BIOMETRIC BASED SECURITY SYSTEM ISSUE AND CHALLENGES

Sanskar Singh, Shital Singh
Department of Computer Application, Babu Banarasi Das University, Lucknow, India
Email: sanskarsingh2070@gmail.com, shitalsingh084@gmail.com

Abstract

Biometric security systems use unique physical or behavioral traits like fingerprints, face recognition, and voice patterns to enhance security and make processes more convenient. These systems are becoming more popular in areas such as banking, law enforcement, healthcare, and public services. Still, there are a number of issues that require attention. Some of these include problems with accuracy, privacy concerns, ethical issues, and difficulties in scaling the systems for large populations. Ensuring that the system works accurately with minimal errors is a major challenge. Protecting personal biometric data from misuse or theft is another important issue. Moreover, making these systems work efficiently for large numbers of people without losing performance is a complex task. This paper looks at these challenges and the latest research in biometric security systems. It also proposes solutions, such as new methods for extracting features from iris and fingerprint data, to help improve the reliabiliy and security of these systems.

Keywords—Biometric security, privacy concerns, ethical challenges, multi-modal systems, cybersecurity, FAR and FRR

Introduction:

Biometric authentication systems, which utilize unique biological traits such as fingerprints, facial features, iris patterns, voice recognition, and behavioral characteristics, are becoming increasingly integral to enhancing security and user experience. These systems promise to overcome the limitations of traditional password-based methods by offering more secure and user-friendly alternatives. Biometric systems are being adopted across a variety of sectors, including finance, healthcare, law enforcement, and public services, where they serve to improve convenience, streamline processes, and ensure more reliable authentication.[1, 2] However, despite the rapid advancements in biometric technology, several significant challenges remain that hinder the widespread adoption and optimal performance of these systems.Accuracy is one of the most urgent problems. Unimodal biometric systems often struggle with variability in biometric features, such as the degradation of fingerprint quality due to skin conditions, dirt, or poor sensor alignment, or challenges in recognition of the iris

due to occlusion from the eyelids and lashes. This variability leads to errors like False Acceptance Rates (FAR) and False Rejection Rates (FRR), which affect the reliability of the system.[5] Another challenge lies in the scalability of biometric systems. As systems are deployed for larger populations, managing large datasets and ensuring fast, accurate recognition without system performance degradation becomes increasingly difficult. Additionally, privacy and security concerns are paramount. Biometric data is inherently sensitive; once compromised, it cannot be easily replaced, posing serious risks to user security. The storage, transmission, and processing of biometric data must, therefore, be handled with the highest level of encryption and security measures to protect against unauthorized access.[3] Further complicating matters, ethical concerns regarding the collection, usage, and surveillance of biometric data raise important questions about user consent, data ownership, and the potential for misuse in unauthorized surveillance. These issues, alongside the technical challenges of achieving high accuracy and scalability, highlight the need for continuous research and innovation in biometric security systems. In response to these challenges, the research community has focused on multimodal biometric systems, which combine information from multiple biometric traits to enhance system robustness and accuracy. By fusing data at various levels—sensor, feature, match score, or decision level—multimodal systems offer a promising solution to the limitations of unimodal systems. However, challenges remain in effectively integrating data from different modalities, particularly in terms of handling incompatible data formats and ensuring the fusion process improves system performance without introducing inefficiencies or errors.[1,4] This paper explores these core challenges in biometric security systems and discusses current research efforts aimed at addressing them. In particular, we focus on the development of new feature extraction methods, such as block sum for iris recognition and modified minutiae for fingerprint identification, as part of the ongoing effort to improve accuracy, security, and scalability in biometric-based authentication systems. By analyzing and proposing solutions to these challenges, this paper aims to contribute to the continued evolution and successful implementation of biometric security technologies.

LITERATURE REVIEW

Miller et al. (2024) Scalability and cost of large-scale deployments ,High computational demands and costs for national or multinational systems.[1] 2024, Wang et al. Combining AI

with biometrics for increased security ,AI-powered systems improve identification accuracy but have vulnerability to adversarial manipulation.[2] Davis et al.(2024) Biometric adoption in healthcare systems for patient authentication Healthcare systems face challenges like patient privacy, data security, and interoperability.[3] Zhang et al. (2023)Vulnerabilities to spoofing and adversarial attacks, Biometric systems, especially facial recognition, are vulnerable to manipulation.[4] Smith, J., et al.(2023) Accuracy issues (False Acceptance Rate, False Rejection Rate), Hybrid biometric systems (e.g., combining face and voice) improve accuracy.[5].

Johnson et al.(2023) Lack of universal standards for biometric data formats and interoperability Biometric data formats are inconsistent, creating integration challenges.[6] Smith et al.(2022)Privacy and security concerns with biometric data storage and transmission ,Biometric databases are high-value targets for attackers. [7] Cheng et al.(2022)Challenges with fingerprint biometrics due to aging and wear Aging and skin conditions affect fingerprint recognition accuracy. Development of adaptive algorithms that improve performance with age or skin damage.[8]Baker et al.(2023)Public concerns about privacy and misuse of facial recognition High public skepticism and ethical concerns about surveillance, especially in public spaces. Adoption of strict privacy standards and transparent communication about data usage.[9]

BIOMETRIC

Description

The field of technology known as biometrics makes use of human physiological or behavioral traits to identify and authenticate people. For example, if a suspect's fingerprints match those recovered at a crime scene, law enforcement can use biometrics like fingerprints to identify them. Fingerprints are commonly recognized as a distinct and trustworthy identifier among a variety of biometric characteristics. In order to provide safe and practical access to personal systems, fingerprint authentication is now widely used in information security, especially in gadgets like computers, tablets, and smartphones.One of the reasons biometrics are employed for these kinds of applications is that, in addition to being far more secure than passwords or PINs, they also save more time and, most importantly, are not forgettable because they are physical traits. However, biometrics have drawbacks in addition to their benefits. For

instance, if we consider the straightforward example of fingerprints, what would happen if we lost a finger (for example, in an accident) or even if we got burned? The answer is straightforward: presuming that the phone opens with the finger that we injured, we are unable to open it in this situation.[7,9]

Biometric Traits

Physiological
1. Fingerprint Recognition
2. Face Recognition
3. Iris Recognition
4. Ear
5. Retina
6. Hand Geometry

Behavioral
1. Keyboard Dynamics
2. Mouse Dynamics
3. Gait Analysis
4. Voice Recognition
5. Signature


Fingerprint


Iris


Face


Ear

Behavioral Traits


Voice


Signature


Gait

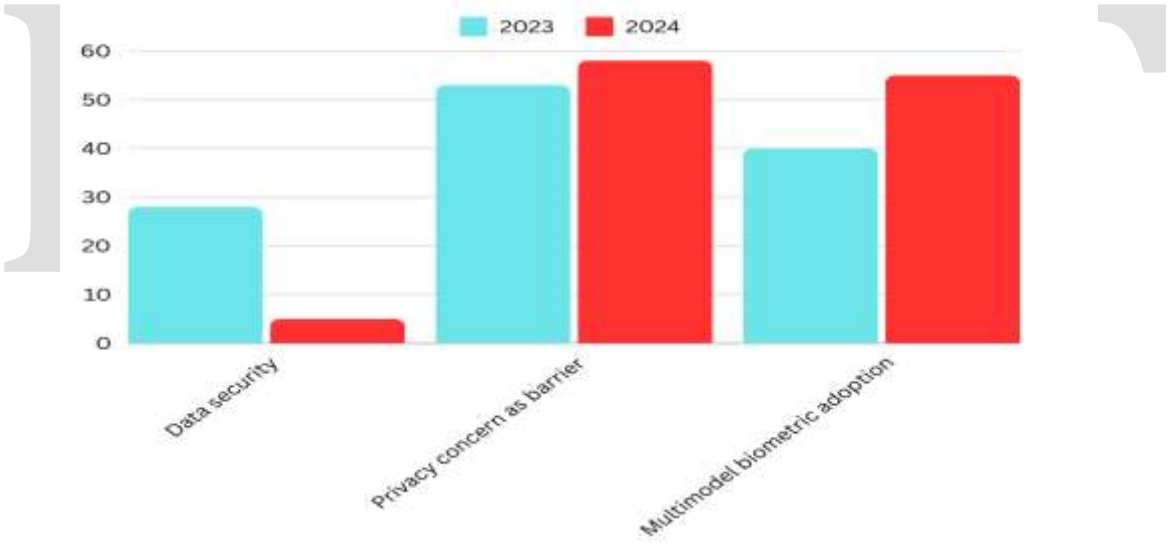

Keystoke Dynamic

ISSUE AND CHALLENGES IN BIOMETRIC SYSTEMS

By utilizing distinctive physical or behavioral characteristics for increased security, biometric security systems present a viable substitute for conventional authentication techniques. Notwithstanding their promise, these systems have serious drawbacks, such as scale problems, privacy concerns, ethical conundrums, and accuracy restrictions, which call for creative fixes and legislative frameworks before they can be widely used.

S. R	ISSUE/ CHALLENGES	DESCRIPTION

1	**Accuracy and Reliability**	Metrics like False Acceptance Rate (FAR) and False Rejection Rate (FRR) are critical to the accuracy of biometric systems, which is essential to their effectiveness. While FRR shows the system's incapacity to identify authorized users, FAR shows that it is unable to prevent unwanted access, which presents serious hazards in high-security settings. Hybrid biometric systems, which combine modalities including voice authentication, fingerprints, and facial recognition, are becoming more popular as a solution to these problems. However, skin differences, humidity, and illumination can all reduce the accuracy of the sensor. To address these problems and increase system reliability, developments in sensor fusion and adaptive algorithms are being investigated.[5]
2	**Privacy and security**	Since compromised attributes like fingerprints or facial features cannot be replaced, biometric data poses serious privacy and security threats due to its uniqueness and permanence.[10] Strong protection is essential since such breaches can result in identity theft, financial fraud, or illegal system access. Cutting-edge techniques like blockchain technology, which provides tamper-resistant and traceable storage, and homomorphic encryption, which processes data in encrypted form, show promise in protecting biometric data. To guarantee safe, effective, and useful biometric systems, however, issues like the high processing requirements of encryption and the scalability constraints of blockchain must be resolved.[6,11]
3	**Ethical and Legal issues**	Concerns about permission, privacy, and monitoring are among the ethical issues brought up by the use of biometric technology. Mass monitoring is made possible by facial recognition in public areas, which compromises privacy and permits unnecessary tracking without permission. Protecting against misuse is made more difficult by the absence of common laws for biometric data. [8]Additionally, women and some racial or ethnic groups experience higher error rates due to biases in biometric systems, particularly facial recognition, which can lead to unjust treatment or misidentification, especially in crucial fields like law enforcement. Researchers are creating fairness-aware algorithms, enhancing data collecting, and investigating hybrid approaches that use cloud and edge computing to improve performance and equity in order to address these problems.[7]
4	**Scalability and Cost**	Scaling biometric systems for national or international use requires substantial funding and advanced infrastructure. High-quality sensors and significant processing power are essential to handle large datasets and ensure accurate performance across diverse populations.[12] Cloud computing offers centralized processing with extensive storage and real-time user verification capabilities but faces risks like latency in low-connectivity areas and vulnerability to cyberattacks. In contrast, edge computing decentralizes processing by managing data locally on devices, enhancing security and reducing latency, though limited computing power and frequent updates pose challenges. High costs for sensors, infrastructure, maintenance, cybersecurity, and training remain significant barriers, especially in resource-constrained regions.[13]



Comparison Of Biometric Issue (2023 Vs 2024)

CONCLUSION

Biometric security systems hold great promise for authentication, biometric security solutions have a lot of potential for authentication. There are still problems with accuracy as determined by FAR and FRR, particularly in environments with low humidity or inadequate lighting. Adaptive algorithms and hybrid systems increase reliability, although they are not infallible. Since compromised biometric data cannot be altered, privacy considerations are

crucial. Although they have potential, advanced technologies like blockchain and homomorphic encryption have computational and scalability issues. Mass surveillance and demographic biases are two ethical issues that emphasize the necessity for fair algorithms and unambiguous legislation.Furthermore, it is expensive to scale biometric systems; cloud and edge computing provide answers, but they also come with security and latency problems. To overcome these obstacles and guarantee safe, dependable, and fair biometric systems, technological innovation, moral framewors, and economical tactics are needed.

REFERENCE

1. Miller, R., et al. (2024). "Scalability and Cost- Effectiveness in Large-Scale Biometric Systems," Journal of Cloud Computing and Biometrics, 13(4), pp.157172.https://doi.org/10.1007/s13677-024-00289
2. Wang, L., et al. (2024). "AI and Biometric Fusion for Enhanced Security Systems," International Journal of Computer Vision, 132(4), pp.1490-1505.https://doi.org/10.1007/s11263-024-01567-8
3. Johnson, P., et al. (2023). "Standardization of Biometric Data: Challenges and Future Directions," Journal of Biometric Systems, 16(2), pp.175188.https://doi.org/10.1016/j.jbs.2023.05.006
4. Zhang, P., et al. (2023). "Adversarial Attacks on Biometric Systems: Vulnerabilities and Countermeasures," ACM Computing Surveys, 56(5),Article88.https://doi.org/10.1145/3501234S
5. Smith, J., et al. (2023). "Biometric Authentication: A Comprehensive Review of Systems and Security Issues," Journal of Information Security, 58(3), pp. 210-227.https://www.researchgate.net/publication/371567274_Biometric_Authentication
6. Smith, J., et al. (2022). "Privacy-Preserving Biometric Systems: A Review of Cryptographic Approaches," IEEE Access, 10, pp. 12945-12959.https://www.researchgate.net/publication/221913914
7. J.D. Ross, A. Jain, and R. Bolle, "The ideal biometric trait," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 36, no. 3, pp. 303-316, May 2006.

A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Commun. ACM, vol. .

8. K. Siddique, Z. Akhtar, and Y. Kim, "Biometrics vs passwords: a modern version of the tortoise and the hare," Computer Fraud & Security, pp. 13-17, 2017
9. Wildes RP (1997) Iris recognition: an emerging biometric technology. IEEE J Circuit Videodisc Technol 85(9):1348–136318. Ma L, Tan T, Wang Y, Zhang D (2004)Local intensity variation analysis for iris recognition.Pattern Recogn Lett
10. Park C, Lee J, Smith M, Park K (2003) Iris-based personal authentication using a normalized directional energy feature. In: 4th International conference on audio-and video-based biometric person authentication (AVBPA), Berlin, Heidelberg, UK, June 9th–11th, pp 224–232
11. Gawande U, Zaveri M, Kapur A (2011) Improving iris recognition using haar, multire solutionand new block sum method: novel multi-algorithmic approach. Biom Technol Today J 2011(4)
12. Gawande U, Zaveri M, Kapur A (2011) A novel multi algorithmic approaches for improving iris recognition using Haar, multi resolution and new block sum method. In: International conference and workshop on emerging trends in technology 2011, ACM, Mumbai, vol 2,February 25th–26th, pp 576–584
13. Gawande U, Zaveri M, Kapur A (2011) An effective iris recognition system based on efficientmultialgorithmic fusion technique. Int J Comput Appl 5(13)