JIRBDAI

Journal of Institutional Research, Big Data Analytics and Innovation

EVALUATING THE SECURITY AND PRIVACY IMPLICATIONS OF USING BIOMETRIC DATA FOR AUTHENTICATION

[1]Victoria Oluwaseyi Adedayo-Ajayi, [2*]Ojo Omotayo Job, [3]Afolabi Akinlolu, [4]Akinola Olufemi Olaoluwa

[1,2,3,4] Department of CyberSecurity,
Ladoke Akintola University of Technology, Ogbomoso, Nigeria
*Corresponding author: ojojo@lautech.edu.ng

ABSTRACT: The increasing adoption of biometric data for authentication in various domains has revolutionized identity verification systems by offering enhanced security, efficiency, and user convenience. Biometric authentication, leveraging unique physical and behavioral traits such as fingerprints, facial recognition, and iris patterns, has become a preferred alternative to traditional password-based systems. However, its implementation raises critical concerns regarding the security and privacy of sensitive biometric information. Unlike passwords, compromised biometric data cannot be reset, posing significant challenges in protecting individuals' identities. This study evaluates the security vulnerabilities inherent in biometric systems, including spoofing attacks, database breaches, and template aging. It also examines the privacy implications of biometric data collection, storage, and potential misuse, emphasizing the importance of transparent data management practices. Furthermore, the research assesses existing regulatory frameworks such as the GDPR and Biometric Information Privacy Act (BIPA), highlighting gaps in global standards for biometric data protection. Through a comprehensive analysis of biometric modalities and their implications, this study identifies key challenges and proposes technological advancements and policy recommendations to enhance the security and privacy of biometric systems. By addressing these concerns, the research aims to support the development of more secure and privacy-conscious biometric technologies, balancing innovation with ethical and legal considerations.

KEYWORDS: Biometric Data Authentication, Data Privacy, Biometric Systems, Cybersecurity

I. INTRODUCTION

The increasing need for security has led to the involvement of biometrics in our daily lives. Biometric authentication is now a popular technique to confirm identities as it replaces and complements ID credentials commonly used as passwords and security tokens [1]. There has been a constraint with these traditional approaches, mainly because they are easy to misplace or lose and can be forged conveniently. Biometrics in their turn use distinctive features of humans, both physical, such as fingerprints and iris scans, as well as behavioral, like vocal recognition, and gait recognition, which belong to the person and cannot easily be emulated or forgotten [2][3]. One of the key underlying technologies that has provided biometric authentication with a shot in the arm is artificial intelligence (AI) and machine learning (ML). These have expanded the precision of biometric systems making identity and verification processes faster and more effective. [4]AI algorithms can now process giant biometric databases to detect a common pattern in the human biometric data stream to avoid problems like false positives and negatives that would formerly degrade the significance of biometric information. As a result, the AI and ML combination has helped provide biometric solutions in consumer electronics, finance, and even in some public areas such as airports [5]. Nonetheless, biometrics technologies have several drawbacks, especially in matters of privacy and security. While passwords or other forms of identification can be easily replaced if ever the criminals get

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.17889996

hold of them, biometric data remains with the person for the rest of their lives [6]. This presents a particularly novel danger: if biometric data is stolen, it can be used for malicious purposes, thereby jeopardizing the privacy and identity of individuals [7]. Such risks explain why protective measures of biometric information as well as the ethical policies to govern the utilization of biometric information should be tight. Secondly, the use of biometric authentication also has problems such as privacy, as well as problems left to everyone and no one at the same time. Not everyone has features that can be easily scanned or have corresponding identifiable features that can be recorded by existing modern technologies. For instance, individuals with some physical impairments will be unable to offer fingerprints or facial images as demanded by traditional biometric systems. This limitation sparks several vital ethical issues regarding biometric security solutions' accessibility since their usage increases in societies' vital sectors such as healthcare and transportation [8]. As biometric systems become more integrated into daily life, understanding their security and privacy implications is essential for policymakers, technologists, and end-users. Therefore, the research fills existing knowledge gaps through an integrated evaluation of biometric authentication system security and privacy risks which uses systematic literature review and expert interview methods. The research aims to document current problems while creating a data-driven assessment for responsible biometric system development and implementation and management.

II. RELATED WORKS

A. Overview of Biometric Modalities

Biometric authentication systems use various physical or behavioral characteristics, known as biometric modalities, to identify and verify individuals [9]. Biometric authentication relies on an individual's unique biological traits to confirm their identity and provide secure access to electronic systems. These technologies operate on the principle that each individual can be uniquely identified through one or more biological features, such as fingerprints, hand geometry, retinal or iris patterns, voice, DNA, or signatures. Figure 1 presents the Classification of Biometrics.

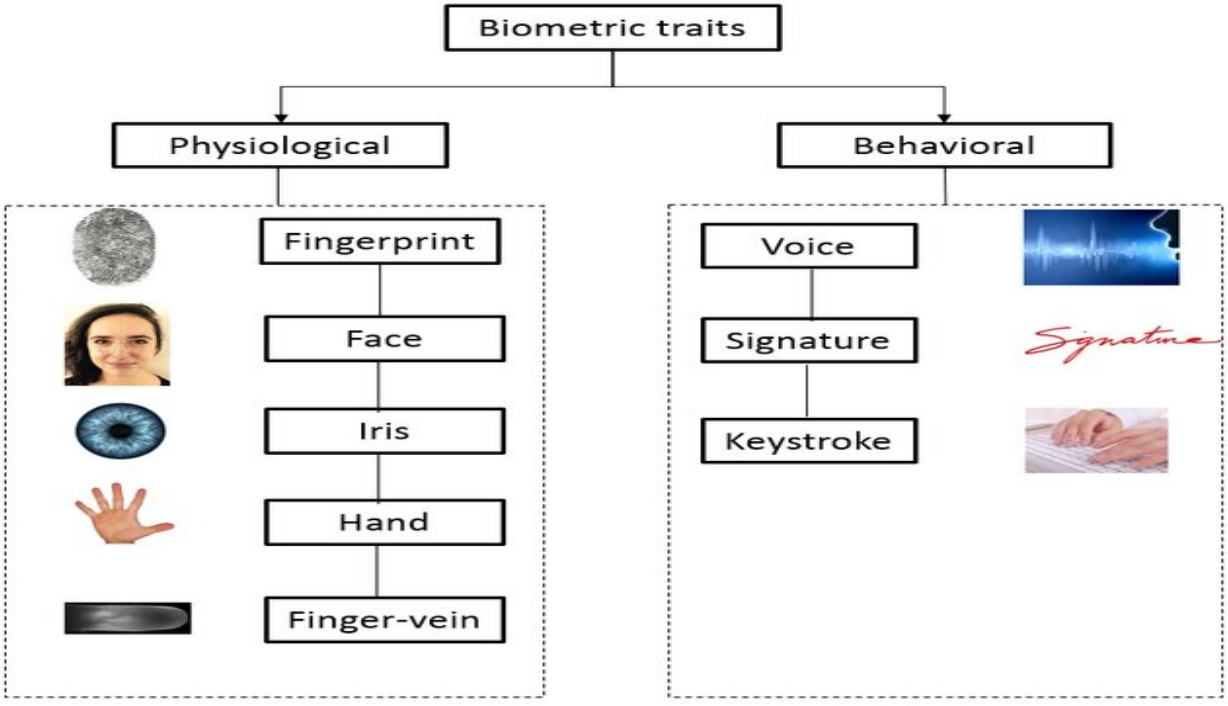

Figure 1: Classification of Biometrics [6]

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.17889996

(a). Physiological Biometrics: These include fingerprints, iris patterns, facial features, and DNA, which remain consistent over time and are unique to each individual.[10]
(b). Fingerprint Recognition: Among the most widely adopted, it is used in smartphones, border control, and workplace access systems.
(c). Facial Recognition: Increasingly popular for surveillance and consumer devices, it leverages the unique structure of an individual's face.
(d). Behavioral Biometrics: These involve traits influenced by an individual's actions, such as voice recognition, typing rhythms, or gait analysis. Behavioral data can vary with time and circumstances, posing distinct challenges.[11]
(e). Emerging Biometrics: Advances in technology have introduced new modalities like DNA-based identification and brainwave patterns, offering promising but untested avenues for biometric authentication.

III. RESEARCH METHODOLOGY

This study adopts a qualitative research design to gain an in-depth understanding of the privacy and security issues associated with biometric authentication. Qualitative methods are well-suited for this research because they enable a comprehensive exploration of complex themes, such as security vulnerabilities, data privacy, and regulatory frameworks. Additionally, secondary data analysis provided insights from existing literature and policy reviews.

Semi-structured interviews were conducted with eight experts in cybersecurity, data privacy, and biometric technology. Participants were selected based on professional experience with biometric design, penetration testing, compliance, or digital identity management. A thematic analysis approach was used. Interview transcripts and literature findings were categorized into themes, including Security vulnerabilities, Privacy issues, Regulatory challenges, Countermeasures, and Future trends. Figure 2 shows the research flowchart

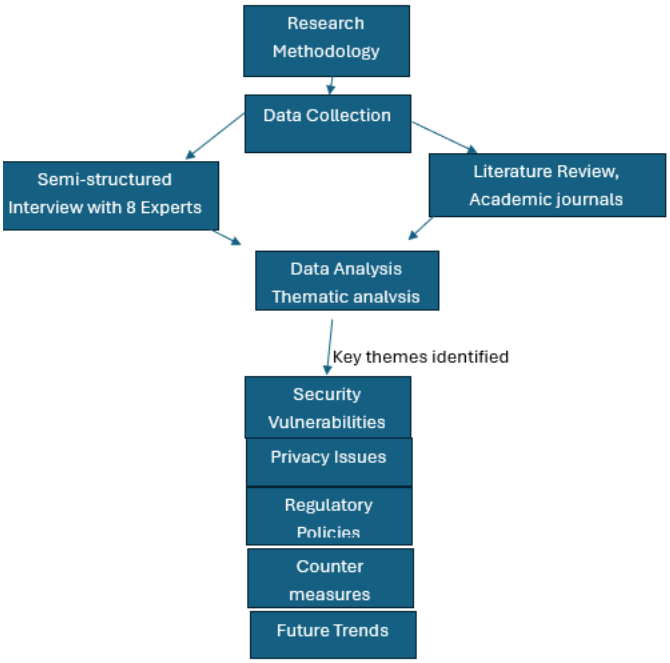

Figure 2: The Research Flowchart

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.17889996

IV. RESULTS AND DISCUSSION

This section presents the findings of the research on the security and privacy implications of biometric authentication systems, based on a combination of secondary data analysis and expert interviews. The results are organized according to the research objectives: an overview of biometric authentication methods, analysis of security vulnerabilities, exploration of privacy concerns, and evaluation of existing regulatory frameworks.

A. Security Vulnerabilities in Biometric Systems

Table 1 identifies Security Vulnerabilities, their potential impact, and typical countermeasures. The analysis identified several critical security vulnerabilities in biometric systems, including spoofing attacks, presentation attacks, template aging, impersonation attacks, and database breaches.

Table 1: Vulnerability, its potential impact, and typical countermeasures

Vulnerability	Description	Impact	Countermeasures
Spoofing Attacks	Use of fake biometrics (e.g., artificial fingerprints or masks) to deceive the system	Unauthorized access, data breach	Liveness detection, anti-spoofing tech
Presentation Attacks	Use of pre-recorded or manipulated biometric samples to bypass authentication	Identity theft, fraud	Presentation attack detection algorithms
Template Aging	Degradation of biometric template over time due to age or physical changes	Reduced accuracy, increased false rejections	Regular template updates, adaptive tech
Impersonation Attacks	Exploitation of weak enrollment processes to register fake biometric data	Fraudulent access	Rigorous enrollment protocols, MFA
Database Breaches	Unauthorized access to databases storing biometric templates	Massive data leaks, privacy violations	Strong encryption, access controls

The study confirmed that spoofing attacks, such as using artificial fingerprints or masks, remain a significant vulnerability. Although countermeasures like liveness detection are increasingly effective, these methods are not foolproof. Furthermore, presentation attacks, which involve manipulating biometric samples, highlight the need for continuous updates to detection algorithms to counter sophisticated attempts at unauthorized access. The research aligns with these findings, indicating that spoofing and presentation attacks are among the top threats in biometric security. Template aging, whereby changes in a user's physical characteristics degrade recognition accuracy over time, is a notable challenge. Findings showed that systems relying on static templates may reject legitimate users, necessitating adaptive or retrainable templates to maintain accuracy. Database breaches emerged as a critical risk, underscoring the need for encrypted storage and restricted access to protect sensitive biometric data. Literature in cybersecurity supports these findings, advocating for stronger protections around biometric databases, as breaches could compromise the immutable traits that define biometric systems.

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.17889996

B. AI-Driven Risks in Biometric Authentication

The combination of artificial intelligence (AI) with machine learning (ML) in biometric authentication systems has brought improved recognition accuracy and enhanced scalability and adaptability. The implementation of these technologies has created new security threats which standard biometric systems were not created to handle. Expert interviews and current studies show that AI technology creates four primary security threats which include: algorithmic bias and explainability challenges and deepfake-based presentation attacks and adversarial machine learning attacks.

(a). Algorithmic Bias in Biometric Recognition

AI-based biometric systems which use facial recognition technology demonstrate racial and gender discrimination through their incorrect identification of people. Research by [15] demonstrated that facial recognition systems produce worse results when identifying darker-skinned women than when identifying lighter-skinned men because of unbalanced training data and discriminatory algorithmic design. The experts confirmed this issue because biased algorithms could result in an authentication system discrimination and a security system misidentification of people. AI-based biometric systems require regular fairness assessments and multiracial training data, and transparent model creation methods to address their ethical and operational and legal issues.

(b). Deepfake-Enabled Attacks.

Generative AI through GANs and diffusion models enables the production of authentic-looking artificial facial content and audiovisual materials. The deepfake technology enables attackers to perform advanced presentation attacks that successfully evade facial and voice authentication systems. The experts documented actual cases where attackers employed voice cloning technology to trick financial authentication systems. The fast-paced development of deepfakes makes it challenging for current liveness detection systems and sensor-based security measures to identify these fake content types.

(c). Expert Insights on Security Measures

Experts interviewed emphasized the importance of ongoing innovation in countermeasures to stay ahead of attackers. Many highlighted that, while traditional anti-spoofing measures remain effective, new technologies such as federated learning and decentralized storage are increasingly used to secure biometric data at its source rather than relying on centralized storage.

(d). Privacy Concerns in Biometric Authentication

The study found that a significant privacy concern in biometric systems is the collection and use of sensitive data without adequate user consent. Experts stressed the need for transparent, informed consent processes to ensure users understand how their data will be used and stored. Table 2 presents an analysis of common privacy concerns, their causes, and potential solutions.

Table 2: Analysis of common privacy concerns, their causes, and potential solutions.

Privacy Concern	Cause	Solution
Unauthorized Data Access	Weak access controls, database vulnerabilities	Robust encryption, strict access policies
Data Misuse (e.g., Surveillance)	Lack of data use limitations	Transparent data policies, clear regulations
Cross-Matching and Sharing Risks	Data sharing across multiple platforms	Data minimization, user consent for sharing

The analysis revealed that users often lack control over their biometric data, raising concerns about informed consent. Findings suggest that many systems do not adequately explain the purposes or duration of data retention, which aligns with privacy scholars' criticism of opaque consent processes in biometric

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.17889996

systems. Also, transparent and user-centric consent practices are necessary to build trust, as supported by literature suggesting that users are more willing to adopt biometric technology when they understand and can control its use. Data misuse, such as unauthorized sharing or surveillance, emerged as a key privacy concern. The study found that cross-matching across systems raises the risk of data misuse, potentially enabling profiling and tracking without user consent. The cross-matching of biometric data across platforms raises concerns about potential misuse. Several experts pointed out that when data is shared without sufficient regulation, it creates a risk of excessive tracking and profiling.

C. Evaluation of Regulatory Frameworks for Biometric Data Protection

The study reviewed key regulatory frameworks, including the General Data Protection Regulation (GDPR) in the EU and the Biometric Information Privacy Act (BIPA) in the U.S. These regulations set standards for data handling, consent, and data retention as presented in Table 3. However, gaps remain, particularly in the consistency of regulatory approaches across countries.

Table 3: Evaluation of Regulatory Frameworks for Biometric Data Protection

Regulation	Region	Key Provisions	Limitations
GDPR	European Union	Informed consent, data minimization, user rights	Limited guidance on emerging technologies
BIPA	United States	Consent, secure storage, private right of action	Only applies in Illinois, lacks federal reach
California Consumer Privacy Act	United States	Data rights, transparency, opt-out provisions	No specific provisions for biometric data

Regulations such as GDPR in the EU and BIPA offer strong protection, including requirements for consent, secure storage, and limited use of biometric data. However, findings suggest that the absence of unified, global standards creates inconsistencies and compliance challenges, particularly for organizations operating across borders. Experts indicated that while existing frameworks cover fundamental aspects of data protection, they often lag technological advancements, especially regarding emerging biometric modalities and new AI-driven techniques. Furthermore, findings highlighted a need for clearer guidelines on data sharing, cross-matching, and retention periods, as current policies may not fully address these practices in biometric systems.

V. CONCLUSION

The research has demonstrated that biometric authentication systems are a significant innovation in identity verification, offering enhanced security, user convenience, and efficiency compared to traditional methods. The study revealed several critical security vulnerabilities, including spoofing attacks, presentation attacks, template aging, and database breaches. While current countermeasures, such as liveness detection and encryption, address some of these risks, they remain insufficient against sophisticated attacks. Additionally, the inherent immutability of biometric traits makes breaches particularly damaging, as compromised data cannot be easily replaced. Addressing these vulnerabilities requires continuous innovation in security technologies and adaptive systems capable of managing biometric changes over time. It is highly recommended that organizations begin to integrate internationally recognized standards for biometric template protection, adopt robust presentation-attack detection mechanisms, and strengthen system resilience against deepfake manipulation and adversarial machine learning. Equally important is the shift

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.17889996

toward decentralized and federated architectures that minimize the risks associated with centralized biometric repositories and reduce the impact of large-scale data breaches. Regulatory frameworks should be enhanced to mandate rigorous impact assessments, enforce clearer consent practices, ensure fairness and transparency in AI-driven decision-making, and provide stronger oversight for biometric deployments across sensitive sectors. Ultimately, a balanced approach that combines technological innovation with ethical, legal, and user-centric safeguards will be essential for building secure, trustworthy, and future-proof biometric authentication ecosystems in an increasingly AI-driven world.

REFERENCES

[1] Albalawi, S., Alshahrani, L., Albalawi, N., Kilabi, R., & Alhakamy, A. (2022). A Comprehensive Overview on Biometric Authentication Systems using Artificial Intelligence Techniques. International Journal of Advanced Computer Science and Applications, 13(4). https://doi.org/10.14569/ijacsa.2022.0130491

[2] Al-Nayyef, H. (2024). Advancing Attendance: a facial recognition system empowered by deep learning techniques. Journal of Al-Qadisiyah for Computer Science and Mathematics, 16(1). https://doi.org/10.29304/jqcsm.2024.16.11435

[3] Talreja, S., Scheirer, W. J., & Valenti, M. C. (2023). Biometric Security in the Age of AI: Robustness, Explainability, and Privacy. ACM Computing Surveys, 56(3), 1–38. https://doi.org/10.1145/3617592

[4] Balamurugan, M. (2024). Biometric Authentication: a Double-Edged Sword for Security? International Journal of Science and Research (IJSR), 13(9), 170–173. https://doi.org/10.21275/sr24901230354

[5] B. Sugandi, I. Dewita, and R. P. Hudjajanto, "Face recognition based on pca and neural network," in 2019 2nd International Conference on Applied Engineering (ICAE), pp. 1–5, IEEE, 2019.

[6] Ghilom, M., & Latifi, S. (2024). The role of machine learning in advanced biometric systems. Electronics, 13(13), 2667. https://doi.org/10.3390/electronics13132667

[7] Jain, A. K., Sahoo, S. R., & Kauba, C. (2024). Biometric Presentation Attack Detection: Are We Ready for Deepfakes? IEEE Transactions on Biometrics, Behavior, and Identity Science, 6(1), 19-35. https://doi.org/10.1109/TBIOM.2023.3327993

[8] Gorodnichy, D. O., & Chumakov, M. P. (2018). Analysis of the effect of ageing, age, and other factors on iris recognition performance using NEXUS scores dataset. IET Biometrics, 8(1), 29–39. https://doi.org/10.1049/iet-bmt.2018.5105

[9] Rahouma, K. H., & Mahfouz, A. Z. (2021). Design and Implementation of a Face Recognition System Based on API mobile vision and Normalized Features of Still Images. Procedia Computer Science, 194, 32–44. https://doi.org/10.1016/j.procs.2021.10.057

[10] Habibu, T., Luhanga, E. T., & Sam, A. E. (2022). Assessment of how users perceive the usage of biometric technology applications. In IntechOpen eBooks. https://doi.org/10.5772/intechopen.101969

[11] Karampidis, K., Rousouliotis, M., Linardos, E., & Kavallieratou, E. (2021). A comprehensive survey of fingerprint presentation attack detection. Journal. https://doi.org/10.20517/jsss.2021.07

[12] Mohd, H. N., Kamarudin, M. N., Lin, C. K., Kamis, Z., & Jaya, H. T. (2013). Biometric voice recognition in security system. *Indian Journal of Science and Technology*, *7*(1), 104–112.

[13] El_Tokhy, M. S. (2021). Robust multimodal biometric authentication algorithms using fingerprint, iris and voice features fusion. Journal of Intelligent & Fuzzy Systems, 40(1), 647-672.

[14] Kindt, E. J. (2023). The EU AI Act and Its Implications for Biometric Data Processing. Computer Law & Security Review, 48, 105790. https://doi.org/10.1016/j.clsr.2022.105790

[15] Schuetz, P. N. (2021). Fly in the face of bias: algorithmic bias in law enforcement's facial recognition technology and the need for an adaptive legal framework. Minn. JL & Ineq., 39, 221.