., face, fingerprint) to produce an overall accept/reject decision.
- **Signature Dynamics**: A behavioral biometric that analyzes how a user signs their name (speed, stroke order, pressure) rather than relying on the static final image. Adds security against forgery but may fluctuate with user context.
- **Spoofing**: An attack where an adversary presents a fake or copied biometric (e.g., silicone fingerprint, photo of a user's face) to trick the system. Robust liveness detection helps mitigate these risks.
- **STQC (Standardization Testing & Quality Certification)**: An Indian certification for technology solutions, including biometric devices. Ensures products meet specific standards for performance and reliability (frequently referenced in Aadhaar-certified hardware).
- **STR (Short Tandem Repeats)**: Repetitive DNA sequences analyzed in forensic DNA profiling. Variation in STR lengths helps identify individuals accurately, although laboratory processing is needed.
- **Template**: The digital representation of extracted biometric features (e.g., fingerprint minutiae, face embeddings). Templates are usually smaller and encrypted for security reasons, rather than storing raw data.
- **User Profiling**: An advanced risk-based authentication strategy that aggregates multiple contextual and behavioral signals (e.g., login time, browser fingerprint, usage patterns). Deviations from a user's profile can trigger alerts or additional verification.
- **Vein Map**: A representation of subcutaneous vein structures captured by near-infrared scanning (palm or finger). Often stored as a branching graph. Vein biometrics are valued for their high spoof resistance.
- **VR (Virtual Reality)**: A fully simulated 3D environment accessed via headsets. VR devices may implement built-in biometric checks (e.g., eye-tracking) to authenticate users or personalize the virtual experience.
- **WebAuthn**: A W3C standard for passwordless web authentication. Allows devices to authenticate locally with biometrics or PIN, then prove identity to online services via public-key cryptography—without exposing raw biometric data to the server.

National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

The National Centre of Excellence (NCoE) for Cybersecurity Technology Development has been conceptualized by the Ministry of Electronics & Information Technology (MeitY), Government of India, in collaboration with the Data Security Council of India (DSCI). Its primary objective is to catalyze and accelerate cybersecurity technology development and entrepreneurship within the country. NCoE plays a crucial role in scaling and advancing the cybersecurity ecosystem, with a focus on critical and emerging areas of security.

Equipped with state-of-the-art facilities, including advanced lab infrastructure and test beds, NCoE enables research, technology development, and solution validation for adoption across government and industrial sectors. By adopting a concerted strategy, NCoE aims to translate innovations and research into market-ready, deployable solutions—contributing to the evolution of an integrated technology stack comprising cutting-edge, homegrown security products and solutions.

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

DATA SECURITY COUNCIL OF INDIA

+91-120-4990253 | ncoe@dsci.in

https://www.n-coe.in/

4 Floor, NASSCOM Campus, Plot No. 7-10, Sector 126, Noida, UP -201303

Follow us on

@CoeNational
nationalcoe
nationalcoe
NationalCoE