Partners Universal Innovative Research Publication (PUIRP)
Volume: 04 Issue: 04 | July - August 2026 | ISSN: 3048-586X | www.puirp.com

Biometric Authentication Contemporary Trends and Systemic Failures- A Review

Dr.A.Shaji George[1], Dr.T.Baskar[2], Dr.P.Balaji Srikaanth[3]

[1]Independent Researcher, Chennai, Tamil Nadu, India.
[2]Professor, Department of Physics, Shree Sathyam College of Engineering and Technology, Sankari Taluk, Tamil Nadu, India.
[3]Associate Professor, Dept of Networking and Communications, School of Computing, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India.

Abstract - Biometric authentication has gone beyond a niche security technology and is now the standard identity layer in a smartphone, banking app, border control, and national identity programs. This review aims to describe the state-of-the-art of biometric authentication and the common failure modes of biometric systems by collating the peer-reviewed literature, standards documentation, government evaluations and documented incident reports from approximately 2015 to 2026. The five trends are server-side matching is becoming obsolete and giving way to on-device cryptographically bound verification, the trend towards multimodal and continuous authentication is gaining traction, industrialization of remote identity proofing is increasing, generative AI is becoming a growing attack vector and defense, and regulation is becoming consolidated. Failure is broken down into five categories presentation and injection attacks, demographic performance gaps, irreversible data breaches, operational and human factor failures, and governance failures. The main conclusion is that failures of matching accuracy are not the main cause of biometric failures, rather, they are failures of system architecture, evaluation practice and institutional oversight. The review finds that the direction of the field is less about the advancement of recognition algorithms and more about the ability to verify the provenance of the input, the requirement for disaggregated evaluation and irrevocability by design of biometric data.

Keywords: Biometric authentication, Presentation attack detection, Injection attacks, Deepfakes, Demographic differentials, Data breaches, Liveness detection, Identity verification.

1. INTRODUCTION

The notion of biometric authentication always has been based on a simple intuition. The body is a more trustworthy credential than anything the mind can remember or the hand can carry. A face, fingerprint, iris or voice cannot be phished or stolen, a token can be stolen, a password can be phished. This intuition has propelled amazing adoption in the last ten years. Fingerprint and face unlock for consumer smartphones became a norm after Apple launched the Touch ID (2013) and Face ID (2017), Aadhaar is a program in India that has registered over 1.3 billion people in the largest biometric identity system in the world, and remote identity verification using facial biometrics is now a regulatory requirement in banking under know-your-customer (KYC) regimes around the world.

But the same decade has also seen a downside the leakage of 5.6 million fingerprint records from the United States Office of Personnel Management and the exposure of more than one million fingerprint and

face records in the Suprema BioStar 2 platform, groundbreaking government assessments of the accuracy disparities in face recognition systems across different demographic groups, wrongful arrests based on facial recognition misidentification and, most recently, the commercialization of deepfake-driven attacks of the ability to defeat remote biometric verification at industrial scale. This review discusses both trajectories as a whole. Trends and failures in biometrics are not independent of each other almost all of the big trends in biometrics are direct institutional reactions to failure modes which have been documented. To know one without the other results in uncritical enthusiasm or in unwarranted fatalism.

2. SCOPE AND METHOD

This is a narrative review that combines four types of sources peer-reviewed literature in biometrics and security, formal evaluation programs, in particular the United States National Institute of Standards and Technology (NIST) Face Recognition Technology Evaluation (FRTE, formerly FRVT), international standards, the ISO/IEC 19795 series on biometric performance testing and the ISO/IEC 30107 series on presentation attack detection, and documented incident reports, regulatory action and industry threat data from 2015 to 2026. Where independent data are not available, industry sourced statistics are used, but clearly identified as such, as there are commercial incentives that can affect the measurement and framing of the statistics. The review focuses on biometric authentication and identity verification, and does not discuss biometric surveillance e.g., real time identification in public spaces in detail, unless it is relevant to the discussion of authentication risks due to failures in biometric surveillance.

3. CONTEMPORARY TRENDS

3.1 From server side matching to device-bound credentials

The most significant architectural shift in the last 10 years has been the shift of biometric matching from a centralized server to a secure hardware on the user's device. In the FIDO Alliance model that is used in platform passkeys, the biometric never moves off of the device, and instead, only a signed cryptographic assertion is sent across the network, which is unlocked by a match of the face or fingerprint locally. This is because this design separates the two functions early biometric systems dangerously combined identifying a person and demonstrating that identification to a remote party and because it is not possible to obtain any biometric data by compromising a server. The trend is a direct architectural response to the breach failures described in 4.3, and its legal meaning is starting to be understood in 2026 the U.S. Seventh Circuit ruled that Illinois' Biometric Information Privacy Act (BIPA) does not apply to biometric information which is processed and stored entirely on a user's device that the vendor has no access to. While not impervious to attack they are as secure as the device and the enrollment process device bound biometrics certainly are a step down in systemic risk.

3.2 Multimodal and continuous authentication

Single modality and point-in-time authentication is no longer considered to be enough for high value transactions. Two complementary answers have grown up. Multimodal systems combine two or more characteristics e.g. face and voice or fingerprint and behavior, making it more difficult for an attacker to spoof a system as they have to overcome multiple channels. Continuous authentication, which usually is based on behavioral biometrics like keystroke dynamics, gait or patterns of interaction with the device, spreads authentication throughout a session instead of focusing on the logon process. The literature has consistently demonstrated that fusion enhances robustness, but at the same time it also exacerbates the

problem of exposure to privacy, as well as the problem of fairness assessment, as the distribution of errors needs to be assessed across modalities in addition to demographics.

3.3 The industrialization of remote identity proofing

During the pandemic, digitization has come to dominate banking, fintech, gig and government account opening and onboarding, with the predominant method being to take a photo of an identity document and a live selfie. This resulted in a new attack surface of value that was just where there were no trusted hardware, no prior relationship, and no in-person fallback. Today, the main theatre of operations where the shortcomings of 4.1 are manifested is that of remote identity proofing, and the main stimulus for the need of liveness detection and injection-attack countermeasures.

3.4 Generative AI as attack vector and defense

The threat model has been changed more than ever in its history with generative artificial intelligence. According to industry telemetry read with a grain of skepticism since it comes from the verification vendors the use of deepfakes in biometric fraud attempts has risen to around 20% in 2025, while injection attacks have increased by around 40% year-over-year. In January–August 2025, Group-IB reported 8,065 attempts to evade liveness checks of a single financial institution with the help of AI-generated faces, which were injected via virtual cameras, and discovered a mature deepfake-as-a-service market, where the tooling for face swapping, synthetic identities, and voice cloning are sold at commodity prices. As seen in the 2024 Hong Kong case, where a finance worker approved transactions of around US$25 million following a video meeting with all participants being deepfakes, the risk is not just limited to automated verification systems, but to human judgment as well. Gartner predicted in 2024 that by 2026, 30% of enterprises would no longer rely on face biometrics alone and, based on evidence, this seems to have been largely realised. At the same time, AI is being used to power the defense in fact, the latest presentation attack and deepfake detection systems are also deep learning, and the arms race is very real and continuous, and there's no sign of anyone coming to a halt.

3.5 Regulatory consolidation

The governance landscape has become much more challenging. The EU AI Act bans, with limited exceptions, the use of real-time remote biometric identification in publicly accessible areas by law enforcement and deems most other uses of biometric identification as high-risk, which must be assessed for conformity and supervised by a human operator. BIPA is the most litigiously aggressive biometric law in the United States and responsible for settlements such as Meta's US$650 million settlement of face template claims, and Clearview AI's scraping of billions of facial images has resulted in a total regulatory penalty of more than US$75 million across various jurisdictions. A standardized assurance baseline is now available in the form of ISO/IEC 30107-3 testing by accredited laboratories or the FIDO Alliance's Face Verification Certification program, which was launched in 2024, but is still incomplete.

4. A TAXONOMY OF FAILURES

4.1 Spoofing failures presentation and injection attacks

The standards vocabulary of the field makes a distinction between two attack classes, based on the location of the failure. Presentation attacks involve presenting an artefact printed photo, replayed video, 3D mask in front of a real sensor and are the topic of the ISO/IEC 30107 series, which is becoming more and more effective in countering such attacks, with certified liveness detection. Injection attacks completely circumvent the sensor and inject synthetic imagery into the verification pipeline through virtual cameras,

device emulators or network level tampering. The key thing to know about the 2024-2026 period is that the certification against presentation attacks does not say anything about the injection this is because it certifies resistance to physical artifacts, not the origin of the input signal. Commercial face recognition APIs have been tested and published results have shown a success rate of deepfake impersonation between 68-78% on systems that have no proper checks for liveness and provenance, but have significantly lower success rate where such checks are implemented. The hardy lesson is architectural If a biometric system is depending on its own input channel, it's an unexamined dependency, and AI has made it easy and inexpensive to exploit.

4.2 Fairness failures demographic performance differentials

NIST's ground-breaking demographic evaluation NISTIR 8280 evaluated 189 algorithms, and found a factor of 10 to 100 false positives across demographic groups for many algorithms, with higher false-match rates for West and East African, and East Asian faces for many algorithms developed in the West, and higher false positive rates for women, the elderly and children. There are two criteria that are necessary for the balanced interpretation. First, the differentials were very algorithm dependent the smallest differentials were obtained by the most accurate algorithms, indicating that the differentials are not intrinsic properties of the algorithms, but engineering properties, and NIST's continued FRTE reporting routinely publishes disaggregated report cards showing these differentials. Second, false negatives in cooperative authentication situations are usually not catastrophic, and can be easily recovered by retesting, while false positives in identification applications are potentially lethal. In the United States, the documented misidentifications have all occurred in the context of identification, and have been the result of a combination of factors the accuracy of the algorithm, the quality of the images in the probe, and most importantly, the human over-reliance on the machine's output, in contravention of investigative policy, as was the case with Robert Williams of Detroit in 2020 and others since. Failure of fairness in biometrics is thus best thought of as socio-technical: the algorithm provides the differential and the institution provides the harm. A related, but less studied differential is disability, in that the liveness challenges of systems can have higher rejection rates for users with motor impairments, blindness, or assistive technology use, who are not the norm.

4.3 Irrevocability failures biometric data breaches

Biometrics' unique severity stems from its defining property, that it is permanent. A face and fingerprints can't be rotated, a password can. There is a lot on the record of incidents. In 2015, OPM's data breach compromised 5.6 million fingerprint records and the background-investigation files for 21.5 million people. The Suprema BioStar 2 exposure in 2019 resulted in over a million fingerprint and face images, as well as plain text administrator passwords, being left on a publicly accessible database used by banks, police departments and even defense contractors in a variety of countries. In 2024, two Indian technology vendors' unsecured databases leaked approximately 500 GB of biometric data fingerprints, facial scans and identifying marks of police, military and civilians. New York City Health + Hospitals revealed that it had been attacked and that attackers had exfiltrated fingerprints and palm prints along with medical records of at least 1.8 million people, who had been living in their network for more than two months through a third-party vendor, and researchers revealed the existence of an unsecured database containing around 9.1 million facial images linked to a people-search service. Three themes emerge from these incidents: the compromise is usually at a vendor or due to simple configuration mistakes, the biometric data was kept in a centralized repository, when an alternative architecture could have been used, and the damage is ongoing and unlimited as stolen biometrics can be used for spoofing for the victim's lifetime. For this

purpose, template-protection techniques cancelable biometrics, biometric cryptosystems have been developed in the literature but their use is still far behind what has been published in the literature.

4.4 Operational and human-factor failures

Many cases of actual biometric failure are not an attack or bias but simply a normal fragility in operation. Where the biometric gates are used to provide access to core services, the failure mode is exclusion, which occurs among manual laborers with worn fingerprints, the elderly and in low-end sensors and in poor lighting. The cases of large-scale public distribution systems with Aadhaar authentication have reported instances where the fingerprints of beneficiaries did not match, resulting in them being denied food rations, which is not an inconvenience in a welfare context, but a denial of entitlement. The other half of biometric engineering that's been overlooked is fallback design. A system is only as secure as its weakest recovery path, and only as inclusive as its most accessible one. Voice clone and social-engineering attacks have been favored targets of attacks, in part because the channels used for account-recovery and call-center are typically less stringent about verification, where the key channel failed to do so.

4.5 Governance failures

The last category of failure is institutional. The paradigm case of collection outpacing governance is Clearview AI's creation of a multi-billion-image face database, which is comprised of photos scraped from the internet without consent and not for the purposes of their publication. In 2026, Brazil's data protection authority ordered the end of biometric classroom-attendance matching, which is a common example of proportionality failure, as it is used for a trivial purpose and is an irrevocable identifie. The constant difference between what vendors report as accuracy on populations and conditions the vendor chooses and what happens in the field is a more subtle governance failure of evaluation practice that is addressed by the ISO/IEC 19795 standards but cannot be enforced.

5. DISCUSSION

Four cross cutting lessons can be gleaned.

1. First, it's not the matcher anymore that's the weakest link. For top algorithms, accuracy of recognition on high-quality samples is amazingly high, while current failures are focused on data custody breaches, tail-of-distribution users fairness and accessibility, and input provenance injection, and recovery paths. This should result in a reweighting of research and procurement focus.
2. Secondly, architecture is more important than algorithm. The biggest risk reduction of the decade was the device bound credentials, which did not require any changes in the matching process, but instead eliminated the central honeypot and the transmission of biometric data over the network.
3. Third, evaluation should be an adversarial, longitudinal and disaggregated process. Headline equal error rate hides who is responsible for the errors, performance degradation over time and template aging, as well as the system's performance against the current attack toolkit versus last year's.
4. Fourthly, the nature of biometrics is changing from proof to signal. The growing opinion in both industry and the standards path is that a biometric match is one of several factors that should be considered in a multi-layered decision, with other factors such as device integrity, session provenance and behavioral context. It's not a retreat from biometrics, it's a maturation the early marketing of the technology supported the notion of certainty and the future of biometrics is one of calibrated confidence.

Equally, a balanced assessment should not be 'declinist'. But there are also documented failures and real success on a large scale, with billions of authentications now taking place without any hassles or insecurities, measurable reduction in account-takeover fraud through the use of biometrics instead of passwords, and financial inclusion gains in populations lacking documentary identity. Failure record points to particular architectures and governance practices, not the modality per se.

6. LIMITATIONS

There are three caveats to this review.

1. First, there are several quantitative statements about the prevalence of attacks that are based on vendor telemetry specifically Entrust and Group-IB, and so may not be representative of the general population of attacks, since the customers of those vendors and their detection capabilities may not be representative independent, population-representative measurement of biometric fraud is not currently available.
2. Second, a record of incidents is survivorship-biased, that is, it only reflects those incidents that have been detected and disclosed, leaving out those that are not detected and jurisdictions that do not have disclosure requirements.
3. Thirdly, the field is evolving so rapidly that any description of the current state of deepfake–defense dynamics is a snapshot any 2025-2026 findings are provisional.

7. CONCLUSION

To sum up the past decade of the history of biometric authentication, it has been a shifting of the Achilles heels the matching algorithms became more accurate, the break points were moved to the input channel, the database, the demographic margins, and the institutions that are introducing the technology. The most significant open problems of the field are similarly not recognition problems. They are ensuring that pixels are from a real sensor observing a real person that there is no central repository of irrevocable identifiers that can be broken into that there is no central evaluation or burden of error placed on already marginalised groups and that biometric decisions are made in a governance structure that is commensurate with the consequences of those decisions. Security and inclusion are the clear hallmarks of systems and jurisdictions that internalize these lessons those that rely on a biometric match as an assumption in itself are, by the evidence gathered here, mistaken.

REFERENCES

[1] Chen, H. and Magramo, K. (2024). Finance worker pays out $25 million after video call with deepfake 'chief financial officer'. [online] CNN. Available at: https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
[2] Drèze, J., Khalid, N., Khera, R., & Somanchi, A. (2017). Aadhaar and food security in Jharkhand: Pain without gain? Economic and Political Weekly, 52(50).
[3] Entrust. (2025). 2026 identity fraud report. https://www.entrust.com/resources/reports/identity-fraud-report
[4] European Union Agency for Cybersecurity (ENISA). (2022). Remote identity proofing: Attacks & countermeasures. https://doi.org/10.2824/183066 (ISBN 978-92-9204-549-4)

[5] European Union Agency for Cybersecurity (ENISA). (2024). Remote ID proofing good practices. https://www.enisa.europa.eu/sites/default/files/2024-11/Remote%20ID%20Proofing%20Good%20Practices_en_0.pdf

[6] European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). EUR-Lex. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[7] FIDO Alliance. (2024, May 29). FIDO Alliance addresses accuracy and bias in remote biometric identity verification technologies with first industry testing and certification program [Press release]. https://fidoalliance.org/fido-alliance-addresses-accuracy-bias-in-remote-biometric-identity-verification-technologies-industry-first-testing-certification-program/

[8] Fowler, J. (2024, May 23). Indian military & police biometrics exposed in data breach. Website Planet. https://www.websiteplanet.com/news/india-biometric-breach-report/

[9] Fowler, J. (2026, August). Facial recognition database leak exposes 9M images [Research disclosure]. ExpressVPN. https://www.expressvpn.com/blog/clarity-check-data-exposed/

[10] Gartner. (2024, February 1). Gartner predicts 30% of enterprises will consider identity verification and authentication solutions unreliable in isolation due to AI-generated deepfakes by 2026 [Press release]. https://www.gartner.com/en/newsroom/press-releases/2024-02-01-gartner-predicts-30-percent-of-enterprises-will-consider-identity-verification-and-authentication-solutions-unreliable-in-isolation-due-to-deepfakes-by-2026

[11] Grother, P., Ngan, M., & Hanaoka, K. (2019). Face recognition vendor test (FRVT) Part 3: Demographic effects (NISTIR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

[12] Borak, M. (2026). Deepfake-as-a-service revolutionizing biometrics spoofing and identity fraud: Report. [online] Biometric Update | Biometrics News, Companies and Explainers. Available at: https://www.biometricupdate.com/202601/deepfake-as-a-service-revolutionizing-biometrics-spoofing-and-identity-fraud-report [Accessed 22 Aug. 2026].

[13] George, D. (2025c). Sanchar Saathi Digital Security versus Civil Liberty in India 's Smartphone Era. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17838468

[14] G.T. v. Samsung Electronics America, Inc. (7th Cir. 2026). (Reporter volume/page and docket number: manual check required.) Verified case analysis: Mayer Brown. (2026, August). Seventh Circuit holds that BIPA does not reach biometric data that remains on a user's device. https://www.mayerbrown.com/en/insights/publications/2026/08/seventh-circuit-holds-that-bipa-does-not-reach-biometric-data-that-remains-on-a-users-device

[15] George, D. (2025b). Digital Watermarking in Cloud Environments for Copyright Protection: A Comprehensive review. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17726895

[16] Hill, K. (2020, June 24). Wrongfully accused by an algorithm. The New York Times. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

[17] George, D. (2025a). Beyond the dashboard critical perspectives on digital employee monitoring and the paradox of productivity measurement in contemporary organizations. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17702042

[18] Information Commissioner's Office. (2022, May 23). ICO fines facial recognition database company Clearview AI Inc more than £7.5m [Press release]. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/

[19] George, D. (2026a). Digital dividend data taxation's potential to transform India's economy and redefine fiscal policy in the mobile era. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19021896

[20] George, D. (2026b). Digital Inclusion vs. Fiscal Revenue Assessing India's Per-Gigabyte Data Tax. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.20922074

[21] International Organization for Standardization. (2023). ISO/IEC 30107-3:2023 — Information technology — Biometric presentation attack detection - Part 3: Testing and reporting. https://www.iso.org/standard/79520.html

[22] George, D., & Dr.T.Baskar. (2026). India's Unified Payments interface architecture, adoption, and the policy challenges of a public digital payment infrastructure. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.21891881

[23] National Institute of Standards and Technology. (n.d.). FRTE 1:1 verification - Demographic effects [Ongoing evaluation]. https://pages.nist.gov/frvt/html/frvt_demographics.html (standing evaluation page; confirm current URL, as FRVT pages have been renamed FRTE)

[24] NPR. (2015, September 23). OPM now says more than 5 million fingerprints were stolen in cyberattack. https://www.npr.org/sections/thetwo-way/2015/09/23/442861282/opm-now-says-more-than-5-million-fingerprints-were-stolen-in-cyberattack

[25] Ólafsdóttir, B., Rathgeb, C., & Kolberg, J. (2024). A case study on the inclusiveness of biometric technologies for individuals with congenital disabilities. In Proceedings of the Nordic Conference on Human-Computer Interaction (NordiCHI 2024). ACM. https://doi.org/10.1145/3679318.3685485

[26] Ramiro, A. (2026, August). Brazil's data protection agency faces landmark test on kids and facial recognition. Tech Policy Press. https://www.techpolicy.press/brazils-data-protection-agency-faces-landmark-test-on-kids-and-facial-recognition/

[27] Tariq, S., Jeon, S., & Woo, S. S. (2022). Am I a real or fake celebrity? Evaluating face recognition and verification APIs under deepfake impersonation attack. In Proceedings of the ACM Web Conference 2022 (WWW '22). ACM. https://doi.org/10.1145/3485447.3512212

[28] Taylor, J. (2019, August 14). Major breach found in biometrics system used by banks, UK police and defence firms. The Guardian. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

[29] TechCrunch. (2026, May 18). NYC Health + Hospitals says hackers stole medical data and fingerprints during breach affecting at least 1.8 million people. https://techcrunch.com/2026/05/18/nyc-health-and-hospitals-says-hackers-stole-medical-data-and-fingerprints-during-breach-affecting-at-least-1-8-million-people/