ज्ञानविविधा

कला, मानविकी और सामाजिक विज्ञान विषयों की अंतर्राष्ट्रीय सहकर्मी समीक्षित, मूल्यांकित, त्रैमासिक शोध-पत्रिका

ISSN : 3048-4537(Online)
3049-2327(Print)
Impact Factor-8.002 (SJIF)
Vol.-3; Issue-4 (Oct.-Dec.) 2026
Page No.- 06-14
©2026 Gyanvividha
https://journal.gyanvividha.com

Author's :
DISHA KAUSHIK

Corresponding Author :
DISHA KAUSHIK

The biometric security paradox : balancing false rejections, fraud prevention, and financial inclusion in emerging cashless economies

1. Abstract : As emerging economies shift from cash to digital, biometrics are used to both empower financial inclusion and facilitate Know Your Customer protocols. In this context, the Biometric Security Paradox emerges as a key structural tension, wherein the effort to increase security thresholds to stop fraud causes exclusion of vulnerable populations who cannot pass biometric tests. This paper employs a qualitative multi-methodological approach to examine the phenomenon of the Biometric Security Paradox and its consequences for the digital finance ecosystem. Drawing upon 60 semi-structured in-depth interviews, 8 focus group discussions (comprising 8 additional participants), and field observation in cash-in/cash-out agents in the Haridwar district of Uttarakhand, India, the paper explores the perspectives of the four key stakeholders involved in financial inclusion in India's digital economy. These include: vulnerable consumers (n = 30), banking correspondents (n = 15), fintech software designers (n = 10), and financial regulators (n = 5). Using Gioia's iterative process for qualitative data analysis, the paradox is dissected in terms of its manifestations and mechanisms. False Rejection Rates (FRR) in the context of emerging markets are produced by occupational ridge abrasion among working-age adults and biometric degradation among the elderly. At the point of sale, such FRR instances result in frustration, psychological distress and – in extreme cases – loss of livelihood. In their effort to balance the needs of the system and the customers' ability to perform, informal sector employees act as street-level bureaucrats. By highlighting the human cost of algorithmic security checks, this paper makes the case for designing more humane digital financial services. A standardized set of fallback authentication measures (soft tokens, OTPs,

etc.) is proposed, alongside more ethical considerations in the design of financial technology.

Keywords : Biometric Security Paradox, Financial Inclusion, Biometric Verification, biometric authentication, False Rejection Rate, Cash-in/Cash-out Agents, Know Your Customer (KYC), Ridge Abrasion, Digital Financial Services, Qualitative Research, Socio-Technical Frictions

2. Introduction : The shift from cash-intensive to digital financial systems in emerging economies constitutes both a huge opportunity for financial inclusion and a major headache for know-your-customer protocols. At the center of strategies to achieve both is the rise of large-scale biometric identification systems, such as India's Aadhaar, Nigeria's Bank Verification Number and Kenya's Huduma Namba. While aiming to increase access to services for the officially unbanked and undocumented, such systems create a dilemma for regulators and providers about their very nature. First identified in the context of fingerprint banking machines, the Biometric Security Paradox refers to the situation where efforts to make identification more secure, fraudulent proof and therefore automated, lead to the exclusion of precisely those vulnerable to being wrongly rejected by the system. Now largely overlooked in the technical literature, which focuses on the accuracy of minutiae recognition, matching algorithms and the statistical assessment of False Rejection Rates, the issue has real-life consequences for billions of informal workers and customers. This paper seeks to contribute an ethnographic perspective on the challenges posed by the BSR by examining the often indirect ways in which cash-in/cash-out agents, vulnerable customers, fintech developers and regulators negotiate the constraints of the system. The paper uses the example of the Indian state of Uttarakhand, focusing on the Haridwar district, a region with a preponderance of daily wage farm and factory workers, as well as pensioners, to discuss the costs of pursuing a policy of absolute security. In particular, it aims to demonstrate how informal agents use their positions to offset some of the pressures caused by the strict requirements of the system.

3. Review of Related Literature : The literature on the topic of biometrics as it relates to digital finance draws from a range of thematics including socio-technical systems, development economics, and human-computer interaction.

Pillar 1: Biometric Drift, Biological Aging, and Physiological Degradation : A foundational challenge in biometric verification systems is the tendency for physiological traits to degrade over time, a phenomenon often termed biometric drift. Biometric characteristics enrolled at a point-in-time can often become unrecognizable, particularly as a result of occupational, medical, and biologically driven forces. Occupational/Medical Friction: Biometric recognition is significantly impeded by the presence of physical ridge abrasion and physiological irregularities driven by occupational or medical forces (Rodriguez & Thompson, 2022). These factors affect the fidelity of hardware scans at the point of verification, particularly in occupational settings. Age-related Degradation: Biological aging presents a major challenge to the reliability of commercial recognition systems, as friction ridge and facial features degrade over time, contributing to system instability and temporal drift in matching algorithms (Johnson, 2023; Garcia et al., 2023). Biometric Drift: Das (2023) discusses the multi-factorial nature of physiological drift, arguing that adaptive multi-factor authentication protocols are best placed to address the limitations of single-factor recognition systems, which typically lack mechanisms to update enrolled templates over time (Martinez, 2023).

Pillar 2: System Architecture, Algorithmic Trade-offs, and Liveness Security : Computer science literature and pattern recognition research discuss mathematical and algorithmic aspects of biometric recognition systems, including trade-offs between performance metrics and approaches to enhance liveness security. Foundational Biometric Principles: Canonical textbooks

in computer science discuss fundamental trade-offs in Automatic Fingerprint Identification Systems (AFIS), including the balancing act between False Acceptance Rates (FAR) and False Rejection Rates (FRR) (Jain et al., 2022; Malton et al., 2020). Algorithmic Adaptability and Deep Learning: More recent research focuses on adapting fingerprint minutiae-based pattern recognition algorithms to incorporate deep learning architectures such as Siamese Networks, Swin Transformers, and Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM) to improve performance (Bhattacharya et al., 2023; Li et al., 2022; Nguyen et al., 2026; Smith, 2022). Computer vision research also emphasizes adaptive biometric systems capable of operating in noisy environments that require re- enrolment (Anderson & Smith, 2023; Kim & Lee, 2023; Singh et al., 2023; Xu et al., 2023). Anti-spoofing and Liveness: Contemporary security literature prioritizes spoofing resistance, emphasizing liveness detection algorithms and secondary behavioural biometric traits to improve spoof detection at points of verification and service (Patel, 2023; Sato, 2023).

Pillar 3: Privacy, Cryptography, and Data Protection Infrastructure : Biometrics research and computer science literature also focus on cryptographic aspects of information security and data protection, including emerging approaches to ensure biometric data privacy. Homomorphic Encryption and Privacy: A significant body of research focuses on protecting biometric information using homomorphic encryption and privacy-preserving technologies that enable secure authentication without relying on raw biometric templates (Hassan & Kumar, 2022; Zhang & Liu, 2023). Contemporary practices also emphasize the use of secure storage media such as AES-256 encrypted Automated Teller Machine (ATM) and Internet of Things (IoT) devices to protect biometric data payloads (Ovivo et al., 2026; Wilson, 2023; Yang, 2022). Federated Architectures and Cross-platform Security: Research also explores the use of federated approaches to biometric algorithm training that minimize exposure of sensitive data to centralized storage platforms, improving data security and cross-platform compatibility (Thompson, 2023; Wang & Zhang, 2022).

Pillar 4: The Biometric Paradox, Socio-technical Frictions, and Human Intermediaries : Beyond technical aspects of design and implementation, social science research addresses sociotechnical aspects of biometric authentication systems in general and finger scanning in particular. The Biometric Paradox: Emerging social science literature highlights the unintended consequences of biometric authentication systems, particularly the ways in which they can exacerbate social exclusion, especially under conditions of biometric degradation (Merlin et al., 2025). Street-Level Agency and Human Mediation: An extensive body of social science research, particularly from the field of public administration, discusses the role of street-level bureaucrats in mediating the interactions between impersonal technology and the public (Lipsky, 2010). System Application in Broader Contexts: Practical application of biometric systems in a variety of contexts informs the need for human mediation in fingerprint-based recognition systems, including the importance of designing interfaces around physical characteristics and access to public spaces (Chen & Wang, 2022; Spiceworks, 2022; Zhou, 2023).

4. Research Questions : This study was guided by the following research questions:

RQ1: What are the lived experiences of populations that are unable to meet the requirements of biometric verification at digital financial service points?

RQ2: How do cash-in/cash-out agents navigate the tension between consumer needs and security objectives?

RQ3: What are the factors that contribute to biometric rejections in a cashless economy?

RQ4: What qualitative criteria should be used in recommending alternative verification methods

to protect consumer dignity?

5. Research Objectives : A qualitative study aims to explore the problem of the Biometric Security Paradox through the lens of consumers, agents, designers, and regulators. I intend to achieve the following specific objectives:

1. Understand the downstream impact of the inability to meet biometric verification requirements.
2. Explore tensions in consumer-agent interactions around the theme of security vs. convenience.
3. Determine the perspectives of policymakers and fintech designers on the technical and regulatory aspects.

6. Research Methodology : Fieldwork was conducted in the Haridwar district of Uttarakhand state, India. The choice of this region was dictated by the presence of a considerable number of daily-wage agricultural workers ("Laksar/Khanpur blocks"), industrial daily labourers (SIDCUL Estate), and rural social pensioners ("Bank Mitra PoS touchpoints"). This qualitative inquiry adopts a multiple strategy, including phenomenological inquiry (explored the lived experience of digital finance consumers) and grounded theory (sequential, iterative coding of field notes and interview transcripts). Specifically, this research comprises the following qualitative methods:

Qualitative research methodology : Participant Selection and Data Collection Procedures:

The study adopted a mixed sampling strategy including purposive and maximum variation sampling to recruit 60 participants for this study. These included 52 respondents who participated in semi-structured in-depth interviews. Group A: vulnerable consumers (n=22), Group B: banking agents (n=15), Group C: fintech developers (n=10), and regulatory bodies (n=5). In addition, 8 vulnerable financial consumers were recruited to participate in 8 Focus group discussions (FGDs). The participants are breakdown in group are in following manner:

Group A: Vulnerable financial consumers (n = 30):

Manual agricultural labourers, construction workers, pensioners (>52 years), and informal micro-traders who predominantly use biometric-enabled point-of- sale (PoS) systems.

Group B: Front-line banking agents/operators (n = 15): Rural microfinance correspondents and mobile money agents who provide financial services to Group A.

Group C: Fintech developers (n = 10): Software engineers and managers who design the biometric verification systems used by Groups A and B.

Group D: Financial regulators (n = 5): Compliance officers and policymakers who regulate the operations of Groups A, B, and C.

- **Reasons for the unequal sample size:**

Group A (n = 30): Vulnerable consumers need the biggest sample size among the others because of the high variety of respondents. The group should be large enough to theoretically saturate the pool of people with different characteristics, such as manual workers, farmers, elderly people, pensioners, construction workers, and small business people.

Group B (n = 15): Banking agents were to ensure that the main operational issues and problems with approving transactions would be considered. The group will help identify the problems in all other agents' groups.

Group C (n = 10): Software engineers and product managers will explain the technical side of why FAR is more critical than FRR.

Group D (n = 5): Regulators will have a small sample size because there was theoretical saturation when discussing the policies on the same topic. The group is relatively small and has a homogeneous character.

An uneven sample coverage was intentionally selected for the study, considering the

relative theoretical saturation rates and the degree of heterogeneity of the specific actor groupings. For instance, the consumer group (n = 30) was covered with a more substantial sample because of the diversity of occupations among manual workers, retirees, and micro-traders. By contrast, a smaller group of fintech developers (n = 10) and regulators (n = 5) was sufficient for achieving informational saturation due to the homogeneity of their activities and the standardized nature of their regulatory environments.

7. Data Collection Procedures : The following data collection procedures were used to generate qualitative insights:

1. Semi-Structured In-Depth Interviews : I conducted 52 semi-structured in-depth interviews with members of Groups A ($n = 22$), B ($n = 15$), C ($n = 10$), and D ($n = 5$) using a protocol of my design. Each interview focused on eliciting the participant's lived experiences, perspectives, and expectations.

2. Focus Group Discussions : I conducted 8 Focus Group Discussions (FGDs) with 8 participants from Group A (1 participant per single-session/micro FGD format) to allow them to share their insights on the research questions. Each FGD was conducted in a semi-structured manner.

3. Field Ethnography & Direct Observation : I conducted field observations at 10 rural agent points to interact with agents and consumers and understand the working conditions, pain points, and sources of stress associated with biometric failure.

Procedures for Qualitative Data Analysis : I used NVivo and Gioia's protocol to analyse the interview transcripts and observational notes.

1st-order concepts: Concepts identified directly from the transcripts and field notes.

2nd-order concepts: Grouping of 1 st -order concepts based on similarities and patterns.

Aggregate dimensions: Higher-level categories that cut across all the identified concepts and themes.

8. Result and Findings : Based on the findings from 52 semi-structured in-depth interviews, 8 focus group discussions (n=8), and field observations at cash-in/out agents' touchpoints, the results are clustered into three aggregated themes using Gioia's data structure:

1. Biometric degradation and vulnerability differentiation : The analysis reveals that biometric authentication failures follow a differential pattern, primarily targeting specific categories of the vulnerable population. There are two subthemes:

A. Biological drift and physical work : The discussion with Group A (manual labourers, farmers, and pensioners) uncovered that working in agriculture involves physical work that permanently deforms finger ridges, disrupting the automated fingerprint identification systems' (AFIS) scanning ability.

"I come to collect pension every month, but the machine fails to read my fingers because of forty years of working on the farm. The agent advises me to oil or moisten my fingers, mostly unsuccessfully, after which I am forced to walk back to the queue after waiting three hours to be served".

B. Retrying loop and psychological distress : From the on-site observation at cash-in/out POS terminals, the researcher participated in a retrying loop initiated whenever the AFIS system failed to read the fingerprint. The loop involved long queues of waiting customers, creating psychological distress and humiliation for the victim of the failure.

Observation notes: A female participant failed to scan her fingerprint six times on two different scanners, creating tension, especially when the queue was snaking in the waiting room. When the agent became frustrated, the participant withdrew and bowed her head to the viewers,

apologizing for the inconvenience caused by her inability to be authenticated.

2. Street-level bureaucracy and agent coping

Banking correspondents and agents : (Group B members) experience a tension between their consumer needs and the rigid requirements of PoS systems. They operate as street-level bureaucrats who implement policy with discretion by adopting unofficial strategies to avert transactional disruptions. The subthemes are:

A. Informal workarounds and proxy transactions : To minimize the conflict between the system requirements and the vulnerable consumers' limited capacity to meet the expectations, the agents use unofficial workarounds, including proxy transactions.

"Whenever the biometric scan of the senior customer fails three times after the queue of about ten people, I allow them to clear their transactions without using the AFIS to avoid inconveniencing the many people waiting in the queue. However, the software vendors have remained silent on this issue, noting that our contracts disallow us from using any other means of verification, even on a case-by-case basis"

– (Rural banking agent).

3. Institutional binary failures and dignity costs : The interviewees from the fintech companies (Group C members) and the financial regulatory bodies (Group D members) revealed the underlying conceptual contradictions between the automated systems and the consumer needs. The subthemes are:

A. Fraud-consumer binary : The failure of the AFIS systems to recognize the consumer's fingerprint is primarily interpreted through the lens of fraud detection, and little is done to address the shortcomings of the system requirements.

"When developing the fingerprint scanning system, the main consideration was minimizing the probability of fraud and illicit activities, including money laundering, counterfeiting, and account take-over fraud. Thus, the system's False Acceptance Rates (FAR) are prioritized over the False Rejection Rates (FRR) in mathematical calculations"

– (Fintech software developer).

B. The erosion of dignity : Whenever a bank client fails to meet the PoS scanner's requirements, the human factor is compromised unless various alternatives (one-time passwords, biometric soft tokens, visual identification) are available. The theme manifests in three ways:

Loss of livelihood for those living in remote areas who travel to the regional banks to clear their transactions since the systems do not allow them to rescan the thumb to adjust the AFIS system.

Stigmatization of the vulnerable population as dishonest if the agent suspects them of attempting to perpetrate fraud. The failure of the AFIS scanner to read the fingerprint in small towns creates an invisible binary between the wealthy urbanites and the economically disadvantaged peasants.

"The consumer rights of the vulnerable population are significantly compromised as the automated system prefers mathematical accuracy to the sanctity of human dignity. I see no other way than a public announcement that the fingerprint scanner can only authenticate your identity if you are honest enough. However, this move would compromise the security of the financial system since the FAR (False Acceptance Rates) are deliberately prioritized in the calculation process"

– (Financial sector regulator).

9. Discussion and implications

Need of research : Despite global campaigns promoting biometric identification as a key to

financial inclusion in emerging economies, critical questions about system resilience and user experience at the point of service remain unanswered. This study was initiated to address the following practical and policy-level concerns:

Addressing the Challenges of Biometric Fragility at the Point of Sale: While India's Aadhaar, Nigeria's Bank Verification Number (BVN), and Kenya's Huduma Namba have all contributed to faster Know Your Customer (KYC) processes, automated biometric systems are often challenged by physical abrasion in agricultural labourers, construction workers, and pensioners, thus creating significant False Rejection Rates (FRR) at rural Point of Sale (PoS) terminals.

Assessing the Discretionary Burden on Frontline Agents: The stress on rural bank correspondents and mobile money agents in the absence of reliable Automated Fingerprint Identification Systems (AFIS) is poorly understood. This study explores how "street-level bureaucrats" manage the tension between system-imposed security measures and the demands of impatient customers at the microfinance level.

Reassessing the Fraud Control vs. Dignity Binary: In the quest to minimize transaction fraud, automated systems have been programmed to adopt stringent mathematical thresholds in identifying matches and mismatches, thus creating a FAR (False Acceptance Rate) dilemma. This paper reviews the human cost of absolute security and proposes alternative consumer-friendly solutions.

Significance of the Work : The significance of this work is determined by its potential theoretical, methodological, and practical contributions to the socio-technical literature on digital finance:

Theoretical: This paper provides an extension of Lipsky's (2010) Street-Level Bureaucracy theory by demonstrating how human agents in the financial inclusion ecosystem make policy at the intersection of automated biometric identification and consumer protection.

Empirical: By adopting a multi-actor, multi-methodology research design, this study was able to capture the voices of vulnerable consumers (n=30:n=22 interviews+n=8 FGDs participants =30 , frontline agents (n = 15), fintech developers (n = 10), and regulators (n = 5) to establish the human cost of biometric security.

Methodological: Drawing on phenomenological interviews (n = 52), Focus Group Discussions (8 groups, n=8), and field observations at 10 rural agent locations, this study provides a qualitative research model (Gioia's protocol) for studying socio-technical systems in the global south.

Impact of the Work : The findings of this paper have the potential to influence policy and practice among digital identity designers, fintech developers, and central bank regulators:

By highlighting the human and economic cost of failed biometric scans, this study can contribute to the development of standardized fallback measures (visual scans, One-Time-Passwords, soft tokens) among financial technology developers and regulators. This paper can also help fintech developers to rethink the FAR (False Acceptance Rate) thresholds and transaction algorithms for a more inclusive digital finance. By documenting the extent of discretionary power exercised by frontline agents in processing customer transactions, this study can help central bank regulators to formalize proxy approval protocols in the absence of reliable AFIS. Finally, this paper can help the financial inclusion ecosystem to rethink consumer protection in digital finance by shifting from the status quo of conditional access to the universal right to financial access.

10. Conclusion : Biometric authentication is the cornerstone of the campaign to promote financial inclusion and state welfare in emerging economies. However, as the Biometric Security

Paradox suggests, enforcing the most rigorous fraud prevention measures, despite the intention, tends to make the system exclude the most vulnerable groups. The paradox emerges when mathematical precision overrides the human factor, resulting in intolerable error rates that affect the bottom 90% of society, especially the working class, the elderly, and other vulnerable groups not fully integrated. Generally speaking, by focusing on individual issues and problems, the modern state is capable of managing financial ecosystems in such a way that it ensures a moneyless future.

11. Reference List :

1. Anderson, R., & Smith, J. (2023). Adaptive biometric systems: A comprehensive review. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 45(3), 1123–1142. https://doi.org/10.1109/TPAMI.2022.3189000
2. Bhattacharya, S., Sharma, R., Gupta, A., & Verma, P. (2023). Deep learning approaches in dynamic biometric authentication. *Neural Computing and Applications*, 35(2), 789–806. https://doi.org/10.1007/s00521-022-07890-x
3. Chen, X., & Wang, Y. (2022). The evolution of facial recognition: Challenges and solutions. *Security and Privacy*, 5(4), e442. https://doi.org/10.1002/spy2.442
4. Das, A. K. (2023). Multi-factor authentication in the age of biometric drift. *Journal of Information Security*, 14(2), 178–195. https://doi.org/10.4236/jis.2023.142011
5. Garcia, M., Rodriguez, E., Fernandez, L., & Lopez, D. (2023). Temporal dynamics in biometric security systems. *ACM Computing Surveys*, 55(4), 1–34. https://doi.org/10.1145/3527150
6. Hassan, N., & Kumar, R. (2022). Privacy-preserving biometric authentication: Current trends. *International Journal of Information Security*, 21(5), 623–642. https://doi.org/10.1007/s10207-022-00588-4
7. Jain, A. K., Ross, A. A., & Nandakumar, K. (2022). *Introduction to biometrics* (2nd ed.). Springer. https://doi.org/10.1007/978-0-387-77326-1
8. Johnson, K. L. (2023). The impact of aging on biometric systems. *Biometric Technology Today*, 2023(3), 9–18. https://doi.org/10.1016/S0969-4765(23)00025-6
9. Kim, S., & Lee, J. (2023). Adaptive algorithm models for biometric recognition. *Pattern Recognition*, 136, Article 109124. https://doi.org/10.1016/j.patcog.2022.109124
10. Li, W., Zhang, Y., Liu, X., & Zhao, H. (2022). CNN-LSTM architectures in biometric authentication. *IEEE Access*, 10, 45678–45692. https://doi.org/10.1109/ACCESS.2022.3169000
11. Lipsky, M. (2010). *Street-level bureaucracy: Dilemmas of the individual in public services* (30th anniversary ed.). Russell Sage Foundation.
12. Malton, D., Maio, D., Jain, A. K., & Prabhakar, S. (2020). *Handbook of fingerprint recognition* (2nd ed.). Springer. https://doi.org/10.1007/978-1-84882-254-2
13. Martinez, C. (2023). Re-enrollment strategies in biometric systems. *Journal of Cybersecurity*, 9(2), 156–173. https://doi.org/10.1093/cybsec/tyad012
14. Merlin, B., Shanmugasamy, K., & Balaguru, S. (2025). The biometric paradox: What happens when your identity changes? *International Journal of Innovative Science and Research Technology*, 10(12), 373–379. https://doi.org/10.38124/ijisrt/25dec062
15. Nguyen, T., Le, H., & Vo, K. (2026). Deep learning architectures and transformer models in biometric pattern recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 48(2), 341–356. https://doi.org/10.1109/TPAMI.2026.1042511

16. Ovuevu, C. O., Bamigboye, B. A., Onuibere, S. U., Donatus, S. U., & Thomas, O. E. (2026). Design and evaluation of a secure biometric ATM using fingerprint recognition. *Journal of Advance Research in Computer Science & Engineering*, 11(1), 8–26. https://doi.org/10.61841/c8nyyc77
17. Patel, V. M. (2023). Liveness detection in modern biometric systems. *IEEE Security & Privacy*, 21(1), 44–53. https://doi.org/10.1109/MSEC.2022.3218900
18. Rodriguez, A., & Thompson, B. (2022). Medical conditions and biometric authentication. *Healthcare Informatics Research*, 28(4), 312–327. https://doi.org/10.4258/hir.2022.28.4.312
19. Sato, H. (2023). Behavioural biometrics: A secondary authentication layer. *International Journal of Biometrics*, 15(3), 267–284. https://doi.org/10.1504/IJBM.2023.130500
20. Singh, R., Kumar, M., & Patel, K. (2023). The future of adaptive biometric systems. *Nature Machine Intelligence*, 5(6), 489–502. https://doi.org/10.1038/s42256-023-00670-w
21. Smith, A. B. (2022). Siamese networks in biometric recognition. *Computer Vision and Image Understanding*, 217, Article 103341. https://doi.org/10.1016/j.cviu.2022.103341
22. Spiceworks. (2022). *Biometrics practical applications in identity and access management*. https://www.spiceworks.com/it-security/identity-accessmanagement/articles/biometrics-practical-applications/
23. Thompson, R. (2023). Cross-platform biometric authentication. *Digital Security*, 4(3), 278–295. https://doi.org/10.1016/j.digsec.2023.01.004
24. Wang, L., & Zhang, Y. (2022). Federated learning in biometric systems. *Distributed Computing*, 35(4), 567–584. https://doi.org/10.1007/s00446-022-00420-y
25. Wilson, E. (2023). Biometric data storage and security. *Journal of Data Protection*, 6(2), 89–106. https://doi.org/10.1057/jdp.2023.12
26. Xu, Y., Chen, Z., & Lin, H. (2023). Transfer learning in dynamic biometric systems. *Machine Learning and Applications*, 12(4), 423–440. https://doi.org/10.1016/j.mla.2023.100412
27. Yang, Z. (2022). IoT integration with biometric authentication. *IEEE Internet of Things Journal*, 9(5), 6786–6795. https://doi.org/10.1109/JIOT.2021.3120000
28. Zhang, H., & Liu, Q. (2023). Homomorphic encryption in biometric systems. *Cryptography and Security*, 8(3), 234–251. https://doi.org/10.1016/j.crysec.2023.03.002
29. Zhou, W. (2023). Virtual reality and biometric authentication. *Virtual Reality*, 27(2), 156–173. https://doi.org/10.1007/s10055-022-00712-w

•