International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V6I4P118
Eureka Vision Publication | Volume 6, Issue 4, 125-127, 2025

Original Article

Biometric Authentication UX: Best Practices for Face ID, Fingerprint & Iris Scans

Sajindas Devidas
Independent Researcher, USA.

Received On: 21/10/2025 ***Revised On: 13/11/2025*** ***Accepted On: 21/11/2025*** ***Published On: 28/11/2025***

Abstract - Biometric authentication methods such as Face ID, fingerprint, and iris scans are now common in digital banking, mobile apps, and high-security systems. This paper analyzes best practices in designing user-friendly biometric authentication, focusing on UX patterns, accessibility, privacy, and security. Based on current research, industry guidelines, and application in finance, the goal is to help designers build secure and trustworthy interfaces that are easy for all users while complying with regulations. Design principles, usability outcomes, technical barriers, and future trends are discussed, with IEEE-style references and clear formatting for direct practical use.

Keywords - Biometric Authentication, UX, Face ID, Fingerprint, Iris Scan, Usability, Security, Accessibility, Privacy, Digital Banking.

1. Introduction

With the rising adoption of digital channels, secure and user-friendly authentication is critical. Biometric authentication (using fingerprints, facial structure, or iris patterns) is favored for its speed, convenience, and resistance to credential theft. However, poor UX or insufficient fallback options can lock out users and reduce trust. This paper focuses on best practices for integrating biometric methods into user journeys, especially in sensitive sectors like digital banking and finance.

Figure 1. Biometric Authentication

2. Biometric Authentication Methods

Table 1. Comparison of Major Biometric Methods

Method	Description	Pros	Cons
Face ID	Scans face structure via camera	Touchless, fast, accessible	Sensitive to lighting, may fail with masks
Finger Print	Scans fingerprint via sensor	Familiar, fast	Needs a clean, functional sensor and skin
Iris Scan	Scans unique iris patterns	High accuracy, touchless	May require precise positioning, more expensive hardware

3. User Experience Best Practices

3.1. Clear Instructions and Feedback

To optimize the user experience for biometric authentication, it is important to always present users with simple, action-oriented prompts, such as "Look at the screen" or "Place finger on sensor," so that instructions are easy to understand and follow. Additionally, the interface should provide clear visual or haptic feedback while the system is processing or if an error occurs, using elements like a loading spinner or a short vibration to reassure users or guide them through the process.

3.2. Fallback and Recovery Mechanisms

To ensure accessibility and a smooth user experience, biometric authentication systems should always offer fallback options such as PINs, passwords, or security questions for users who might encounter issues due to injury, disability, wet fingers, or poor lighting. When a biometric attempt fails, the system should guide the user gently by offering helpful tips – for example, suggesting to try better lighting – rather than resorting to immediate lockouts, so users are never left stranded or frustrated.

3.3. Accessibility and Inclusion

When designing biometric authentication flows, it is essential to consider users who may not be able to use face, fingerprint, or iris scans due to medical, physical, or religious reasons. Providing alternative authentication methods and ensuring these flows are inclusive allows everyone to access services securely. It is also important to test biometric onboarding and usage with assistive technologies, such as screen readers and voice controls, so users with visual or motor impairments receive accessible, clear instructions and feedback throughout the process.

3.4. Privacy by Design

Biometric data should be processed and stored securely, with a strong preference for on-device storage to maximize user privacy and reduce risks from cyberattacks or central data breaches. In addition, organizations must clearly communicate their privacy policies and explain how biometric data is used, collected, and protected. To build trust, users should be able to easily opt out or delete their biometric data, with straightforward workflows that ensure proper removal not only from live systems but also from backups and associated platforms.

3.5. Minimize Friction

Biometric authentication flows should enable users to unlock their devices or accounts instantaneously following a successful scan, with minimal or no perceptible waiting time to maximize convenience and satisfaction. It is also important to limit the number of repeated biometric prompts during a single session, as unnecessary re-authentication can quickly lead to user frustration and reduced trust in the system.

4. Security Considerations

For sensitive transactions or situations requiring higher security, it is beneficial to use multi-modal biometrics by combining methods such as Face ID, fingerprint, or voice recognition, which greatly increases the difficulty of unauthorized access while providing flexibility for different user needs. Security can be further enhanced through liveness detection, such as checking for eye blinks or natural movements, to prevent spoofing attempts with photos, masks, or artificial fingerprints. To stay ahead of emerging threats, security models should be updated regularly to adapt to new spoofing methods and device vulnerabilities, and organizations should routinely conduct fairness audits to detect and correct any bias in recognition accuracy across various skin tones, age groups, or abilities, ensuring equitable user experiences.

5. Challenges and Solutions

Table 2. Common Biometric UX Challenges and Solutions

Challenge	Impact	Best Practice Solution
Lighting/fingerprint quality	Failed authentication	Use multi-modal biometrics, fallback UX
Accessibility barriers	Excludes some users	Alternative flows, inclusive testing
Privacy concerns	User mistrust, compliance risks	On-device storage, transparency, opt-out
False positives/negatives	User lockout or security risk	Liveness checks, adaptive models

Figure 2. Common Biometric UX Challenges

6. Case Study: Banking App Biometric UX

In mobile banking, fingerprint authentication is the most widely used due to its speed and reliability. Recent studies show a false acceptance rate as low as 0.0001%, with integrated fallback measures improving user satisfaction by 35% in major US and European banking apps. Privacy concerns are addressed by processing fingerprints on the user's device, never transmitting data to the cloud.

7. Future Trends

The adoption of multi-modal biometrics, which combines methods such as face, fingerprint, iris, and voice recognition, provides higher security assurance and greater accessibility for diverse user needs. Non-contact and behavioral biometrics, including voice, gait analysis, or facial recognition, are increasingly preferred for hygiene and

enable passive authentication without requiring any physical touchpoint, thus improving both user experience and public health considerations. As biometric solutions advance, they are being more deeply integrated with IoT ecosystems and wearable technology, allowing secure and seamless biometric unlocks across multiple devices and environments—from smartphones to smart homes and health devices. Alongside these innovations, privacy regulations are becoming more robust, with growing interest in decentralized privacy frameworks such as blockchain and on-device storage, which empower users to control their own biometric data and reduce risks from centralized repositories or mass data breaches.

8. Conclusion

Effective biometric authentication UX means balancing security, privacy, and usability. Designers should offer clear instructions, fast and forgiving flows, visible feedback, accessible alternatives, and transparent privacy protections. With multi-modal authentication and privacy-centric design, biometric UX in finance and other sectors can be both trustworthy and inclusive.

References

[1] T. Williams, "Personalized Banking: The AI Advantage," Alkami, Mar. 2025.

[2] "Biometric Authentication Design: Lessons from Sci-Fi," Bits Kingdom, Aug. 2025. https://bitskingdom.com/blog/biometric-authentication-ux-lessons/

[3] "What's on the Horizon: 10 Biometric Trends for 2025," HID Global, Jan. 2025. https://blog.hidglobal.com/whats-horizon-10-biometric-trends-2025

[4] "Biometric Authentication Systems in Banking," IEEE Xplore, Jul. 2024. https://ieeexplore.ieee.org/document/10731026/

[5] "Navigate biometric data protection with confidence in 2025," TrustCloud, Jul. 2025. https://community.trustcloud.ai/docs/grc-launchpad/grc-101/governance/biometric-data-protection-emerging-technologies-and-privacy-concerns-in-2024/

[6] "AI-Powered Financial Assistants: Designing for Proactive Money Management," Oct. 2025.

[7] "Transforming UX with Biometric Authentication," Mantra Labs, May 2023. https://www.mantralabsglobal.com/blog/transforming-ux-with-biometric-authentication/

[8] "Advancements in Biometric Security: What to Expect in 2025," Security Force Now, Jan. 2025. https://securityforcenow.com/advancements-in-biometric-security-what-to-expect-in-2025

[9] "Biometric authentication: A comprehensive guide," Descope, Jun. 2025. https://www.descope.com/learn/post/biometric-authentication

[10] M. Thompson, "AI in Banking: 7 Game-Changing Applications," Netscribes, May 2025

[11] Kanji, R. K. (2020). Federated Learning in Big Data Analytics Privacy and Decentralized Model Training. Journal of Scientific and Engineering Research, 7(3), 343-352.