A BIOMETRIC-BASED AUTHENTICATION FOR SECURE PAYMENT SYSTEM: A COMPREHENSIVE REVIEW

Dr. G. RAJKUMAR
Head & Assistant Professor, Department of Computer Applications,
N.M.S.S.Vellaichamy Nadar College, Madurai, Tamilnadu, India.
mdugrk@gmail.com

ABSTRACT

In the modern financial technology landscape, securing digital payment channels against unauthorized access, credential exploitation, and advanced identity theft is a paramount challenge. Traditional knowledge-based authentication mechanisms—such as passwords, Personal Identification Numbers, and physical tokens—are increasingly insufficient due to vulnerabilities like social engineering, phishing, card skimming, and shoulder surfing. Biometric authentication has emerged as a robust, non-transferable alternative, binding financial transactions directly to user identity. This paper provides a comprehensive, state-of-the-art review of biometric-based authentication systems deployed within global digital payment infrastructures. We analyze physiological modalities alongside emerging behavioral dynamics. Furthermore, we examine contemporary structural paradigms, detailing local Secure Element matching versus cloud architectures, and investigate advanced template protection frameworks including Cancelable Biometrics, Biometric Cryptosystems, and industry interoperability standards. Finally, this review highlights critical security vulnerabilities, notably Presentation Attacks and Deepfake-driven synthetic identity injection, outlining future research trajectories for zero-trust, privacy-preserving financial ecosystems.

Keywords: *Biometric Authentication, Digital Payments, Financial Technology Security, Presentation Attack Detection, Cancelable Biometrics, Behavioral Dynamics.*

INTRODUCTION

The global transaction ecosystem is undergoing an epochal transformation, driven by cash-lite policy directives, mobile-first banking applications, and the

democratization of e-commerce channels. While the transition from physical legal tender to digitalized transaction rails offers unprecedented efficiency and consumer convenience, it has simultaneously exposed systemic fractures in traditional digital security frameworks. Financial fraud patterns have pivoted rapidly from localized, physical interactions to highly sophisticated, distributed cyber-attacks targeting the transaction authorization layer.

Historically, transaction security has relied on two foundational pillars:

1. **Knowledge Factors:** Passwords, security phrases, and static Personal Identification Numbers.
2. **Possession Factors:** Integrated circuit smart cards, hardware tokens, and one-time password generators.

Despite widespread adoption, these models suffer from a core defect where the credential can exist independently of the authorized user. A password can be cracked via brute-force or harvested through structured phishing campaigns; a physical token can be intercepted, cloned, or extracted via automated skimming devices. Biometric authentication solves this issue by basing authorization on inherency factors, which evaluate what a person is or what they do. By capturing unique physiological markers or behavioral cadences, biometric payment systems bind the act of financial clearing to the verified physical presence of the account holder.

However, moving biometric processing into high-volume, low-latency financial systems creates complex engineering, privacy, and security challenges. If a password is stolen, it can be immediately revoked and reset. If a user's raw fingerprint or facial geometric map is compromised during a commercial database breach, that specific trait is permanently exposed. This fundamental challenge has driven extensive research into privacy-preserving, non-invertible, and highly accurate biometric processing systems.

Objectives and Scope of this Review

While existing literature often covers biometrics as a general access control mechanism, this review focuses Java-level constraints, performance trade-offs, and attack vectors unique to financial transactional infrastructure. The scope of this paper encompasses:

- A comparative breakdown of dominant physiological and behavioral modalities optimized for retail point-of-sale and mobile e-commerce environments.
- An architectural analysis of local client-side authentication versus decentralized and cloud-based verification networks.
- A deep dive into template security methodologies, specifically cancelable mappings and zero-knowledge architectures designed to comply with global data regulations.
- A technical taxonomy of contemporary threat vectors, focusing on Presentation Attacks and the emerging threat of generative artificial intelligence deepfakes, alongside state-of-the-art mitigation strategies.

TAXONOMY OF BIOMETRIC MODALITIES IN PAYMENT SYSTEMS

Biometric modalities utilized in securing transaction systems are broadly categorized into physiological biometrics, which evaluate static, structural anatomical attributes, and behavioral biometrics, which isolate dynamic, learned patterns executed over time.

Physiological Modalities

Fingerprint Recognition

Fingerprint scanning remains the most mature and widely integrated modality within commercial banking environments. Modern systems deploy three primary sensor typologies: capacitive, optical, and ultrasonic. Fingerprint verification algorithms extract local discontinuities along the epidermal ridge paths, prioritizing minutiae configurations such as ridge endings and bifurcations.

Educational Research and Development Centre

- **Advantages:** High distinctiveness, low implementation footprint on smart cards, and rapid matching execution.
- **Limitations:** Vulnerable to superficial epidermal degradation from abrasions or aging effects, and susceptible to physical spoofing via high-resolution silicone cast templates.

Facial Recognition

Driven by the ubiquity of high-resolution front-facing mobile cameras, facial payment gateways have achieved mass commercial adoption. These systems transform raw image captures into localized landmark coordinates, generating a dense geometric

feature vector via deep convolutional neural networks. True three-dimensional systems combine optical sensors with infrared dot-projectors to calculate depth topology.

- **Advantages:** Contactless operational profile, high user convenience, and integration capability with standard smartphone hardware.
- **Limitations:** Performance drops under dramatic illumination variances, peripheral occlusions such as medical masks or eyewear, and vulnerability to digital presentation injections like deepfakes.

Iris Recognition

Iris authentication assesses the complex, chaotic patterns present within the iris stroma. Using near-infrared illumination, scanners map the unique structural details of the eye, converting the pattern into a highly deterministic binary representation.

- **Advantages:** Unparalleled stability across a user's lifespan, mathematical immunity to structural aging, and an extraordinarily low False Acceptance Rate.
- **Limitations:** Requires specialized imaging hardware, induces higher user discomfort due to strict alignment tolerances, and carries higher cost metrics for point-of-sale integration.

Palm Vein and Vascular Pattern Recognition

Vascular biometrics capture the subcutaneous deoxygenated hemoglobin absorption signatures within a user's palm or finger using near-infrared light paths. The hidden vascular matrix is extracted as a unique geometric coordinate network.

- **Advantages:** High immunity to structural forging or superficial surface damage; inherently verifies user liveness due to the absolute requirement of active blood flow.
- **Limitations:** Requires larger physical scanner dimensions, restricting its use to fixed commercial point-of-sale terminals rather than ultra-thin mobile form factors.

Behavioral Modalities

Touchscreen Dynamics and Keystroke Cadence

Deployed primarily within online banking portals and mobile banking apps, this passive authentication vector analyzes user interaction mechanics. Captured metrics

include the exact dwell time, which measures how long a finger rests on a virtual button, alongside flight time, touch surface area, and variable pressure profiles.

- **Advantages:** Operates transparently without explicit user intervention, providing continuous authentication throughout the entire active banking session.
- **Limitations:** Susceptible to variance caused by environmental conditions like entering a payment while walking versus sitting down, and exhibits a higher False Rejection Rate compared to static physiological checks.

Voice Biometrics

Voice authorization transforms auditory input into time-frequency spectrogram representations, parsing physiological traits such as vocal tract geometry alongside behavioral mannerisms like accent, speech velocity, and cadence. It is increasingly utilized to authorize smart-home internet-of-things transactions and remote telephone banking clearing.

- **Advantages:** Ideal for remote hands-free payment interfaces and automated drive-thru environments.
- **Limitations:** Highly vulnerable to ambient acoustic noise pollution and vulnerable to synthetic audio clones generated via advanced generative adversarial networks.

COMPARATIVE EVALUATION FRAMEWORK

To guide system architects in selecting appropriate biometric modalities for specific payment architectures, this section provides an analytical comparison based on standard performance criteria:

- **Fingerprint Systems:** Deliver high accuracy and low latency profiles at a low hardware cost. They feature high user acceptance and moderate resilience to spoofing, making them ideal for mobile wallets and biometric smart cards.
- **Facial Recognition:** Offers high accuracy and medium latency profiles using standard hardware. It features very high user acceptance but lower raw resilience

to spoofing unless paired with robust depth sensors, making it ideal for mobile applications and retail self-checkout.

- **Iris Scanning:** Provides extremely high accuracy at the cost of high latency and high hardware expenditures. User acceptance is moderate, but resilience to spoofing is exceptionally high, making it ideal for high-value corporate banking terminals.
- **Palm Vein Verification:** Delivers extremely high accuracy and low-to-medium latency profiles. Hardware costs are high, but user acceptance is high and resilience to spoofing is extreme, making it optimal for physical retail point-of-sale hubs.
- **Touch Dynamics:** Exhibits medium accuracy profiles but operates continuously with no additional hardware cost. User acceptance is high due to its passive nature, and resilience to spoofing is high, making it excellent for risk-based fraud detection.
- **Voice Verification:** Provides medium accuracy and medium latency profiles at a low cost. User acceptance is high, but resilience to spoofing is low due to replay vectors, making it suited primarily for internet-of-things smart home commerce.

ARCHITECTURAL PARADIGMS IN PAYMENT ECOSYSTEMS

The deployment of biometric payment infrastructure typically follows one of three structural distribution models: Centralized Cloud Verification, Local Match-on-Device, or Federated Decentralized Frameworks.

Centralized Cloud Architectures

In early implementations, raw or compressed biometric features were transmitted directly across communication channels to a centralized institutional database for matching. While this architecture allows for centralized management and reduces terminal hardware costs, it creates severe security vulnerabilities. Centralized biometric repositories represent a single point of failure and highly lucrative targets for malicious actors. A compromise of such a database permanently invalidates the identities of all enrolled users.

Local Match-on-Device

To mitigate database risks, modern financial frameworks favor a decentralized decentralization model, such as Match-on-Card or Match-on-Device. The user's biometric template is stored exclusively within a physically isolated microchip, such as a hardware Secure Element or a processor-level Trusted Execution Environment on a smartphone.

During a transaction, the sensor forwards data to the Secure Element, which processes the matching locally. If verified, the Secure Element releases a digital signature to authorize the transaction. The raw biometric data never leaves the physical perimeter of the device, eliminating server-side leakage vectors.

Industry Standardization Standards

The industry has standardized this local paradigm through contemporary authentication suites, which utilize standard web authentication specifications. Under this standard, the biometric check serves simply as a local user verification step to unlock a unique asymmetric cryptographic key pair. The transaction server issues a challenge token, the device signs it with the local private key unlocked by the biometric verification, and the server validates the signature using the pre-registered public key. This architecture successfully separates identity verification from transaction authorization, providing a robust blueprint for secure, modern mobile commerce.

ADVANCED BIOMETRIC TEMPLATE PROTECTION FRAMEWORKS

Because biometric traits cannot be modified or reissued if compromised, protecting stored templates is a critical research focus. Contemporary systems utilize cryptographic techniques to ensure templates remain non-invertible, discriminative, and cancelable.

Cancelable Biometrics

Cancelable biometrics apply a repeatable, non-invertible mathematical transformation to the biometric feature vector during the registration phase. The matching process is performed entirely within the transformed domain. If a cancelable template database is breached, the compromised record is revoked. A new template is

generated simply by applying a different transformation function or modifying the user-specific seed key.

Common transformation techniques include random projections, where the raw vector is mapped into a lower-dimensional subspace via an orthogonal matrix, and functional distortions, which shift feature coordinates based on complex non-linear polynomials. The engineering challenge lies in designing transformation functions that preserve the spatial topology of the features without introducing performance degradation or elevating the False Rejection Rate.

Biometric Cryptosystems

Biometric cryptosystems bind a standard cryptographic key directly to the biometric template or generate the key natively from the biometric features. These systems are broadly split into helper-data methods like Fuzzy Commitment and Fuzzy Vault schemes. In a Fuzzy Vault design, a secret cryptographic key is encoded as the coefficients of a unique polynomial. The legitimate user's features are placed as valid coordinates on this polynomial curve. The vault is then filled with a large volume of random decoy coordinates that do not sit on the polynomial path.

During transaction authorization, the user provides a fresh biometric scan. If the feature points match closely enough to filter out the decoy points, the system reconstructs the polynomial via error-correcting codes, successfully unlocking the underlying payment authorization key.

SECURITY VULNERABILITIES AND COUNTERMEASURES

As biometric payment systems scale, attackers increasingly target the boundaries between the physical sensors, local processing chips, and network layers.

Presentation Attacks

Presentation attacks involve presenting a synthetic or counterfeit artifact to the physical biometric capture sensor to deceive the system. In fingerprint applications, this includes the production of artificial overlays constructed from materials like silicone, gelatin, or wood glue. For facial recognition frameworks, presentation attacks range from basic printed photographs to sophisticated sculpted lifelike masks.

Countermeasures: Presentation Attack Detection

Modern systems implement standardized presentation attack detection frameworks, combining hardware and software-based liveness detection:

- **Hardware-Based Mitigation:** Sensors capture auxiliary physiological markers, such as pulse oximetry, localized skin temperature, blood flow velocities via laser Doppler imaging, or multispectral light absorption signatures.
- **Software-Based Mitigation:** Machine learning models analyze texture micro-structures, surface illumination reflectance, and involuntary physiological micro-movements, such as blinking patterns or minute pupillary dilations.

Deepfakes and Digital Injection Vectors

The rapid evolution of generative adversarial networks and real-time diffusion models has created a critical threat vector known as digital injection deepfake attacks. Rather than spoofing a physical sensor, attackers intercept the device's internal camera data stream and inject high-fidelity, synthetically animated video loops that match the account holder's identity. This bypasses traditional software liveness checks by presenting realistic ocular and facial movements.

Countermeasures

Defending against digital injection requires strict hardware-software co-design. Hardware abstraction layers within mobile operating systems must enforce cryptographic signing of sensor data streams directly inside the protected camera processor module. This ensures that the downstream authentication engine only accepts video payloads that match a verified, tamper-proof hardware certificate signature.

SOCIO-TECHNICAL AND REGULATORY CHALLENGES

Deploying biometric authentication within global payment systems requires navigating a complex web of user experience constraints and strict regulatory mandates.

Algorithmic Bias and Demographic Inequity

Extensive empirical testing has revealed systemic demographic bias across many mainstream facial and fingerprint recognition algorithms. Systems often display highly

disparate False Rejection Rates when processing diverse ethnic groups, varying age brackets, or different genders.

In a commercial payment environment, a high False Rejection Rate translates directly to rejected transactions and consumer friction at point-of-sale terminals. Resolving these performance disparities requires using deeply diversified training datasets and refining algorithmic loss functions to prioritize demographic equity.

Global Privacy Regulations

Financial institutions face strict legal constraints regarding how biometric identities are captured, processed, and maintained. International regulations classify biometric identifiers as sensitive category data, explicitly prohibiting processing unless the explicit, unambiguous consent of the data subject is obtained. Under typical data deletion mandates, institutions must maintain architectures capable of completely purging all biometric references upon user request.

These strict regulatory frameworks highlight the necessity of transitioning away from raw template storage toward decentralized, cancelable, and local tokenization paradigms.

CONCLUSION

Biometric-based authentication represents a major step forward in securing digital payment systems. By replacing easily exploitable knowledge and possession-based credentials with inherent identity features, biometrics significantly reduce card-not-present fraud, simplify checkout latencies, and eliminate reliance on static passwords. As detailed in this review, the industry's transition toward local match-on-device execution, standardized cryptographic trust architectures, and cancelable biometric algorithms effectively addresses the core privacy concerns that impacted early centralized implementations.

REFERENCES

[1] Jain, A. K., Deb, D., & Engelsma, J. J. Biometrics: Trust, Privacy, and Security Challenges. *ACM Computing Surveys*.

[2] Ratha, N. K., Connell, J. H., & Bolle, R. M. Enhancing Security and Privacy in Biometric-Based Authentication Systems. *IBM Systems Journal*.

[3] Yang, W., Wang, S., Hu, J., Ibrahim, A., & Valli, C. A Security and Privacy Analysis of Cancelable Biometrics. *IEEE Access*.

[4]G. Rajkumar, "Linear cryptanalysis of substitution ciphers using particle swarm optimization," Oriental Journal of Computer Science and Technology, vol. 10, no. 3, pp. 580–584, 2017.

[5] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. *Handbook of Fingerprint Recognition*. Springer Science & Business Media.

[6] A.Ruba, G.Rajkumar, and K.Parimala, "Biometrics based Cryptographic Key Generation using Finger Print," Int. J. Comput. Eng. Res. Trends, vol. 4, no. 6, pp. 259 262, Jun. 2017.

[7] Meng, Y., Wong, D. S., Schlegel, R., & Kwok, L. F. Touchscreen Motion Biometrics for Mobile User Authentication: A Review. *IEEE Transactions on Communications*.

[8] ISO/IEC Standards. *Information Technology — Biometric Presentation Attack Detection — Part 1: Framework*. International Standard Organization.

[9] Dr. G. Rajkumar, Dr. K. Parimala and A. Ruba "An Innovative approach to Genetic Algorithm based Cryptography." International Journal of Computer Science" 2017; 5(1):1199 – 1202.

[10] Sundararajan, K., & Woodard, D. L. Deep Learning for Biometrics: A Review. *ACM Computing Surveys*.

[11] Anusha , A. K. R. S., Rajkumar, G. (2017). Privacy and Security Issues in Aadhaar, IJRASET, 5(8).

[12] Patel, V. M., Ratha, N. K., & Chellappa, R. Computational Methods for Biometric Template Protection. *IEEE Signal Processing Magazine*.