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

(RESEARCH ARTICLE)

Check for updates

Biometric-Sealed Keys Using iOS Secure Enclave for Zero-Trust On-Device Security

Venkata Kalyan Pasupuleti *

Independent Researcher, Cumberlands and Silicon Valley University.

World Journal of Advanced Engineering Technology and Sciences, 2026, 18(02), 034-040

Publication history: Received on 20 December 2025; revised on 28 January 2026; accepted on 31 January 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.18.2.0062

Abstract

The ongoing evolution of cybersecurity has necessitated a paradigm shift toward zero-trust architectures, in which no single component, user, or device is inherently trusted. In this context, the emerging technology of on-device security (such as iOS Secure Enclave based on biometric-sealed keys) can be regarded as a novel security system wherein cryptographic functions are hard-bound to user-specific biometric data stored within a secure, non-exportable enclave. This review discusses the technical foundation of biometric-sealed keys, privacy-preserving biometric systems, and their integration with federated identity and post-quantum cryptography. The importance of mutable biometrics, the generation of dynamic keys utilizing fuzzy logic, and low-latency encryption in relation to multi-hop authentication are further examined. Despite the considerable advantages, fallback vulnerabilities, device interoperability issues, and ethical concerns must also be considered in efforts to fully harness the potential of this technology. Privacy-first security architectures will be redefined through biometric sealing and secure execution environments that are resilient to hardware-level attacks and aligned with zero-trust principles in the modern digital ecosystem.

Keywords: Biometric-Sealed Key; Ios Secure Enclave; Zero-Trust Architecture; On-Device Security

1. Introduction

The increasing complexity of cybersecurity challenges, alongside the proliferation of digital ecosystems, has transformed the role of data privacy and device-level security. The shift toward zero-trust architecture and away from perimeter-based security models is driven by growing concerns over unauthorized access, device compromise, and data exfiltration. Within this framework, every device, application, and user must continuously verify its trustworthiness. One of the most forward-looking approaches in this area is the implementation of biometric-sealed keys on secure hardware platforms such as Apple's iOS Secure Enclave, which enables cryptographic operations to be gated by biometrics and locally constrained.

Biometric-sealed key technology utilizes physiological or behavioral data—such as fingerprints or facial features—to bind and unlock cryptographic keys stored in a secure, isolated environment. The iOS Secure Enclave is a Trusted Execution Environment (TEE) that leverages hardware to enhance the protection of sensitive data by performing secure operations within a subsystem that is physically isolated. These technologies can be deployed within a zero-trust security framework to provide robust user authentication and cryptographic operations, even under untrusted network conditions or when operating systems are compromised.

This brief examines the intersection of biometric-sealed keys, the iOS Secure Enclave, and zero-trust systems, and how these three components are combined to usher in a new era of on-device protection. The paper will also include a comparison of emerging techniques and technologies, an analysis of practical implementations, and an assessment of potential weaknesses and limitations in current research.

* Corresponding author: Venkata Kalyan Pasupuleti.

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0.

2. The Evolution of Biometric-Based Security Mechanisms

The ubiquitous use of biometrics in identity verification and access control has evolved into an important tool in encryption key management. Traditional forms of authentication, such as passwords and PINs, are no longer sufficiently effective due to their susceptibility to phishing, brute-force attacks, and poor user practices. The non-transferability and difficulty of forging biometric traits offer distinct advantages by making them harder to compromise; however, they also introduce challenges, particularly in cases involving compromised or irreversibly lost biometric templates.

Recent studies indicate converging tendencies between biometric authentication and cryptographic sealing, where user biometrics are no longer merely used to unlock devices but are directly involved in guiding cryptographic operations. These advancements depend on enhanced sensor precision, real-time processing capabilities, and the secure storage of biometric templates [1].

Apple's Secure Enclave utilizes biometric information through Touch ID and Face ID, where the biometric templates are encrypted and stored locally in a manner that is inaccessible to both the application layer and the operating system. This architecture ensures that biometric data cannot be leaked or transferred, making biometric-sealed keys both feasible and secure within the on-device environment—particularly in the context of zero-trust systems [1].

3. Privacy-Preserving Biometric Techniques

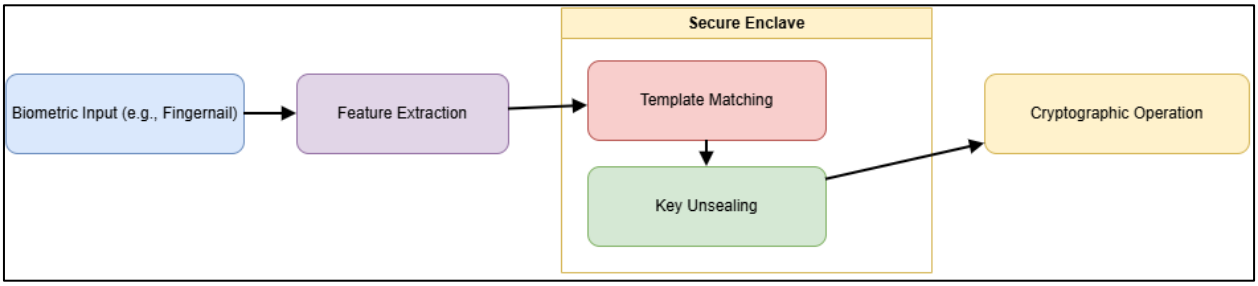
The zero-trust environment will inherently incorporate privacy preservation. Once compromised, biometric data cannot be revoked or altered, making robust protection measures essential. Research into privacy-sensitive approaches—such as cancellable biometrics, biometric cryptosystems, and homomorphic encryption—aims to mitigate this vulnerability. These techniques are designed to maintain the accuracy and effectiveness of biometric authentication while transforming or obscuring the raw biometric template to safeguard user privacy.

Computational efficiency remains the primary challenge in applying these solutions to consumer devices. Fuzzy vaults and fuzzy commitment schemes, while effective in binding cryptographic keys to secure biometric data, often involve performance trade-offs. Additionally, for these mechanisms to be viable in everyday environments, they must demonstrate low false acceptance rates (FAR) and false rejection rates (FRR) [2].

The computational requirements are managed by specialized hardware capable of performing real-time encryption and decryption without exposing biometric data, using the biometric-sealed key algorithm within the Secure Enclave. In addition, the architecture supports non-exportable keys, ensuring that the key material remains inaccessible and cannot be exported or utilized by other devices [2].

4. Mutable Biometrics and Device-Level Adaptability

Though traditional biometric systems utilize immutable biological traits, current trends are promoting changeable biometrics, where elements such as fingernails or even behavioral characteristics can change slightly over time. Such fluid biometric systems enhance resilience to re-enrollment while maintaining a high level of security and privacy. The NailKey system, for instance, is based on fingernail patterns that are unique yet slightly modifiable, making it well-suited for implementing revocable biometrics in secure environments [3]. Figure 1 illustrates the concept of mutable biometric input and its interaction with hardware-backed secure elements.



Source: Adapted from [3]

Figure 1 Conceptual Diagram of Mutable Biometric-Sealed Key Lifecycle Using Secure Enclave

This is a flexible feature that proves useful in zero-trust environments, where continuous authentication and adaptability are essential. Unlike permanent biometrics, mutable biometrics can support lifecycle management without exposing users to the risk of total identity theft, thereby enhancing both user privacy and system resilience [3].

5. Federated Identity Systems and EUDI Wallet Integration

A key application of biometric-sealed key systems is the development of federated identity platforms, such as the European Digital Identity (EUDI) Wallet. These platforms utilize passkeys and remote Wallet Secure Cryptographic Devices (WSCDs) as authentication mechanisms that operate not only across countries but also across multiple services. In such implementations, biometrics are used to verify the user and to unlock passkeys, which are then employed for cross-platform identity verification [4].

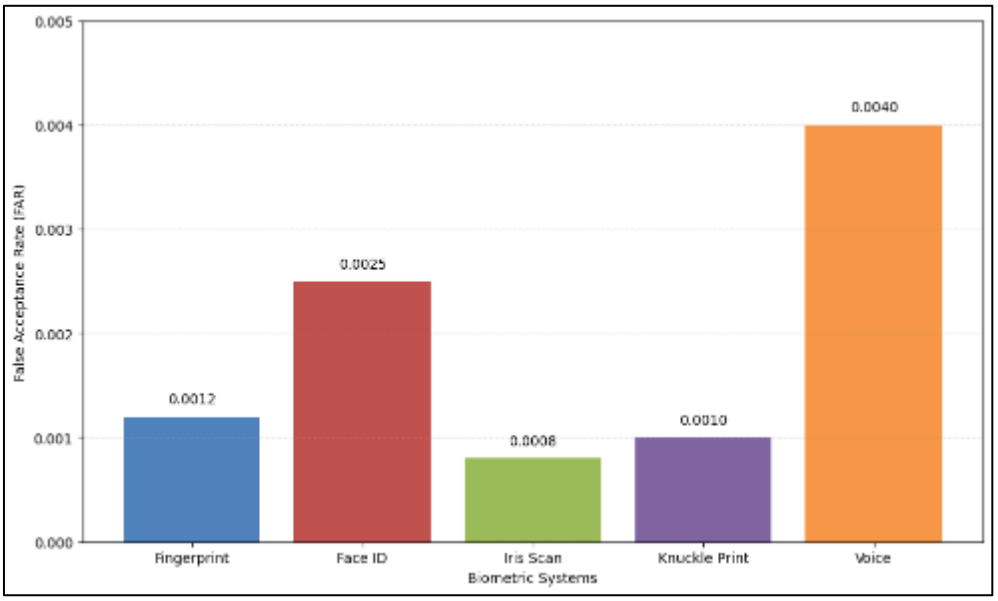
The EUDI Wallet consists of biometric-based passkeys that are stored within a secure enclave or a hardware token. When a user attempts to establish a connection, the enclave compares the stored biometric data with a newly captured sample, and upon successful verification, the user is permitted to utilize the relevant passkey. This model also ensures that passkeys are non-phishable and device-bound, aligning with the principles of zero-trust security, in which each authentication request is independently verified [4].

The Secure Enclave plays a critical role in minimizing the attack surface—not only for biometric information but also for the key material and execution environment—thereby reducing vulnerability even when operations are conducted over publicly accessible or potentially compromised networks.

6. Knuckle Print Authentication and Template Protection

In addition to traditional methods of identification such as fingerprints and facial recognition, new biometric identifiers—such as knuckle prints—have been introduced. These features are unique and relatively stable, with the added benefit of being difficult to spoof due to their three-dimensional geometry. Template protection systems, known as knuckle print systems, exemplify how alternative biometric modalities can be effectively secured through techniques such as encryption, hashing, and feature transformation [5].

Figure 2 demonstrates the performance efficiency of various biometric template protection schemes including knuckle print-based systems.



Source: Adapted from [5]

Figure 2 Graph Showing Comparative False Acceptance Rates (FAR) for Different Biometric Template Protection Methods

When these systems are implemented within secure hardware environments, they benefit from an added layer of encryption through sealing. The risk of biometric data leakage is further reduced by template transformation schemes, as the templates cannot be reversed or reused—even in cases of theft. Additionally, they can be re-issued with modified templates, which is well-suited to compromised environments and aligns with zero-trust principles, where frequent re-authentication and template regeneration are necessary requirements [5].

7. Post-Quantum Cryptography and Multi-Factor Authentication

Post-quantum cryptography (PQC) is being used to future-proof the latest implementations of biometric-sealed key systems. As quantum computers pose a growing threat to the security of classical encryption algorithms, PQC must be integrated into cloud-based multi-factor authentication (MFA) systems. These implementations leverage device-bound biometrics, PQC algorithms, and Trusted Execution Environments (TEEs) to ensure quantum resilience and robust local authentication [6].

In these systems, biometric information stored within the enclave is used to unlock keys that are processed using post-quantum algorithms to perform transactions in the cloud. The operations within the enclave are secure to the extent that neither biometric templates nor key materials are exposed during the authentication lifecycle. This interaction enables secure cross-platform operations without compromising privacy or introducing vulnerabilities, as is often the case with traditional Public Key Infrastructure (PKI) systems [6].

8. Cryptographic Key Generation Through Fuzzy Logic

Biometric-sealed key systems are largely characterized by dynamic key generation. Unlike traditional systems based on fixed keys, modern implementations are designed to generate cryptographic keys dynamically using fuzzy logic. This approach allows for a degree of tolerance to minor discrepancies in biometric input, which is crucial for ensuring user acceptance and reliability in practical applications.

In the latest models, the use of fuzzy logic has been proposed for evaluating biometric input vectors, generating cryptographic material, and enabling on-demand key regeneration. Fuzzy logic-based real-time cryptographic systems have been shown to offer greater flexibility and security in resource-constrained environments such as smartphones. This ensures that keys can be generated and sealed even when biometric capture conditions are suboptimal [7].

Table 1 summarizes the operational differences between static and fuzzy logic-based dynamic key generation.

Table 1 Comparison of Static and Fuzzy Logic-Based Dynamic Key Generation

Feature	Static Key Generation	Fuzzy Logic-Based Generation
Key Reusability	High	Low (New key per session)
Tolerance to Input Variance	Low	High
Biometric Input Sensitivity	Strict Match Required	Approximate Match Supported
Suitability for On-Device Usage	Moderate	High
Support for Template Privacy	Limited	Enhanced via Key Volatility

Source: Adapted from [7]

9. Secure Hardware Enclaves and Blockchain Integration

The intersection of blockchain applications with Secure Enclave solutions is becoming increasingly relevant, as decentralized systems require high-quality key management on devices. Notably, Hyperledger Fabric is a permissioned blockchain system where strict identity control and secure transaction signing are essential. Traditional key storage mechanisms in blockchain systems typically rely on local files or software-based wallets, which leave private keys vulnerable—particularly when devices are infected with malware or targeted by phishing attacks.

To address this, recent researchers have deployed Intel Software Guard Extensions (SGX) alongside blockchain infrastructures to create sealed environments for key management. These secure spaces prevent cryptographic keys from being accessed by any unauthorized process, including privileged system software. This model ensures that all

signing-related operations for blockchain transactions are performed within the enclave, maintaining the privacy and integrity of the cryptographic materials [8].

This architecture resembles the iOS Secure Enclave, which similarly ensures that cryptographic operations are executed within the enclave. However, biometric gating is also a unique strength of iOS, meaning that even access to cryptographic capabilities is governed by biometric verification. The combination of these two paradigms—biometric sealing and secure hardware execution—offers a very high level of assurance that private keys used in decentralized systems are not only non-exportable but also human-bound and biometrically secured [8].

This level of isolation is particularly valuable in zero-trust environments, where the system operates under the assumption that all components outside the secure enclave may be compromised. In such scenarios, the enclave functions as a self-contained trust anchor, and biometric controls serve as the final layer of authentication, linking the cryptographic key to the legitimate user.

10. Multi-Hop Authentication and Low Latency Encryption

The second area where biometric-sealed keys and secure enclaves could offer revolutionary benefits is in multi-hop biometric authentication. As data or access control requests traverse multiple nodes within a distributed system, maintaining the continuity of the authentication process becomes challenging without introducing new vulnerabilities. Traditional hop-by-hop models—based on credentials or token passing—are susceptible to man-in-the-middle attacks and session hijacking.

The concept of low-latency encryption in multi-hop biometric authentication systems can address these challenges by generating temporary keys at each hop through local biometric authentication. Each node biometrically verifies the user, encrypts a key within the enclave, encrypts the data, and then transmits it forward. This architecture reduces the need for centralized identity validation and instead implements localized assertions of trust at every node—aligning with the zero-trust security model, which mandates authentication at every point of interaction [9].

The iOS Secure Enclave is among the most suitable hardware platforms for implementing such applications, as it is capable of rapid biometric verification and hardware-based cryptographic operations. This system ensures low latency and minimizes network-related risks, since biometric authentication can be performed on-device without reliance on cloud services. Additionally, binding cryptographic keys to both the user and the device reduces the feasibility of credential theft, making it practically impossible to impersonate an authenticated user in a well-designed system [9].

11. Evaluating Limitations and Implementation Challenges

Despite their strong features, biometric-sealed keys cannot be operated within secure enclaves arbitrarily. To begin with, hardware dependency on secure enclaves—such as Apple's Secure Enclave—can hinder platform interoperability. Devices lacking compatible hardware cannot participate in the same authentication ecosystems, leading to multi-device fragmentation. Furthermore, there is no direct access to biometric templates or cryptographic keys within the enclave; however, side-channel attacks—though rare—can still be executed. These attacks may extract sensitive information through microarchitectural characteristics, particularly when physical access to the device is obtained [10] .

Another challenge is biometric fallback. Many systems allow users to revert to passcodes or PINs in the event of biometric authentication failure. While this is essential for accessibility and usability, it introduces a potential vulnerability that can be exploited by adversaries—particularly in cases involving stolen devices. Designing zero-trust systems that effectively balance security, usability, and accessibility remains a critical concern.

There are also legal and ethical implications associated with linking biometric data to cryptographic functions. Unlike passwords, biometrics are inherently recognizable and permanent, which raises important questions regarding user consent, data sovereignty, and the lawful acquisition of biometric information. Governments and regulatory bodies must define how these technologies should be audited, monitored, and controlled to prevent misuse or unwarranted surveillance. While enclaves can provide technical guarantees of privacy, these capabilities must be supported by governance frameworks that ensure real-world protection [1][2].

12. The Future of Zero-Trust On-Device Security

Biometric-sealed keys, when combined with secure hardware enclaves and the zero-trust model, represent a significant step toward post-identity security architectures. In modern systems, identity can no longer be treated as a static element; rather, it becomes a dynamic construct—verified behaviorally and continuously through biometric signatures, usage patterns, and contextual data. The device itself also evolves into a dynamic trust broker, not only confirming the user's presence but also evaluating the legitimacy of the user in real time.

It is likely that future architectures will incorporate distributed ledger technologies, post-quantum cryptographic algorithms, and machine learning–enabled authentication profiles to dynamically adapt to evolving threat landscapes. Multi-modal biometrics—comprising a combination of biometric features such as facial characteristics, voice, and gait—will also be integrated, further enhancing authentication processes. These systems will be organized within secure enclaves that gate access through cryptographic controls.

Another potential evolution of the Secure Enclave concept would be its transition to an open standard, enabling broader ecosystem interoperability with the same level of confidence that hardware-based isolation currently provides. This shift could help eliminate existing vendor lock-ins and stimulate platform innovation. Moreover, edge computing and federated learning could extend the capabilities of enclaves into collaborative, privacy-conscious systems—where learning occurs locally, and only abstract, non-sensitive models are distributed.

Biometric-sealed keys are not a standalone solution but rather a key component within a broader zero-trust security framework. Defensive strategies must evolve in tandem with the threats they are designed to counter. The future of cybersecurity will be more confidential and resilient, with identity and access control increasingly grounded in secure, hardware-backed, and biometric-gated systems.

13. Conclusion

A 2021 milestone in the advancement toward privacy-oriented, on-device security was the integration of biometric authentication, secure enclave technology, and zero-trust architecture. Biometrically sealed keys offer a compelling method for securing cryptographic processes by human-binding devices—ensuring that, even in a compromised environment, the keys remain protected by default and resistant to intrusion.

These systems ensure that cryptographic processes are executed within secure, isolated environments and that sensitive key material is protected against software-based attacks, leveraging the capabilities of the iOS Secure Enclave. Biometrics promote user-specific, non-transferable access and are inherently difficult to forge. Biometric-sealed keys enhance flexibility and trust across domains such as federated identity, blockchain, multi-hop authentication, and post-quantum security.

Nevertheless, device interoperability, legal regulation, and vulnerability to fallback mechanisms must be addressed as part of an integrated security framework. As technological and regulatory environments continue to mature, the next generation of secure digital systems will increasingly focus on biometric-sealed keys to enable robust deployment within a zero-trust landscape.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Rodríguez, B. F. (2025). Biometric Breakthroughs. Digitalization and Artificial Intelligence in Courts: Opportunities and Challenges, 104, 89.

[2] Prakasha, K. K., & Sumalatha, U. (2025). Privacy-preserving techniques in biometric systems: Approaches and challenges. IEEE Access.

[3] Hang, Y., & Yang, Z. (2025, August). NailKey: Mutable Biometric Using Fingernails. In Proceedings of the 20th ACM Asia Conference on Computer and Communications Security (pp. 1506-1519).

[4] Franco, C., Lancha, C., Flores, D., Arjona, R., & Baturone, I. (2025, August). A High-Level-of-Assurance EUDI Wallet with a Remote WSCD Supporting Biometrics and Passkeys. In International Conference on Availability, Reliability and Security (pp. 93-110). Cham: Springer Nature Switzerland.

[5] Sumalatha, U., Prakasha, K. K., Prabhu, S., & Nayak, V. C. (2025). Secure Knuckle Print Authentication: Template Protection and Attack Analysis. IEEE Access.

[6] Franco, C., Arjona, R., & Baturone, I. (2025, August). A cloud-based multifactor authentication scheme using post-quantum cryptography and trusted execution environments. In International Conference on Availability, Reliability and Security (pp. 217-234). Cham: Springer Nature Switzerland.

[7] Bhand, K., Khubchandani, P., & Khubchandani, J. (2025). A Fuzzy Logic-Based Cryptographic Framework For Real-Time Dynamic Key Generation For Enhanced Data Encryption. arXiv preprint arXiv:2511.14132.

[8] Ren, Z., Li, H., He, G., Yu, R., Tong, Y., Xu, S., & Deng, L. (2025). An SGX-based key protection scheme for Hyperledger Fabric: Z. Ren et al. Cluster Computing, 28(16), 1042.

[9] Lee, S. J., Lee, J. M., & Lee, I. G. (2025). Low latency and secure data encryption for multi-hop biometric authentication in distributed networks. Internet of Things, 30, 101501.

[10] Zinoviev, A. V. (2025). On the Discovery of a Fossil Seal Scapula in Ancient Panticapaeum (Crimean Peninsula). International Journal of Osteoarchaeology, e70002.