World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(Review Article)

Check for updates

Biometrics authentication trends and failures

Minul Mindula Subasinghe * and Don Nimeshi Lakshani Ranasinghe

Independent Researcher.

World Journal of Advanced Engineering Technology and Sciences, 2026, 18(02), 196-208

Publication history: Received on 04 January 2026; revised on 10 February 2026; accepted on 12 February 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.18.2.0088

Abstract

Biometric authentication is now central to modern identity and access management, offering stronger security and a better user experience than traditional passwords. From 2025 to 2026, advances in artificial intelligence, sensor technology, and decentralized identity models have broadened the adoption of biometric systems in consumer, business, and government sectors. However, emerging threats such as deepfakes, adversarial machine learning, and large-scale data breaches have exposed significant vulnerabilities and ethical issues. This paper reviews recent trends and shortcomings in biometric authentication, comparing major methods, including fingerprint, facial, iris, voice, and behavioral recognition. It assesses their performance, reliability, usability, scalability, and security, and examines the increasing adoption of multimodal, continuous, and privacy-preserving authentication systems. The analysis addresses key challenges, including spoofing, bias, template theft, and accessibility, to identify current system limitations. The paper proposes a layered mitigation framework that integrates technical safeguards, system design enhancements, governance measures, and user-focused strategies. It contends that the effectiveness of biometric authentication relies on both technological advancement and ethical, transparent practices that foster public trust. Addressing technical and social factors is essential to developing secure, fair, and widely accepted biometric systems.

Keywords*:* Biometric authentication; Identity and access management (IAM); Multimodal biometrics; Deepfake and spoofing attacks; Privacy and data protection; Behavioral biometrics; Bias and fairness in biometrics; Password-less authentication; Decentralized identity; Ethical and regulatory challenges

1. Introduction

Authentication is central to information security, as it determines how users prove their identity to access digital resources. While traditional methods focus on what users know, have, or are, the rise of biometrics over the past two decades signals a shift: the future of secure and user-friendly authentication lies in the growing adoption and challenges of biometric systems.

The problems with knowledge-based authentication, such as passwords, are well known. People frequently reuse passwords, choose weak ones, or lose them to phishing, malware, or data breaches. Methods that use what users already have, such as tokens, offer greater security but can still be lost, stolen, or copied. Biometric authentication leverages unique human traits that adversaries find hard to copy or share. Everyday devices now often include biometric sensors, which fuels broader adoption by providing a practical blend of security and convenience.

By 2025, biometric authentication will be a regular part of daily digital life. People use facial recognition to unlock phones and approve payments; fingerprints secure business systems and border control; iris scans protect critical infrastructure; and voice recognition helps in call centers and intelligent assistants. Behavioral biometrics, such as typing or walking patterns, are increasingly used for ongoing authentication and fraud detection.

* Corresponding author: Minul Mindula Subasinghe.

Even with these improvements, biometric authentication does not offer a perfect solution. If someone steals a fingerprint or facial data, they cannot change it like a password. This creates a lasting risk. Biometric systems also work probabilistically, so they sometimes incorrectly accept or reject users, which can cause problems. Concerns about surveillance, discrimination, consent, and the misuse of biometric data have grown, prompting greater regulation and public debate.

The years 2025 and 2026 mark a turning point for biometric authentication. New advances in artificial intelligence, sensors, and edge computing have made these systems more accurate, faster, and able to serve more users. However, advanced attacks, such as deepfakes, adversarial machine learning, and large-scale biometric data breaches, have revealed serious weaknesses. Meanwhile, changes in laws and data protection rules are shaping how people design and deploy biometric systems.

This article critically examines trends and failures in biometric authentication from this period. Its research goals are:

- To identify and characterise major technological and operational trends in biometric authentication between 2025 and 2026.
- To analyse key failure modes and vulnerabilities across different biometric modalities and deployment contexts.
- To compare biometric technologies in terms of performance, reliability, usability, security, and scalability.
- To propose mitigation frameworks that address both technical and non-technical risks.
- To examine ethical and regulatory considerations shaping the present and future of biometric authentication.

This article argues that, while technical innovation propels biometric authentication forward, the trustworthiness and societal impact of these systems hinge equally on how failures and ethical issues are addressed. Understanding current trends, vulnerabilities, and responsible risk management is essential to building authentication systems that are not only technically strong but also accepted and trusted by society.

2. Current Landscape & Trends (2025–2026)

Biometric authentication has moved from specialized security settings to a central part of modern identity and access management (IAM). Between 2025 and 2026, faster digital change, new rules, artificial intelligence (AI), new types of security threats, and changing user needs have pushed this shift. This section examines the main trends in biometric authentication over this period, drawing on recent research, industry reports, and real-world examples.

2.1. **Market Growth and Mainstream Adoption**

The world market for biometric systems is growing fast, pushed by demand from governments, businesses, banks, and users. Experts say the market will go from about USD 53 billion in 2025 to almost USD 95 billion by 2030. This means it will grow more than 12% each year (Security World Market, 2024). This shows biometrics are now a fundamental part of ID systems, not just an optional tool.

Consumer technology has made biometrics common. By 2025, over 70% of smartphones worldwide will have biometric sensors. Most will use them for fingerprint and facial recognition. (Qube Bio , 2025). As a result, using biometrics to unlock devices, make payments, and access apps is now commonplace.

2.2. **Password-less and Adaptive Authentication**

A significant trend in 2025 and 2026 is moving from passwords to password-less systems that use biometrics, such as fingerprints or facial recognition. Passwords are less secure due to phishing (tricking users into giving up passwords), reused passwords, and data breaches. Many groups are switching to biometric passkeys that follow standards such as FIDO2 (Fast Identity Online 2, a password-less authentication protocol) and WebAuthn (a web authentication protocol for password-less logins) (VSecure360, 2025).

Biometric authentication is central to password-less identity systems. Users can log in with facial recognition, fingerprints, or voice. They do not need to remember passwords. Studies show that biometric passkeys lower the risk of phishing and stolen credentials. This makes systems safer and easier to use (Forbes, 2025).

Adaptive authentication systems use biometrics and other information, such as device location, time of day, and risk scores (numbers that estimate the likelihood of a fake login attempt). The system changes its security checks based on this risk level. This aligns with zero-trust security models, which means never trusting any user or device by default and constantly verifying their identity. (Forbes, 2025).

2.3. Multimodal and Hybrid Biometric Systems

Multimodal biometric systems use two or more biometric types, such as face and fingerprint or iris and voice, making them more accurate and harder to fool. Some systems even combine behavioral traits (how someone acts) with physical characteristics (how someone looks or sounds)

Studies show that multimodal systems outperform single-mode systems in terms of accuracy and security. This is especially true in high-risk areas such as border control, critical infrastructure, and finance. (Al-Refai, et al., 2025). Using multiple biometric types improves reliability and accessibility.

Recent research shows that different types of biometrics are changing in how well they work. Fingerprints still perform well, but facial recognition has improved dramatically because of deep learning (a type of artificial intelligence that trains computers to learn from large amounts of data), so the difference in accuracy between them is now minor. (Al-Refai, et al., 2025). This means it is essential to pick the best method for each situation.

2.4. Contactless and Touchless Authentication

The COVID-19 pandemic led to more use of contactless biometric tech. This trend keeps going in 2025 and 2026. Touchless systems, such as face recognition, iris scanning, palm vein recognition, and camera-based fingerprint scanning, help people avoid touching shared devices and keep public places cleaner (Forbes, 2025)

Studies show that touchless fingerprint recognition using camera-based systems can achieve the same accuracy as traditional sensors. These systems are easier to use and last longer. (Zhang, et al., 2024). They are helpful in busy places like airports, hospitals, and retail kiosks.

Contactless biometrics help people with mobility challenges or those who cannot use physical sensors easily. As a result, touchless authentication is now standard in public biometric systems.

2.5. Artificial Intelligence and Deep Learning Integration

Artificial intelligence (AI), intense learning (a subset of AI that uses complex algorithms and neural networks to learn from large datasets), is now a key part of biometric authentication. Deep neural networks (computer systems modelled on the human brain) help better find and match features for face, voice, fingerprint, and iris checks. (Alduhailan, et al., 2025).

Studies show deep learning works much better than older rule-based methods, especially in challenging situations. (Alduhailan, et al., 2025). For example, in facial recognition, neural networks handle changes in lighting, position, age, and expression well. In voice recognition, new models do better even when sounds change.

But using AI also brings new risks, such as making systems easier to hack, harder to explain, and possibly unfair if the training data is unbalanced. (Alduhailan, et al., 2025) . Because of this, more research is underway to make AI more straightforward to use, train it more effectively, and build fairer systems.

2.6. Behavioral and Continuous Authentication

Traditional biometric systems verify user identity only at specific times. This includes during login or when approving a transaction. Due to rising cyber threats, there is a move toward continuous authentication. These systems monitor user identity throughout a session using behavioral biometrics.

Behavioral traits, such as how someone types, moves a mouse, uses a touchscreen, walks, or holds a device, can be used to verify identity all the time. Users do not have to do anything special. These systems can spot odd behavior that may indicate an account is hacked, a session has been taken over, or an insider threat is present. This allows quick action. (Forbes, 2025)

Research suggests behavioral biometrics work best when combined with physical biometrics. Hybrid systems are both secure and easy to use (Forbes, 2025). Continuous authentication marks a shift from one-time checks to ongoing identity assurance.

2.7. Privacy-Preserving and Decentralized Identity Models

Storing biometric data in large central databases raises privacy and security concerns, prompting interest in privacy-first, distributed ID systems. Techniques such as homomorphic encryption (encryption that allows computations on encrypted data), secure multi-party computation (joint data processing without sharing raw data), federated learning (training AI models across devices without centralizing data), and zero-knowledge proofs (showing something is accurate without revealing the underlying data) enable biometric matching without sharing raw information.

Decentralized ID systems let users store their biometric info on their own devices, usually in secure hardware (such as a secure chip inside a phone). They use cryptographic proofs (mathematical methods to confirm identity) instead of sending biometric data to central servers. This fits with data protection rules such as the General Data Protection Regulation (GDPR) in Europe and new EU ID standards.

Studies show decentralized biometric systems lower the impact of data breaches, build user trust, and help meet regulatory requirements. However, there are still challenges. These include integrating systems, scaling, and setting standards. (Forbes, 2025).

2.8. Biometric Payments and Frictionless Commerce

Biometric authentication is changing shopping both online and in person. More stores now use facial recognition, palm vein scanning, and fingerprint authentication for payments, transit, and ID checks. (VSecure360, 2025)

Pilot programs in countries like India show that large-scale biometric payment systems are possible. For example, the use of Aadhaar-based facial authentication for large financial transactions indicates that institutions are becoming more confident in biometric security. (Times of India, 2025).

Biometric payments are easy to use and can cut fraud. But they also raise concerns about consent, data storage, and surveillance. This means strict rules and oversight are needed. (VSecure360, 2025).

2.9. Regulatory and Ethical Imperatives

As biometric authentication spreads, people are paying more attention to right and wrong issues, mainly privacy, watching, bias, and blame. People and groups want stronger laws to regulate biometrics, especially in public and by law enforcement. (The Guardian, 2025).

In Europe, biometric data is a specific type of personal data under the GDPR. This gives it extra protection and rules. Regulators are also making new rules for AI and automated systems that use (Biometrics Research Group, 2025).

Around the world, biometric rules vary. Some places have strict limits or bans on biometric surveillance, while others use these systems more widely in government and national ID programs. This shows that we need global standards and clear ethical rules. (Biometrics Research Group, 2025).

2.10. Deepfake and AI-Generated Threat Mitigation

Generative AI has created new threats to biometric authentication by making realistic deepfakes, including fake faces, voices, and actions. These tools make it easier to trick systems with fake identities, which current technology finds hard to detect.

Recent studies suggest using multiple layers of defense, such as dynamic biometric signals, ongoing authentication, and cryptographic checks, to combat deepfake attacks. Governments and cybersecurity agencies now see deepfake identity fraud as a national security issue, leading to more investment in detection tools and new regulations. (Biometrics Research Group, 2025).

2.11. Integration with IoT and Edge Computing

Biometric authentication is increasingly used in Internet of Things (IoT) systems, which include devices such as smart home appliances, connected cars, industrial equipment, and city sensors that communicate over the internet. Edge

computing (data processing on local devices rather than in large, remote data centers) enables biometric data processing closer to users, making systems faster and keeping more data private by sending less to the (Biotime Technology, 2026).

Studies show that edge-based biometric systems are more reliable in critical settings such as industrial control systems and healthcare, where real-time identity checks are crucial.

3. Failure Modes and Vulnerabilities

Biometric authentication systems have improved, but still face technical, operational, and social risks. Addressing these vulnerabilities is essential to developing reliable and secure systems. (Jain, et al., 2006) (Ratha, et al., 2001).

3.1. Spoofing and Presentation Attacks

After outlining general vulnerabilities, it is essential to examine specific technical attack types. Spoofing, also known as a presentation attack, occurs when someone uses a fake biometric sample, such as a copied fingerprint or artificial face, to trick a biometric sensor and impersonate someone else. (Galbally, et al., 2014) . Examples include:

- Fingerprint Spoofing: Using gelatine, silicone, or 3D-printed moulds to replicate fingerprints (Galbally, et al., 2014).
- Facial Spoofing: Using photographs, videos, masks, or deepfake-generated faces to deceive facial recognition systems (Galbally, et al., 2014)
- Voice Spoofing: Using recorded audio, voice synthesis, or voice conversion technologies to mimic a target speaker (Galbally, et al., 2014)
- Iris Spoofing: Using high-resolution printed images or textured contact lenses to replicate iris patterns (Galbally, et al., 2014)

Liveness detection methods such as pulse detection, blink analysis, texture checks, and challenge-response have improved. Yet attackers keep finding ways to bypass these defenses, especially as the rise of generative AI makes them more effective.

3.2. Adversarial Machine Learning Attacks

Modern biometric systems increasingly rely on machine learning algorithms that learn patterns from data to make decisions. Adversarial attacks, which use small, intentional changes to input data, can trick these models into making mistakes that people usually cannot. (Biggio & Roli, 2018).

Attackers use adversarial examples, specially crafted data inputs, to evade detection, impersonate users, or weaken systems by tampering with data. (Biggio & Roli, 2018). In biometrics, this often involves minor modifications to faces, voices, or fingerprints to bypass security measures. (Biggio & Roli, 2018).

3.3. Template Theft and Database Breaches

Biometric systems store digital versions of biometric traits, called templates, in databases. If templates are stolen through data breaches, insider activity, or supply chain attacks, the consequences can be severe. (Ratha, et al., 2001).

Unlike passwords, biometric templates cannot be changed. Stolen templates put a person's identity at risk, making them vulnerable to identity theft, fraud, and surveillance. (Ratha, et al., 2001). These can also be used to create fake biometric samples. (Jain, et al., 2006).

3.4. False Acceptances and False Rejections

Biometric systems work by comparing similarity scores against predefined thresholds to determine whether a match occurs. This process can lead to two main errors: false acceptance rate (FAR) and false rejection rate (FRR) (Jain, et al., 2006).

Lowering FAR improves security but may increase false rejections. Lowering FRR improves usability but can raise security risks. (Jain, et al., 2006) (Ratha, et al., 2001). In critical sectors such as border control and healthcare, both errors can have serious consequences. (Jain, et al., 2006).

3.5. Bias and Demographic Performance Disparities

A significant problem in biometric authentication is demographic bias: the system may perform differently for people of various races, genders, ages, ethnicities, or disabilities. (Jain, et al., 2006)

Bias may arise from non-diverse training data, poor algorithms, or limitations in sensors and environments, leading to unfair outcomes and reduced public trust. (Jain, et al., 2006) (Ratha, et al., 2001).

3.6. Usability and Accessibility Failures

Biometric systems must balance security, ease of use, and accessibility. Poor design frustrates users, hinders adoption, and can exclude people with disabilities or unusual biometric traits. (Jain, et al., 2006).

Fingerprint scanners may not work for people with worn fingerprints or certain skin conditions. Facial recognition struggles with coverings or appearance changes, and voice recognition fails in noisy environments. (Jain, et al., 2006) (Galbally, et al., 2014). These raise ethical and legal questions, especially where biometrics are required. (Ratha, et al., 2001).

3.7. Environmental and Operational Vulnerabilities

Biometric systems are sensitive to lighting, noise, humidity, temperature, sensor settings, and network connections. (Jain, et al., 2006) (Galbally, et al., 2014).

Problems also come from poor setup, inadequate staff training, poor integration with security systems, and inconsistent policy enforcement. (Ratha, et al., 2001).

3.8. Insider Threats and Abuse

Biometric systems face insider threats. Those with access to biometric data might misuse it for surveillance, profiling, or identity theft. (Ratha, et al., 2001).

Poor management, weak access controls, and insufficient auditing increase these risks. Using systems beyond their intended purposes can erode trust and violate ethical norms. (Jain, et al., 2006) (Ratha, et al., 2001) .

3.9. Comparative Performance Analysis

To understand the strengths and weaknesses of biometric authentication, it helps to compare different types based on accuracy, security, usability, scalability, and resilience.

3.10. Fingerprint Recognition

- Accuracy and Performance- Fingerprint recognition is a well-established and reliable method. Modern sensors and software are highly accurate in controlled settings, with few errors in accepting or rejecting users.
- Security - Fingerprints can be copied using molds, prints, or leftover residues. While liveness detection has improved, advanced attacks remain possible. If a fingerprint is stolen, it cannot be changed, which is a security risk.
- Usability and accessibility - Fingerprint recognition is quick and easy for most people. However, it may not work well for those with worn fingerprints, injuries, skin problems, or specific jobs.
- Scalability - Fingerprint systems are widely used in both personal and business settings because sensors are common and standards are in place.
- Resilience - Moisture, dirt, and temperature changes can affect how well fingerprint systems function.

3.11. Facial Recognition

- Accuracy and Performance- Facial recognition has become much more accurate thanks to deep learning. It works well in good conditions, but its performance drops in poor lighting, at odd angles, or with low-quality images.

- Security- Photos, videos, masks, or deepfakes can trick facial recognition. Liveness checks and anti-spoofing tools help, but they are not foolproof.
- Usability and accessibility - Facial recognition is easy to use and does not require touch. However, it may not work for people with facial differences, those who wear specific clothing, or those with privacy worries.
- Scalability - Facial recognition can be used for large-scale group identification and surveillance, but it raises important ethical and legal issues.
- Resilience - How well facial recognition works depends on the environment and the camera's quality.

3.12. Iris Recognition

Accuracy, Performance, and Security - Iris recognition is highly accurate because each person's iris pattern is unique and stable. It is often seen as one of the most reliable biometric methods. It is hard to copy someone's iris, and liveness checks make it even more secure. Still, in some cases, high-quality images can be used to trick the system.

- Usability and accessibility - Iris recognition requires users to align their eyes with a camera, which can be hard or uncomfortable for some people. It is also not common on most personal devices.
- Scalability - Iris recognition works well in secure settings, but regular consumers do not widely use it because of hardware and ease-of-use issues.
- Resilience - Lighting, eye health, glasses, and contact lenses can all affect how well iris recognition works.

3.13. Voice Recognition

- Accuracy and Performance- Voice recognition has improved significantly, but it still struggles with background noise, microphone quality, and changes in a person's voice due to illness, stress, or age.
- Security- Recordings, synthetic voices, or voice-changing tools can easily fool voice recognition. Deepfake audio has made these risks even greater.
- Usability and Accessibility- Voice authentication is convenient and hands-free but may exclude users with speech impairments or in noisy environments.
- Scalability - Voice recognition is well-suited for remote applications, such as call centers and virtual assistants.
- Resilience - How well voice recognition works depends on background noise, the communication channel, and the device used.

3.14. Behavioral Biometrics

Accuracy and Performance- Behavioral biometrics like keystroke patterns and walking style are somewhat accurate on their own but work much better when used with other methods.

- Security- It is hard to fake someone's behavior over time, so behavioral biometrics are practical for ongoing authentication and spotting fraud. Still, attackers might try to copy or model these behaviors.
- Usability and Accessibility- Behavioral biometrics usually run in the background and do not bother users, making them easy to use. However, they may not work well for people with unusual behaviors or disabilities.
- Scalability - Behavioral biometrics can be widely used online and do not require specialized hardware.
- Resilience - Changes in a person's behavior, devices, or environment can affect how well behavioral biometrics work.

3.15. Multimodal Systems

- Accuracy and Performance- Multimodal systems, which use more than one method, usually work better because they combine different strengths and cover each method's weaknesses.
- Security- Multimodal authentication is much harder to trick because an attacker would need to break into multiple systems simultaneously.
- Usability and Accessibility- Multimodal systems can be more inclusive by giving users different options. But if not well designed, they can become complicated and more challenging to use.
- Scalability - How well multimodal systems can be scaled depends on their design, the available hardware, and their ease of integration.
- Resilience - Multimodal systems handle changes in the environment and operations better than single-method systems.

4. Proposed Mitigation Frameworks

To address the weaknesses and risks of biometric authentication, it is essential to adopt a comprehensive, layered approach that integrates technical, organizational, legal, and ethical protections. This section suggests ways to reduce risks in four main areas: technical design, system architecture, governance and policy, and user-focused practices.

4.1. Technical Design and Algorithmic Safeguards

4.1.1. Robust Liveness Detection

Liveness detection plays a key role in preventing spoofing attacks. Some advanced methods are:

- Physiological Signals: Detecting pulse, blood flow, micro-movements, or skin conductivity.
- Behavioural Challenges: Requiring users to perform random actions, such as blinking, smiling, or speaking specific phrases.
- Multispectral Imaging: Using infrared, thermal, or depth sensors to capture features not visible in standard images.
- AI-Based Texture Analysis: Identifying artifacts indicative of spoofing materials or digital manipulation.

Liveness detection systems need regular updates to keep pace with new attack methods, especially those enabled by generative AI.

4.1.2. Secure Template Protection

It is essential to protect biometric templates. Some standard techniques are:

- Template Encryption: Use strong cryptographic algorithms to encrypt templates both when stored and during transmission.
- Cancellable Biometrics: Apply transformations to biometric data that cannot be reversed, so compromised templates can be revoked and replaced.
- Biometric Cryptosystems: Link biometric data to cryptographic keys rather than storing raw templates.
- Secure Enclaves: Store and process biometric data in secure hardware environments, like trusted execution environments (TEEs).

Adversarial Robustness

To reduce the risk of adversarial machine learning attacks, systems can use the following methods:

- Adversarial Training: Train models with adversarial examples to make them more robust.
- Input Validation and Sanitization: Check for and reject any unusual or suspicious inputs.
- Model Monitoring: Track model performance to detect drift, degradation, or signs of tampering.
- Explainability and Transparency: Use models and tools that are easy to interpret, so you can understand and check how the model behaves.

4.1.3. Bias Detection and Mitigation

To address demographic bias, it is essential to:

- Use diverse, representative datasets so that the training data reflects the full range of users.
- Conduct bias audits and testing by regularly checking how the system performs for different demographic groups.
- Design fairness-aware algorithms by including fairness goals and constraints in the model.
- Monitor performance continuously, track any disparities over time, and adjust models as needed.

4.1.4. System Architecture and Infrastructure Safeguards

Decentralized and Edge-Based Architectures

Relying less on centralized databases lowers the risk of data breaches and helps protect privacy. Some ways to do this are:

- On-Device Processing: Biometric matching happens directly on the user's device.

- Federated Learning: Models are trained across many devices, so raw data does not need to be collected in a single location.
- Decentralized Identity Frameworks: Users can manage their own biometric credentials and choose which identity details to share.

Défense-in-Depth and Zero Trust Models

Biometric authentication works best when it is part of a layered security system that includes:

- Multi-Factor Authentication (MFA): Biometrics are used alongside other factors to confirm identity.
- Continuous Risk Assessment: The system continuously checks device security, location, user behaviour, and network status.
- Least Privilege and Access Controls: Only people who need access to biometric data or systems, based on their role and risk, are allowed access.

Secure System Integration and Interoperability

Biometric systems need to integrate safely with existing IT systems, including identity management, access control, logging, and incident response tools. Using standard interfaces, secure APIs, and frameworks that support multiple systems helps reduce integration risks and strengthen the system as a whole.

4.1.5. Governance, Policy, and Organizational Controls

Legal and Regulatory Compliance

Organizations must comply with all laws and regulations that apply to biometric data, including:

- Data protection and privacy laws.
- Biometric-specific legislation.
- Sector-specific regulations (e.g., healthcare, finance, government).

Compliance should be built into the system design through privacy-by-design and security-by-design principles.

Ethical Oversight and Accountability

Ethical governance should cover the following areas:

- Ethics Committees or Review Boards: Evaluating biometric deployments for potential harms and benefits.
- Impact Assessments: Conducting biometric impact assessments (BIAs) and data protection impact assessments (DPIAs).
- Transparency and explainability: Provide clear information about how biometric systems function and how data is used.
- Accountability mechanisms: Set clear responsibilities, reporting channels, and steps for resolving issues.

Risk Management and Incident Response

Organizations should have comprehensive risk management plans that address:

- Threat Modelling: Identifying and prioritizing biometric-specific threats and vulnerabilities.
- Incident response plans: Be ready to handle data breaches, system failures, and misuse.
- Regular audits and assessments: Conduct internal and external reviews of biometric systems, policies, and controls.

4.1.6. User-centred Design and Trust-Building Practices

Informed Consent and User Agency

Users should have meaningful control over their biometric data, including:

- Clear and accessible information about data collection, use, storage, and sharing.
- Genuine choices about participation, where feasible.

- Options to withdraw consent and delete biometric data.

Consent processes should be explicit, voluntary, and appropriate to the situation in which they are used.

Accessibility and Inclusivity

Biometric systems should be accessible to everyone, including people with disabilities, individuals with unique biometric traits, and people with different cultural backgrounds. This involves:

- Offering alternative authentication methods.
- Testing systems with diverse user groups.
- Adhering to accessibility standards and guidelines.

User Education and Engagement

To build trust, organizations should inform users about:

- How biometric systems work.
- What risks exist and how they are mitigated.
- What rights users have and how to exercise them.

Including users as stakeholders supports acceptance, accountability, and shared responsibility.

4.2. Ethical and Regulatory Considerations

Biometric authentication brings up important ethical and regulatory questions that go beyond how well the technology works. These concerns involve fundamental rights, social values, power dynamics, and the interactions among people, organizations, and technology.

4.3. Privacy and Data Protection

Biometric data is very sensitive because it is tied to a person's identity and cannot be changed. Ethical and legal rules stress the importance of protecting this data from unauthorized access, misuse, or exploitation.

Some key privacy principles are:

- Data Minimization: Collecting only the biometric data necessary for a specific purpose.
- Purpose Limitation: Using biometric data solely for the stated and legitimate purpose.
- Storage Limitation: Retaining biometric data only as long as necessary.
- Security Safeguards: Implementing appropriate technical and organizational measures to protect data.
- Transparency: Informing individuals about data practices in clear and accessible terms.

Laws like the European Union's General Data Protection Regulation (GDPR) treat biometric data as a special type of personal information, which means it gets extra protections and restrictions.

4.4. Consent and Autonomy

Using biometrics ethically means getting real consent. But in practice, consent can be complicated by power imbalances, limited alternatives, or rules requiring biometrics to access essential services.

At work, in schools, in public services, and at borders, people may feel they have to give their biometric data to avoid adverse outcomes. This makes it unclear whether their consent is truly voluntary or valid.

Ethical guidelines recommend:

- Providing non-biometric alternatives where feasible.
- Ensuring consent is informed, specific, and revocable.
- Avoiding coercive or deceptive practices.

4.5. Surveillance, Social Control, and Chilling Effects

Biometric technologies, especially facial recognition, enable monitoring public and private spaces at scale and in real time. While this can improve security and efficiency, it also threatens civil liberties, free speech, and democratic participation.

Widespread biometric surveillance can:

- Enable pervasive monitoring of individuals' movements, associations, and behaviours.
- Facilitate profiling, discrimination, and social control.
- Create chilling effects that discourage lawful activities such as protest, assembly, or dissent.

Increasingly, ethical and legal discussions are about whether, when, and how biometric surveillance should be allowed, limited, or banned.

4.6. Bias, Fairness, and Non-Discrimination

Biometric systems can show demographic biases that often impact marginalized groups more than others. Ethical standards call for fairness, equity, and non-discrimination in these technologies.

Fixing bias takes more than just technical solutions. It also needs wider social and organizational efforts, such as:

- Inclusive design and stakeholder engagement.
- Transparency about system limitations and performance disparities.
- Accountability mechanisms for harm caused by biased systems.
- Legal remedies and oversight for discriminatory outcomes.

Laws and regulations are increasingly requiring bias testing, impact assessments, and records of fairness measures.

4.7. Accountability, Transparency, and Redress

Biometric systems often work in ways that are hard to understand, so people may not know how decisions are made or how to challenge them. Good governance requires accountability and transparency, such as:

- Clear documentation of system design, operation, and decision-making processes.
- Mechanisms for individuals to access, correct, or delete their biometric data.
- Processes for appealing or contesting biometric-based decisions.
- Independent oversight and audits.

If these safeguards are missing, people may lose trust in biometric systems, and the systems could lose legitimacy and fail to comply with essential rules.

4.8. Global Regulatory Landscape

By 2025 and 2026, rules for biometric authentication worldwide are becoming more complex and varied. Some main trends are:

- Europe has strong data protection laws, treats biometric data as sensitive, and is paying more attention to facial recognition and AI systems.
- In the United States, there is a mix of federal, state, and local laws. Some places have strict rules or a ban on specific biometric uses.
- In Asia, both public and private sectors are quickly adopting biometrics, and the rules are changing to keep up.
- Groups such as ISO, IEC, and IEEE are developing technical and ethical standards for biometrics worldwide.

Organizations operating in different countries must navigate diverse laws, cultural practices, and ethical standards.

5. Conclusion

Biometric authentication now plays a key role in modern identity and access management, making processes more convenient, efficient, and secure. From 2025 to 2026, the field has seen significant improvements in accuracy, scalability,

and integration, thanks to advances in artificial intelligence, multimodal systems, contactless technology, and decentralized identity frameworks.

Despite these advances, key vulnerabilities and challenges remain. Biometric systems can still be tricked, attacked, or breached, and they may show bias or be misused. Because biometric traits cannot be changed, any compromise has lasting effects. Differences among groups and concerns about surveillance also risk undermining trust, fairness, and legitimacy.

This article has shown that biometric authentication is not just a technical tool, but part of a larger system shaped by organizations, laws, and ethics. To address risks, we need a broad approach that combines strong technical protections, reliable system design, sound governance, and a user-focused approach.

Future research and practice should focus on the following areas:

- Improving privacy-preserving and decentralized biometric technologies.
- Creating standard ways to detect, reduce, and take responsibility for bias.
- Making regulations stronger and improving international cooperation.
- Making systems more transparent, easier to understand, and giving users more control.
- Encouraging people from technology, policy, ethics, and other fields to work together.

In the end, biometric authentication will only succeed if it works well and earns lasting trust from society. By facing problems, fixing weaknesses, and acting ethically, these systems can become safer, fairer, and more reliable for digital identity in the future.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] VSecure360, 2025. Top Biometric Industry Trends & Transformations to Watch In 2025. [Online] Available at: https://vsecure360.com/2025/09/09/biometric-industry-trends-2025/?utm_source [Accessed 28 November 2025].

[2] Alduhailan, A., Kamarudin, N. H. & Dau, S. N. H. S. A. a. A., 2025. Deep Learning in Biometric Authentication: Challenges, Recent Advancements, and Future Trends. Journal of Advances in Information Technology, 16(4), p. 458–472.

[3] Al-Refai, R. et al., 2025. A Comprehensive Re-Evaluation of Biometric Modality Properties in the Modern Era, New York: Cornell University.

[4] Biggio, B. & Roli, F., 2018. Wild patterns: Ten years after the rise of adversarial machine learning. Science direct, Volume 84, pp. 317-331.

[5] Biometrics Research Group, 2025. Digital trust: Reflections on 2025 and outlook for 2026. [Online] Available at: https://www.biometricupdate.com/202512/digital-trust-reflections-on-2025-and-outlook-for-2026?utm_source
[Accessed 8 December 2025].

[6] Biotime Technology, 2026. Biometrics in 2026: which trends will transform security?. [Online] Available at: https://www.biotime-technology.com/en/biometrics-in-2026-which-trends-will-transform-security/?utm_source
[Accessed 18 January 2026].

[7] Forbes, 2025. The Future Of Authentication: Why AI And Biometrics Will Replace Passwords For Good. [Online] Available at: https://www.forbes.com/councils/forbesbusinessdevelopmentcouncil/2025/06/05/the-future-of-authentication-why-ai-and-biometrics-will-replace-passwords-for-good/
[Accessed 24 November 2025].

[8] Galbally, J., Marcel, S. & Fierrez, J., 2014. Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. IEEE , 23(2), pp. 710 - 724.

[9] Jain, A., Ross, A. & Pankanti, S., 2006. Biometrics: a tool for information security. IEEE Xplore, 1(2), pp. 125 - 143.

[10] Qube Bio , 2025. Global Biometric Market Update: Where Our Tech Stands in 2025. [Online] Available at: https://www.qubebio.com/global-biometric-market/?utm_source [Accessed 28 November 2025].

[11] Ratha, N. K., Connell, J. H. & Bolle, R. M., 2001. Enhancing security and privacy in biometrics-based authentication systems. IEEE, 40(3), pp. 614 - 634.

[12] Security World Market, 2024. TheUnited Kingdom Security Market. [Online] Available at: https://www.securityworldmarket.com/uk/News/Business-News/biometrics-systems-market-to-show-strong-growth-to-20301?utm_source
[Accessed 09 December 2025].

[13] The Guardian, 2025. Facial recognition technology needs stricter regulation. [Online] Available at: https://www.theguardian.com/technology/2025/jun/17/facial-recognition-technology-needs-stricter-regulation?utm_source
[Accessed 7 December 2025].

[14] Times of India, 2025. NPCI may allow Aadhaar-based face authentication for high-value transactions.. [Online] Available at: https://timesofindia.indiatimes.com/technology/tech-news/npci-may-allow-aadhaar-based-face-authentication-for-high-value-transactions/articleshow/124381239.cms?utm_source
[Accessed 3 December 2025].

[15] Zhang, L., Chen, H. & Wang, Y., 2024. Touchless fingerprint recognition using camera-based imaging. Computer Vision and Image Understanding. ScienceDirect, Volume 238, p. 103–118