Legal Frameworks for Biometric Authentication in Financial Transactions

Abhijit Jorvekar[1], Dr. Shirish Dattatraya Kulkarni[2], Vikas Haribhau Satonkar[3], Rishikesh Balkrishna Pansare[4], Ganesh Shelke[5], Dr. Lalita Kiran Wani[6]

[1]MBA Department, Sandip University Nashik, Nashik, Maharashtra, India. abhijit.jorvekar@sandipuniversity.edu.in

[2]Symbiosis Law School (SLS) Symbiosis International (Deemed University) (SIU) Vimannagar, Pune, Maharashtra, India. sdkulkarni@symlaw.ac.in

[3]Assistant Professor, Department of Computer Engineering, Sandip Institute of Engineering & Management, Nashik, Maharashtra, India. vikas.satonkar@siem.org.in

[4]Assistant Professor, Department of Information Technology, Sandip Institute of Technology & Reserch Centre, Nashik, Maharashtra, India. rishikesh.pansare@sitrc.org

[5]Vishwakarma Institute of Technology, Pune, Maharashtra, India. ganesh.shelke@viit.ac.in

[6]Bharati Vidyapeeth's College of Engineering, Lavale, Pune, Maharashtra, India. Email: lalita.wani@gmail.com

Abstract: Biometric authentication has become an integral part of financial transactions due to its enhanced security features and ease of use. However, the increasing reliance on biometric data raises significant legal and privacy concerns. This paper explores the current legal frameworks governing biometric authentication in financial transactions, focusing on international regulations such as GDPR and BIPA, as well as country-specific laws. The analysis highlights inconsistencies in global regulatory approaches, challenges in data privacy, storage, and cross-border transfers. Case studies from the U.S., EU, and India are used to examine the real-world implications of these laws. Emerging threats, including deepfakes and synthetic identities, expose the gaps in current regulations. The paper concludes by offering recommendations for harmonizing global standards, enhancing data privacy protections, and strengthening enforcement mechanisms to address these risks.

Keywords: Biometric authentication, financial transactions, data privacy, legal frameworks, GDPR, BIPA.

Introduction

Biometric authentication refers to the process of verifying an individual's identity using unique biological traits such as fingerprints, facial recognition, iris patterns, or voice recognition. Unlike traditional authentication methods such as passwords or PINs, biometric systems rely on physiological or behavioral characteristics that are difficult to replicate or steal. This makes biometrics an increasingly favored security solution in financial transactions, where safeguarding sensitive personal data and ensuring secure access to accounts are critical[1], [2].

In the realm of financial technology (fintech), biometrics have evolved from simple fingerprint recognition to more advanced multimodal systems that integrate several biometric markers. Banks and financial institutions are adopting these technologies to streamline user verification processes, enhance transaction security, and reduce fraud. For example, biometric-enabled ATMs, mobile banking apps using facial recognition, and voice-based authentication are transforming how financial services are accessed[3], [4].

As the use of biometric authentication expands in fintech, so too does the need for robust legal frameworks. The increasing reliance on these systems introduces several risks, including potential data breaches, misuse of personal information, and the violation of individual privacy rights. Given that biometric data is inherently sensitive and irreplaceable, there is a heightened urgency to implement regulatory oversight to safeguard users.

Without clear legal guidelines, financial institutions may face challenges related to data collection, storage, and sharing, as well as issues of consent and user rights. Furthermore, as biometric authentication becomes more common, it is essential to ensure that legal frameworks are updated to address emerging risks such as deepfakes and identity theft[5].

This paper aims to analyze the existing legal frameworks governing biometric authentication in financial transactions. It will identify gaps within these regulations and propose recommendations for strengthening global standards, enhancing data privacy protections, and ensuring more effective enforcement.

Biometric Authentication in Financial Transactions: A Technological Overview

Biometric authentication in financial transactions leverages the uniqueness of biological traits to ensure secure access and identity verification. As financial institutions seek more reliable security solutions, biometrics provide an advanced layer of protection beyond traditional passwords or PINs. Below is an overview of the main types of biometric systems and their implications[6].

Types of Biometric Systems

- Fingerprint Recognition: One of the most widely used biometric systems, fingerprint recognition scans the unique ridges and patterns of a user's fingerprint to verify identity. Commonly deployed in mobile banking apps and biometric-enabled ATMs, fingerprint recognition offers a fast and reliable method of authentication.
- Facial Recognition: Facial recognition uses algorithms to map facial features, creating a unique digital profile for each individual. In financial transactions, it allows users to access accounts or authorize payments simply by scanning their face, providing a seamless and contactless experience.
- Voice Authentication: Voice recognition systems analyze vocal patterns, pitch, and tone to verify identity. This method is increasingly being used in call centers and mobile banking applications, allowing for secure transactions without requiring physical input.
- Iris and Retina Scanning: These systems focus on capturing the unique patterns in the iris or retina. Iris and retina scanning are highly secure and accurate, though less common due to their complexity and higher implementation costs.

Advantages and Risks

Biometric authentication offers significant security benefits in financial transactions. Since biometric traits are unique to each individual and difficult to replicate, these systems reduce the risk of fraud and unauthorized access. Additionally, biometrics provide a more convenient user experience, eliminating the need to remember passwords or carry physical tokens[7], [8].

However, privacy concerns and potential misuse of biometric data present notable risks. If biometric information is compromised, it cannot be reset like a password, leading to irreversible security breaches. Furthermore, improper handling of biometric data by financial institutions raises concerns about user consent, data storage, and possible identity theft. Thus, implementing strict privacy laws and regulations becomes crucial to mitigate these risks.

Data Privacy and Security Laws Related to Biometrics in Finance

Biometric data plays a critical role in financial transactions, requiring careful regulation to ensure user privacy and security. Different jurisdictions have established laws that address the collection, storage, and transfer of biometric data, each with its unique set of rules[1], [9].

Importance of Explicit Consent in Collecting Biometric Data

The collection of biometric data is highly sensitive and requires explicit consent from users. This is essential to ensure individuals are aware of how their data is being used, stored, and shared. Financial institutions must obtain clear and unambiguous consent before collecting biometric information, which helps prevent unauthorized access and data misuse.

Key Differences in Regional Laws Regarding Consent

- United States (BIPA): Requires written consent before collecting or storing biometric data. Individuals must be informed about the purpose of the data collection and how it will be used.
- European Union (GDPR): Biometric data is classified as a special category of personal data, requiring explicit consent from individuals, except under specific circumstances where data processing is necessary (e.g., for legal or vital interests).
- India (Aadhaar Act): Biometric data collection is mandatory for Aadhaar enrolment, but individuals must give consent for its use in authentication processes.

These variations reflect differing attitudes toward user control and privacy across regions, requiring global companies to navigate a complex regulatory landscape.

Legal Stipulations for Secure Storage of Biometric Data

Countries impose strict guidelines for the secure storage of biometric data. Financial institutions must implement strong encryption protocols, restrict access to authorized personnel, and conduct regular security audits. Biometric data must be protected against unauthorized access, breaches, and theft[10], [11].

Retention Period Regulations in Different Jurisdictions

- BIPA (USA): Companies must destroy biometric data when it is no longer needed or within three years of the individual’s last interaction with the company.
- GDPR (EU): Personal data, including biometric data, must not be retained for longer than necessary for the purpose it was collected. Institutions are required to define a clear retention period and ensure data is erased once that period expires.
- Aadhaar Act (India): Biometric data should be stored securely, but regulations around specific retention periods are less defined.

International Regulations on Cross-Border Data Transfers

Cross-border data transfers involving biometric information introduce significant legal complexities. Countries often impose restrictions to prevent data from being transferred to jurisdictions that do not offer adequate privacy protections.

- GDPR: Only permits data transfers to countries with adequate data protection standards. Transfers to non-compliant regions require additional safeguards, such as binding corporate rules or standard contractual clauses.
- BIPA: Does not explicitly regulate cross-border transfers but imposes obligations to ensure biometric data is handled responsibly, regardless of location.
- India: Aadhaar data cannot be stored outside the country, reflecting strict localization requirements.

Data Localization Laws and Their Impact on Financial Transactions

Several countries have introduced data localization laws, which require that biometric data be stored within national borders. This presents challenges for multinational financial institutions that rely on global data-sharing networks[12], [13].

- India’s Aadhaar mandates strict data localization, making it difficult for global companies to integrate Aadhaar authentication across borders.
- Russia’s Data Localization Law mandates that all personal data, including biometrics, be stored on servers located within Russia.

These regulations aim to protect biometric data but can create friction in international financial transactions, complicating cross-border collaborations and data exchanges.

Challenges and Gaps in the Current Legal Frameworks

The current legal frameworks governing biometric authentication face several challenges and gaps that hinder their effectiveness in a rapidly evolving technological landscape are shown in table-1[14], [15].

Table 1 Challenges and Gaps In The Current Legal Frameworks

Category	Description	Impact
Inconsistencies in Global Regulations	Lack of harmonization between different legal systems affecting global operations.	Creates challenges for financial institutions in cross-border transactions.
Emerging Threats and Legal Limitations	Deepfake technology and synthetic identities expose gaps in current laws.	Opens opportunities for identity fraud and other security risks.
Enforcement Issues	Difficulty in enforcing regulations and addressing legal consequences for non-compliance.	Leads to inconsistent protection and limited accountability for data breaches.

Addressing these challenges requires a more harmonized approach to regulation, updated legal frameworks to account for emerging threats, and stronger enforcement mechanisms to ensure compliance and protect biometric data globally.

Recommendations for Strengthening Legal Frameworks

As biometric authentication becomes more prevalent in financial transactions, the need for stronger and more coherent legal frameworks is increasingly urgent. Current regulations, though essential, face challenges due to varying global standards, emerging threats such as deepfakes, and inconsistent enforcement. To ensure the effective protection of biometric data, a unified and proactive approach is needed. Table-2 outlines key recommendations for strengthening existing legal frameworks, focusing on global harmonization, enhanced data privacy, addressing new security risks, and bolstering enforcement mechanisms.

Table 2 Suggested Recommendations for Strengthening Legal Frameworks

Recommendation	Description	Expected Outcome
Harmonization of Global Standards	There is a need for uniformity in biometric regulations across countries to facilitate seamless international transactions and compliance.	Simplifies cross-border financial operations and ensures consistent protection of biometric data worldwide.
Enhancing Data Privacy and Security	Stricter guidelines for data storage, explicit consent, and secure transfer processes should be implemented globally.	Ensures stronger protection of sensitive biometric information, reducing the risk of data breaches and misuse.
Addressing Emerging Risks	Legal mechanisms must be developed to tackle emerging threats, such as deepfakes and synthetic identities, which pose new challenges to security.	Helps mitigate identity fraud and strengthens overall trust in biometric authentication systems.
Stronger Enforcement Mechanisms	Frameworks for better enforcement, including clear penalties for non-compliance and improved oversight, need to be established.	Enhances accountability and ensures stricter adherence to legal regulations concerning biometric data.

Strengthening the legal frameworks for biometric authentication is critical for maintaining security, privacy, and trust in financial systems. By harmonizing global standards, enhancing data privacy protections, addressing emerging threats, and improving enforcement mechanisms, regulatory bodies can better safeguard biometric data and mitigate risks. These recommendations offer a pathway toward a more robust legal structure that not only protects users but also facilitates innovation and secure cross-border financial transactions.

Conclusion and Future scope

Presented work identified several critical legal challenges and gaps in the current frameworks governing biometric authentication in financial transactions. Key issues include the lack of global harmonization, inadequate provisions to address emerging threats like deepfakes, and challenges with enforcing existing regulations. These gaps leave biometric data vulnerable to misuse, making it essential to update and strengthen legal structures.

Biometric authentication technology is expected to evolve with advancements such as more secure multimodal biometric systems, AI-driven identity verification, and more seamless integration with financial platforms. As these technologies advance, new legal concerns will arise, particularly regarding data privacy, security, and cross-border data flow. Legal frameworks will need to adapt to these advancements to ensure continued protection of user data.

Robust legal frameworks are indispensable for securing the future of biometric-based financial systems. By addressing current gaps and preparing for future technological shifts, these frameworks can ensure that biometric authentication remains a secure, trusted, and compliant solution in global finance. Ultimately, effective regulation will balance innovation with the necessary safeguards to protect individual privacy and data security in an increasingly digital world.

References

[1] H. U. Khan, M. Sohail, S. Nazir, T. Hussain, B. Shah, and F. Ali, “Role of authentication factors in Fin-tech mobile transaction security,” *J. Big Data*, vol. 10, no. 1, p. 138, 2023, doi: 10.1186/s40537-023-00807-3.

[2] C. A. Toli and B. Preneel, “Privacy-preserving biometric authentication model for E-finance applications,” *ICISSP 2018 - Proc. 4th Int. Conf. Inf. Syst. Secur. Priv.*, vol. 2018-January, no. Icissp, pp. 353–360, 2018, doi: 10.5220/0006611303530360.

[3] A. Bodepudi and M. Reddy, “Cloud-Based Biometric Authentication Techniques for Secure Financial Transactions: A Review,” *Int. J. Inf. Cybersecurity*, pp. 1–18, 2022.

[4] M. Marani, M. Soltani, M. Bahadori, M. Soleimani, and A. Moshayedi, “The Role of Biometric in Banking: A Review,” *EAI Endorsed Trans. AI Robot.*, vol. 2, pp. 1–15, 2023, doi: 10.4108/airo.3676.

[5] A. K. Al Hwaitat *et al.*, “A New Blockchain-Based Authentication Framework for Secure IoT Networks,” *Electronics*, vol. 12, no. 17. 2023, doi: 10.3390/electronics12173618.

[6] P. Datta, S. Bhardwaj, S. N. Panda, S. Tanwar, and S. Badotra, “Survey of Security and Privacy Issues on Biometric System BT - Handbook of Computer Networks and Cyber Security: Principles and Paradigms,” B. B. Gupta, G. M. Perez, D. P. Agrawal, and D. Gupta, Eds. Cham: Springer International Publishing, 2020, pp. 763–776.

[7] A. Malik, S. Gehlot, and S. Vyas, “Proposed Framework for Implementation of Biometrics in Banking KYC BT - Proceedings of Fourth International Conference on Computing, Communications, and Cyber-Security,” 2023, pp. 193–202.

[8] E. J. Kindt, “A Legal Perspective on the Relevance of Biometric Presentation Attack Detection (PAD) for Payment Services Under PSDII and the GDPR BT - Handbook of Biometric Anti-Spoofing: Presentation Attack Detection,” S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, Eds. Cham: Springer International Publishing, 2019, pp. 481–501.

[9] C.-H. Tsai and P.-C. Su, “The application of multi-server authentication scheme in internet banking transaction environments,” *Inf. Syst. E-bus. Manag.*, vol. 19, no. 1, pp. 77–105, 2021, doi: 10.1007/s10257-020-00481-5.

[10] H. U. Khan, M. Z. Malik, S. Nazir, and F. Khan, “Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis,” *IEEE Access*, vol. 11, pp. 80181–80198, 2023, doi:

10.1109/ACCESS.2023.3298824.

[11] A. Y. A. B. Ahmad, “Fraud Prevention in Insurance: Biometric Identity Verification and AI-Based Risk Assessment,” in *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, 2024, vol. 1, pp. 1–6, doi: 10.1109/ICKECS61492.2024.10616613.

[12] A. K. Ganguly, S. Bhattacharya, and S. Chattopadhyay, “A Design of Efficient Biometric based Banking System Through AI-Powered Transaction Security Fintech System for Secure Transactions,” in *2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2024, pp. 492–496, doi: 10.1109/ICACITE60783.2024.10617391.

[13] A. Modibbo and Y. Aliyu, “Cashless Society, Financial Inclusion and Information Security in Nigeria: The Case for Adoption of Multifactor Biometric Authentication,” *Int. J. Innov. Sci. Res. Technol.*, vol. 4, no. 11, pp. 872–880, 2019, [Online]. Available: www.ijisrt.com.

[14] O. Ogbanufe and D. J. Kim, “Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment,” *Decis. Support Syst.*, vol. 106, pp. 1–14, 2018, doi: https://doi.org/10.1016/j.dss.2017.11.003.

[15] S. Baichoo, M. Heenaye-Mamode Khan, P. Bissessur, N. Pavaday, N. Boodoo-Jahangeer, and N. R. Purmah, “Legal and ethical considerations of biometric identity card: Case for Mauritius,” *Comput. Law Secur. Rev.*, vol. 34, no. 6, pp. 1333–1341, 2018, doi: https://doi.org/10.1016/j.clsr.2018.08.010.