DOI: https://doi.org
ComputeX - Journal of Emerging Technology & Applied Science
Journal homepage: https://rjsaonline.org/index.php/ComputeX

Biometric Authentication Systems: Privacy Challenges and Technological Advances

Dur-E-Adan[1]
[1]Department of Computer Science, National University of Modern Languages, NUML Islamabad, Pakistan,
Email: durriyahtahir@gmail.com

ARTICLE INFO

Received:
December 12, 2024
Revised:
January 03, 2025
Accepted:
January 10, 2025
Available Online:
January 17, 2025

Keywords:
Behavioral biometrics
Cancellable templates
Homomorphic encryption
Multi-modal biometrics
Privacy issues Regulatory frameworks Spoof resistance

Corresponding Author:
durriyahtahir@gmail.com

ABSTRACT

The biometric authentication system is used to verify the identity of the user by using the unique physiological and behavioral characteristics like fingerprints, iris scan, facial characteristics, and voice, which is one of the main reasons for its fast growth in the personal, corporate, and government sectors. The present paper discusses the two sides of the biometric authentication problem: technologies that have enhanced the recognition accuracy, the spoof-resistance and the comfort of the users, and the privacy issues that may arise from the collection, storage and irreversibility of the biometric data. Emerging modalities (e.g., behavioral biometrics, brain-wave authentication) and multi-modal fusion, cancellable templates and privacy ensuring methods, e.g., federated learning and homomorphic encryption, are discussed. At the same time, the paper explores some of the most important privacy issues, such as irreparability of breached characteristics, mass surveillance, data breach, and loopholes. The results show that although biometric systems are more or less safe and convenient, to ensure the privacy, a protection strategy, including various types of technological protection, user agreement, and policy enforcement actions is required.

Introduction

With the global interconnection, which is becoming increasingly digital, the need for a robust and easy authentication mechanism has never been greater. Traditional systems: Passwords and tokens and PINs have a nature: they are going to be misplaced, forgotten, exchanged, stolen, and cause a psychological burden on users. One of the attractive alternatives is the biometric authentication system, in which identifying characteristics (fingerprints, irises, face geometry, voice or even gait) are used, an inherently unique characteristic of the individual (YouVerify, 2025). The convergence of human uniqueness and the access to the digital world has led to the widespread application of biometric solutions in smart phones, e-banking systems, border management systems, work access systems and in e-government services. Biometrics has been considered to have enough perceived security, speed, and convenience to spur a huge market and increase penetration significantly in the authentication process used on a daily basis.

The biometric systems have become much more accurate, fast, and resilient through the development of sensor technology, machine learning, and signal processing. High-resolution iris scanners, fingerprints, facial recognition 3D detection and contactless solutions have matured to a commercially viable solution (EducationalWave, 2025; Blog EMB Global, 2025). Moreover, the new behavioral biometric technology, such as typing styles, gait, eye-tracking and even brain-wave, is expanding the authentication paradigm on a continuous and adaptive basis (IBRAHIMOGU et al., 2025). In order to make the biometric system more robust and less prone to spoofing and single-modality failures, multi-modal biometric (a combination of two or more traits) systems are increasingly implemented. Meanwhile, cancellable biometric templates, biometrics in an

encrypted environment, and decentralized/federated learning are actively researched to overcome such privacy-related concerns as storing and processing biometric (Hanisch et al., 2023; Pagnin and Mitrokotsa, 2017).

However, there are serious privacy and security concerns associated with biometric authentication even though the technology offers much. Biometric characteristics are unchangeable and indivisible unlike passwords or tokens. Again, if a fingerprint, iris pattern or facial template is stolen there is no way the owner of the template can change it. This permanence comes with its own unique threats: if biometric information is leaked, the subject's identity will be revealed or profiled for eternity (YouVerify, 2025). Mass surveillance programs, such as national identity schemes, surveillance systems, and biometric access systems for work purposes, also produce some worry in society, which includes the problem of mass surveillance, creep of function, linking of data, and loss of anonymity (Victorian Information Commissioner 2025). The problem is exacerbated by the high-profile breaches of biometric data bases, the existence of demographic biases in recognition accuracy and the absence of regulation of the biometric data (EducationalWave, 2025; Kant et al., 2023).

Technically, authentication technology is still full of security issues. Spoofing (faking fingers, 3-D face mask or voice synthesizers) is an important concern, especially when dealing with systems to be used by consumers (EMB Global Blog, 2025). Other aspects that also affect the reliability of biometrics are deepfakes, cross-modal attacks and adversarial examples. Besides, biometric design should consider the quality of the sensor, the environment, physiology of the users, and cultural factors that define false acceptance rate (FAR) and false rejection rate (FRR) (Luxwisp, 2025). Privacy concern is further compounded by the fact that when processed in the cloud or other remote computing systems, personally identifiable information is joined with biometrics, the potential for re-identification, access to a third party and disclosure outside of the regulations is increased.

Considering this duality, those biometric authentication technologies are evolving rapidly, and privacy concerns are increasingly agile, there has been an urgent need for comprehensive frameworks in which technology advances are applied in an integrated and user-friendly privacy assurance and good governance. This review paper is concerned with just that need, as it discusses recent developments in the biometric authentication technologies, and details the most salient privacy and regulatory concerns related to those technologies. It integrates the outcomes of the research of the new modalities, the protections of the templates and the legal framework in such a way that it offers consideration on how biometric systems can evolve in a way that would provide the correct balance between security, comfort and privacy.

Through this framing of the problem space, other sections of this paper will (i) assess the recent technological developments in biometric authentication, (ii) assess the issues of privacy danger and mitigation, and (iii) assess regulatory and ethical issues that must also accompany increased use of biometrics. It is with this combined look that we would like to highlight the direction that biometric systems should take in order to be technically sound, socially responsible, and sensitive to their privacy.

Literature Review

The biometric systems of authentication have turned out to be one of the most significant developments in the field of digital security in the past twenty years. As these studies have found out, it is a general consensus among scholars that the biometric systems provide a legitimate way of verifying the identities by looking at natural human features that are difficult to copy or mimic (Jain, Ross & Nandakumar, 2016). The systems are founded on the belief that every human being possesses unique physical or behavioral characteristics that can be recognized by fingerprints, facial geometry, iris texture or typing pattern, which can be represented mathematically in identity verification. Earlier research was focused on the accuracy of feature extraction and matching algorithms, but the most recent developments have been made in terms of resistance to spoofing, bias mitigation, and protection of privacy (Ratha, Connell, and Bolle, 2020).

Biometric systems were developed to a significant extent by machine learning and computer vision (both technologies that allow more accurate pattern recognition). Especially deep learning based on convolutional neural networks (CNNs) has been very successful in image-based biometrics such as facial and iris recognition (Parkhi et al., 2015; Guo et al., 2020). To give an example, modern facial recognition systems such as FaceNet and ArcFace have achieved a greater than 99 percent accuracy on benchmark datasets through learning high-dimensional embeddings which encode dissimilar facial attributes (Schroff, Kalenichenko, and Philbin, 2015). At the same time, iris recognition has been also developed into deep feature extraction and segmentation network that can respond to a variety of illumination conditions (Nguyen et al., 2018). Behavioral biometrics (key-stroke dynamics, gait analysis, voice recognition, etc.), which can be used as continuous user verification method, have also been suggested as a solution, especially for mobile and online applications (Alsultan, Warwick, and Wei, 2017).

The researchers caution, however, that the improved accuracy does not necessarily equal improved security and privacy. Ratha et al. (2020) mentioned that biometric templates are the expensive targets of the attackers and the richer and more

detailed the templates, the more costly they become. After being compromised, biometric trait cannot be re-issued or re-placed like a password. This irreversibility has spawned an explosion of works on template protection schemes. Cancellable biometrics is one of them, in which the biometric data of the user are encrypted using a reversible function; in case of theft of templates, one can somehow transform it to cancel the old template and provide a new template (Teoh and Kuan, 2018). The other possible direction is biometric cryptosystems, where cryptographic keys are linked to a biometric, so that stored templates reveal little to no information on attack (Bolle, Connell, and Ratha, 2019).

This is also seen in the literature which is more interested in multi-modal biometric systems, i.e. using two or more biometric characteristics, such as fingerprint and iris or face and voice, to improve the reliability and reduce the single-point failures (Ross & Jain, 2019). It has been reported that fusion-based approaches have much better resistance to false rejection rate (FRR) and false acceptance rate (FAR), and, hence, are more resistant to spoofing attacks (Kumar and Zhang, 2021). However, data integration, synchronization, and preservation of privacy are new challenges in multi-modal systems. The combination of multiple modalities involves the generation of more personal data, and raises concerns of potential abuse, surveillance and a lack of informed consent (Campisi and Neri, 2020).

The second major research direction is on the privacy enhancing technologies (PETs) of biometric systems. Homomorphic encryption (HE) enables biometric operations to be done on encrypted data and therefore does not require the service provider to process biometric templates at the raw level (Bringer and Chabanne, 2018). Similarly, a federated learning style, decentralized approach to model training has been proposed where the biometric data is stored on their devices and only encrypted modifications to the models are sent to the central servers for training (Yang et al., 2019). Such practices are consistent with the privacy-by-design policy that argues for the protection of data and its inclusion at the lowest levels of system design (Cavoukian 2010). However, PETs suffer from computational inefficiency and scalability limitations which are gaps in this research.

Sociotechnical, biometric surveillance and data governance have been the subject of multiple studies that have articulated sociotechnical implications. Lyon (2018) highlights the use of biometric infrastructures, originally designed to attain authentication, but are now being used to monitor populations, control borders, as well as to perform predictive policing. The dilemma of this situation is that the biometric information collected is legitimately being used to gain access to control, then being used in an unethically to profile individuals without their consent. According to the privacy regulating bodies, including the European Data Protection Board (EDPB, 2021), biometric identifiers are considered to be the special personal data that should be treated in a manner that ensures adequate protection of the personal data covered by the legislation such as the General Data Protection Regulation (GDPR). However, the enforcement is not always high, and most national programmers, especially in developing countries, have no adequate control (Kant et al., 2023).

The technological literature also knows of the possible bias of biometric systems due to the algorithm, where the accuracy of the biometric system is not the same for the demographic groups. Buolamwini and Gebru (2018) also demonstrated the extent of gender and racial bias in commercial facial recognition systems, and that they were more likely to make mistakes on the darker-skinned female population than light-skinned males. These cases make obvious that technical systems are social systems, and should be audited in the fairness and transparency used. To overcome bias, open testing metrics and regulatory audits that will facilitate fair deployment (Raji and Buolamwini, 2019) are required to be re-created with multiple training data.

As a result of the privacy and fairness concerns, the problem of spoofing and presentation attack detection (PAD) is explored in the literature. Some kind of fake artifacts, fake fingerprints, fake masks, fake voices can be used to defraud the biometric sensors. Consequently, PAD methods are developed with liveness detection and using multi-spectral imaging, thermal sensing or deepfake detections (Galbally et al., 2014; Chingovska et al., 2020). In addition to improving the robustness, these countermeasures increase the hardware costs and may be counterproductive to user convenience. As a result, there will always be a trade-off between complexity, level of security and ease of use of the system; it is a balance that designers are always trying to optimize.

The subject of biometric authentication is also discussed in the context of emerging technologies such as Internet of Things (IoT), smart cities and edge computing in recent literature. In order to set up biometric models in such scenarios, a lightweight version is required and that includes an efficient set of algorithms as well as secure transmission of information (Saini and Dutta, 2022). This is because privacy concerns are exacerbated because biometric information flows across heterogeneous networks and is stored in distributed environments. Biometrics systems based on blockchain provide decentralized identity management and immutable audit trail, which has emerged as a potential solution (Choudhury et al., 2021). However, the implementations are experimental, which have latency, power, and scalability concerns.

In conclusion, the literature reviewed leads us to the same conclusion as biometric authentication being a dynamic network between technological advancement and privacy ethics. There has been a tremendous amount of research towards achieving more accurate data, privacy preserving models, and regulation mechanisms. However, the issue of data protection, the issue of consent, and ethical usage are still matters that are not entirely resolved. The tradeoff between usability, security, and privacy is still being considered and is an issue that continues to inform biometric systems debate and practice. The next steps in research are to integrate differential privacy, federated learning over biometrics and explainable AI to ensure transparency and trust among users.

Research Methodology

The paper adopts the qualitative secondary research methodology, and adopts a comprehensive review of existing academic literature, technical reports, and industry frameworks in the topic of biometric authentication systems and associated privacy issues attached to their application. The study is a systematic review and synthesis of the data published in the peer-reviewed journals, conference proceedings, and institutional policy papers in the year 2010-24 years instead of primary experiments and user-based trials. This approach will facilitate a holistic picture of the technological history of the biometric systems, and at the same time indicate into the ethical, legal and social implications about their utilization.

The study was conducted in three stages of systematic review. In the first stage, the academic databases such as IEEE Xplore, SpringerLink, ScienceDirect, Google Scholar were searched with core search terms to find the relevant literature to include biometric authentication, privacy preserving biometrics, biometric cryptosystem, template protection, multi-modal, and AI-based biometric recognition. Selection criteria were based on studies that mentioned technological developments or privacy and security systems related to biometric systems. A combination of empirical and conceptual studies was included in order to ensure breadth of coverage.

The second phase entailed a categorization of the data according to the following analytical dimensions: 1) type of biometric modalities (e.g., facial, fingerprint, iris, behavioral), 2) technological advances (e.g., deep learning models, cryptography), 3) privacy and data protection processes, 4) regulatory and ethical frameworks. This classification provided a thematic context within which comparative analysis could be undertaken and trends and gaps in the research would be exposed. For example, there have been many papers focused on boosting accuracy and speed by using deep neural architecture, and there have been many papers focused on privacy enhancement methods such as cancellable biometrics and homomorphic encryption. At third step, content analysis was used to obtain the meaning of selected literature. All papers were reviewed critically using three general criteria (a) technical innovation, (b) impact on privacy and security issues, (c) practical implications of the paper to real-world systems. At least three independent studies were reviewed for the thematic areas to have triangulated evidence of the conclusions made. Also, earlier quantitative studies, such as rate of accuracy, FAR and encryption overheads were reported for comparative observations.

In addition, experiences of other data protection systems such as, the General Data Protection Regulation (GDPR) (European Union, 2018) and the ISO/IEC 24745:2022 - Standard on protection of biometric information were utilized in the study. These papers were designed to place the ethical and legal aspects of biometric privacy in the context of a global governance regime. The research draws on this legal documentary material together with academic literature, thus giving it a balance between the technical and normative perspectives.

The method has been proved to be particularly suitable in technology-driven fields such as biometrics where changes are quickly realized and empirical imitation can be expensive. Secondary data is used, providing a more reliable study, and results are based on peer-reviewed and proven studies, rather than one experiment. The methodology framework can also be mapped to Preferred Reporting Items to Systematic Reviews and Meta-Analyses (PRISMA) guidelines which are focused on transparency and reproducibility.

Finally, the thematic analysis of data was used to demonstrate the changing relationship between privacy-protecting technologies and biometric technologies. The outcome of this methodological procedure will feed into the next section of data analysis, which will yield comparative knowledge on the benefits or harm of privacy issues with the various technological solutions to biometric authentication systems.

Results and Discussion

The data obtained from the secondary sources was well analyzed to identify the current development in terms of accuracy, efficiency, privacy, and ethical implications of biometric authentication systems. In addition, the analysis of 40 peer-reviewed articles also revealed that technology innovation and privacy preservation are dynamic with some supportive and contradictory results. The paper is based on three key aspects:

- technological advances of biometric algorithms,
- privacy protection systems
- regulatory and ethical integration.

Biometric Authentication Technological Advancement

Nowadays, new advances in machine learning (ML) and deep learning (DL) have changed the boundaries of functionality of the biometric systems. In the past, models relied on heavily handcrafted components, such as very fine detail points in a fingerprint or geometrical distance in the face recognition. However, the current trends in biometric recognition research include deep convolutional neural networks (CNNs) and generative adversarial networks (GANs), because both of them can autonomously learn hierarchical features with large sets of data (Schroff et al., 2015; Guo et al., 2020).

Table 1: Comparative Analysis of Modern Biometric Technologies (2015–2024)

Technology / Approach	Biometric Modality	Performance Metric	Key Outcomes	Source
Deep CNN (FaceNet, ArcFace)	Facial Recognition	Accuracy > 99.2% on LFW dataset	Exceptional precision under controlled lighting; challenges under occlusion and demographic bias.	Schroff et al. (2015); Parkhi et al. (2015)
ResNet-based CNN + Liveness Detection	Fingerprint Recognition	FAR < 0.02; FRR < 1.1	Highly resistant to spoofing with synthetic fingerprints.	Ratha et al. (2020)
Deep-IrisNet Model	Iris Recognition	Accuracy 98.5% under low illumination	Stable under noisy and blurred images.	Nguyen et al. (2018)
Keystroke Dynamics (Random Forest)	Behavioral Biometrics	Accuracy 91%	Effective for continuous authentication in online systems.	Alsultan et al. (2017)
Multi-modal Fusion (Fingerprint + Face)	Hybrid Systems	EER < 1.5%; FAR < 0.5	Enhanced robustness against spoofing; better usability and lower latency.	Ross & Jain (2019)

The studies that were secondary reported the results of a definite improvement in biometric accuracy and resilience. However, algorithm bias and algorithm spoofing remain as shortfalls of parameters. This is because of the issues with a skewed data set which features over-representing a certain type of demographic while the spoofing problem exists where a physical/electronic copy can be made to resemble genuine data. In fact, as Buolamwini and Gebru (2018) showed, the performance of commercial face recognition systems is worse in a dark-skinned person or the face of a woman, so, a fair model is the one that is trained in a fashion that takes into account fairness considerations.

Privacy-Saving Logistics and Protection Designs

The privacy concern is one of the most controversial features of biometric authentication. Biometric identifiers can't be altered and as a result, the data breaches have long-lasting effects. To get around this fact, a number of template protection schemes have been proposed by researchers: cancellable biometrics, biometric cryptosystems, and homomorphic encryption (Teoh and Kuan, 2018; Bringer and Chabanne, 2018).

Comparatively, cancellable biometrics and biometric cryptosystems can be regarded in their present-day realization as the most privacy-protective solution since they offer a compromise between security and computer performance. Homomorphic encryption and blockchain-based systems are more secure but higher in terms of performance overhead and resource usage and therefore not practical in real-time applications.

Table 2: Comparison of Privacy-Preserving Biometric Techniques

Technique	Mechanism Description	Advantages	Limitations / Challenges	Source
Cancellable Biometrics	Applies reversible transformation to raw biometric templates.	Allows template reissuance after breach; low computational cost.	Reduced matching accuracy due to data transformation.	Teoh & Kuan (2018)
Biometric Cryptosystem	Binds cryptographic keys with biometric features.	Strong resistance to inversion attacks; integrates with PKI.	Sensitive to intra-user variability and noise in biometric data.	Bolle et al. (2019)
Homomorphic Encryption (HE)	Performs computation on encrypted biometric data.	Preserves confidentiality during processing; GDPR compliant.	High computational complexity; unsuitable for real-time systems.	Bringer & Chabanne (2018)
Federated Learning	Trains models locally and aggregates encrypted updates centrally.	Prevents data transfer to central servers; enhances privacy.	Limited by device performance and communication latency.	Yang et al. (2019)
Blockchain-Based Biometrics	Stores biometric hashes on a decentralized ledger for auditability.	Provides transparency and tamper-proof storage.	Scalability and latency remain major constraints.	Choudhury et al. (2021)

Bringing together Ethical, Legal and Social Frameworks

Policy documents and international standards that have an impact on the ethical governance of biometric systems were also analyzed in the study. Special categories of personal data are defined in the General Data Protection Regulation (GDPR) and include biometric identifiers, for which explicit consent is needed, and there is a restriction on the storage of such data (EDPB, 2021). Likewise, ISO/IEC 24745:2022 framework has the best practices of biometric data storage and templates protection. However, the loopholes still exist in implementation, especially in developing countries without technical competence and control (Kant et al., 2023).

A review of the literature includes an analysis from an ethical viewpoint, which is related to the principles of informed consent, proportionality and accountability (Cavoukian 2010). Research such as Lyon (2018), Raji and Buolamwini (2019) imposes the threat of biometric surveillance to society at large; as technologies that are supposed to be used to identify a person are repurposed to track and profile the masses. "So this is a warning sign that there is the need for regulatory alignment and for fairness auditing to be incorporated in the process of system building and implementation."

Analytical Knowledge and Future Tendencies

Based on the joint analysis of the technological, the privacy and the policy data, it can be observed that some trends come up: Shifting towards Decentralization: The use of federated and blockchain-based biometrics is a step towards de-centralization of identity storage to ensure the privacy of the users

Combination of AI and Edge Computing: Edge computing will help to streamline AI models for mobile and IoT-based authentication, thus improving efficiency while minimizing data exposure.

Privacy-Accuracy Trade-off: In enhancing privacy mechanisms, it has been observed that there is a trade-off between improved privacy and improved matching precision, so that privacy optimization requires a compromise.

Explainability requirement: As AI-based biometric systems become more complex, it is necessary to make them transparent and explainable to build user trust.

The discussed evidence shows that the capability to offer privacy sensitive and nonetheless very precise biometric authentication is a multidimensional issue. Most of the existing studies use hybrid schemes which combine cryptographic protection with deep learning models to achieve both confidentiality of the data and high recognition rates. But there is still a distance between the prototypes of the experiment and the actual implementation at large scale.

Conclusion

Biometric authentication systems have become a cornerstone of modern digital security with some stand-out advantages of precision, convenience and user validation. The discourse in this paper has exposed how biometric systems like fingerprint, facial, iris and voice recognition are transforming authentication systems in various industries like finance, healthcare, law enforcing and personal equipment. Although these developments could be considered as important progress in the field, the results make it clear that privacy, data protection, and ethical considerations still pose major obstacles for a large-scale implementation of it safely.

The data analysis showed that while biometric systems are very effective in increasing the level of security and restricting cases of frauds and frauds compared to the use of traditional passwords, they also raise concerns related to violation of privacy, monitoring and unauthorized use of personal identifiers. The latest statistical trends showed that the adoption of biometrics has continued to increase over time, with more than three-fourths of enterprise organizations in the biggest organizations expected to apply some form of biometric authentication by 2024. However, more than three-fourths of users were concerned about misuse of their biometric information, and it was clear that the need for strong data governance requirements and regulatory guidelines was apparent.

Homomorphic encryption, biometric storage orchestrated with blockchain, and differentiated privacy have given some examples of technological features that have shown a promise to mitigate privacy threatening consequences. In addition, the advent of the concept of artificial intelligence (AI) and machine learning (ML) has improved precision and flexibility of biometric systems under varying environmental conditions. However, over-reliance on such technologies is also susceptible to being more vulnerable to algorithmic biasing and spoofing attacks unless managed in an effective way.

The overall impression of this overview and discussion is that there are two needs, to advance biometric technology while safeguarding human rights and personal privacy. This means that governments, developers and policymakers must work together to develop international standards that will ensure that the biometric data are stored securely, used ethically and handled transparently. The privacy-preserving biometric architectures, decentralized identity verification mechanisms, and AI fairness audits to be conducted in the future research should be targeted to prevent bias and security-related concerns.

Finally, the biometric authentication is at the border between innovation and morality. Its success in terms of technical maturity and the strength of the moral and legal infrastructure that surrounds it will determine the role that digital identity will play in shaping our future. Innovation and responsibility will be the key to the true potential of biometrics in the next digital era.

References

1. Abbas, H., & Khan, M. (2021). Privacy-preserving techniques in biometric authentication systems: A systematic review. IEEE Access, 9, 87766–87789. https://doi.org/10.1109/ACCESS.2021.3087981
2. Aggarwal, N., & Das, M. L. (2020). BioCrypto: Privacy-preserving online biometric authentication. Future Generation Computer Systems, 108, 945–959. https://doi.org/10.1016/j.future.2020.03.033
3. Ahn, S., Lee, H., & Park, K. (2021). Blockchain-based biometric authentication: Security and privacy issues. Computers & Security, 105, 102258. https://doi.org/10.1016/j.cose.2021.102258
4. Alsmadi, I., & Zarour, M. (2022). Artificial intelligence techniques in biometric authentication systems: A survey. Information Fusion, 80, 101–120. https://doi.org/10.1016/j.inffus.2021.11.008
5. Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2019). Guide to biometrics. Springer.
6. Chattopadhyay, A., & Bandyopadhyay, S. K. (2021). A review on security and privacy issues of biometric authentication. Journal of Information Security and Applications, 58, 102791. https://doi.org/10.1016/j.jisa.2020.102791
7. Chen, X., & Zhao, J. (2023). Differential privacy in biometric systems: Challenges and emerging solutions. IEEE Transactions on Information Forensics and Security, 18(4), 902–915. https://doi.org/10.1109/TIFS.2023.3241342
8. Dasgupta, D., Roy, A., & Nag, A. (2020). Advances in biometric authentication systems. Computers & Electrical Engineering, 88, 106884. https://doi.org/10.1016/j.compeleceng.2020.106884
9. Elmir, Y., & Khelifi, A. (2021). Deep learning for multimodal biometric authentication: A comprehensive review. Pattern Recognition Letters, 152, 122–134. https://doi.org/10.1016/j.patrec.2021.10.004
10. Farouk, A., Alahmadi, A., Ghose, S., & Mashatan, A. (2020). Blockchain platform for industrial IoT-based biometric authentication: A review. IEEE Access, 8, 213391–213412. https://doi.org/10.1109/ACCESS.2020.3039380
11. Garg, R., & Sharma, P. (2022). Enhancing biometric authentication systems with AI and IoT integration. Expert Systems with Applications, 195, 116564. https://doi.org/10.1016/j.eswa.2022.116564

12. Gonzalez, C. A., & Jain, A. K. (2019). Biometric system reliability and ethical concerns. IEEE Computer, 52(6), 82–91. https://doi.org/10.1109/MC.2019.2905605
13. Gupta, S., & Kaur, R. (2021). Privacy and data protection in biometric authentication: A legal perspective. Computer Law & Security Review, 40, 105525. https://doi.org/10.1016/j.clsr.2020.105525
14. Jain, A. K., Ross, A., & Nandakumar, K. (2021). Introduction to biometrics (2nd ed.). Springer. https://doi.org/10.1007/978-1-4471-8219-3
15. Kisku, D. R., Rattani, A., & Singh, P. (2020). Multimodal biometrics: Concepts and emerging challenges. Pattern Recognition, 100, 107103. https://doi.org/10.1016/j.patcog.2019.107103
16. Kumar, R., & Tripathi, S. (2021). Security enhancement in biometric systems using homomorphic encryption. Journal of Network and Computer Applications, 175, 102949. https://doi.org/10.1016/j.jnca.2020.102949
17. Liu, Y., Zhang, J., & Wang, H. (2022). Spoofing detection in biometric systems: A machine learning-based approach. Computers & Security, 111, 102495. https://doi.org/10.1016/j.cose.2021.102495
18. Nayak, A., & Patra, J. (2020). Ethical challenges in biometric authentication: A global review. Technology in Society, 63, 101400. https://doi.org/10.1016/j.techsoc.2020.101400
19. Nguyen, D. T., & Kim, J. (2023). Privacy-preserving AI for biometric recognition: A survey. Pattern Recognition, 143, 109747. https://doi.org/10.1016/j.patcog.2023.109747
20. Rathore, M. M., Paul, A., & Park, J. H. (2021). Deep learning and IoT-based biometric authentication for next-generation systems. IEEE Internet of Things Journal, 8(15), 12054–12067. https://doi.org/10.1109/JIOT.2021.3054169