International Journal of Economic Practices and Theories (IJEPT)
ISSN: 2247-7225
Volume 2026, Issue 1

Secure Biometric Authentication Systems: Trends and Challenges on Privacy and Security

Tanvi Dalal[1], Mitanshi Rastogi [2], Megha Bansal[3], Neha Goel[4]

[1, 2, 3] Assistant Professor, School of Information Technology, VIPS-TC, Pitampura

[4] Associate Professor, School of Information Technology, VIPS-TC, Pitampura

Abstract

The use of biometric authentication systems in the contemporary security applications has been adopted by many because of the reliability and ease of usage that they offer when it comes to identity verification. However, the growing use of biometric technologies in the large-scale and networked environments has raised the acute issues associated with the security vulnerabilities and privacy in the user domain. The literature review research is mostly conducted in terms of modality-based comparisons or performance assessment, whereas the connection between security threats and privacy-preserving mechanisms is not thoroughly studied. The paper provides an extensive threat-based review of the biometric authentication systems with the focus on privacy maintenance. In addition, the paper also discusses the latest privacy-saving methods, such as cancellable biometrics, biometric cryptosystems, homomorphic encryption, secure multi-party computation, and privacy-conscious machine learning methods. The effectiveness and limitation of the existing approaches is highlighted by the use of a structured threat-to-solution mapping.

Keywords: Authentication Biometric authentication, security and privacy, threat analysis, privacy-preserving biometrics, biometric cryptosystems.

1. Introduction

The ability to offer credible and user-friendly identity checks has seen biometric authentication systems become a fundamental part of contemporary security systems. As opposed to conventional authentication methods like passwords or tokens, biometric offers the use of physiological and behavioural traits such as fingerprints, facial features, iris patterns, voice, and gait which are uniquely associated with the person [1]. This has led to the increased use of biometrics in very diverse contexts including access control, mobile authentication, border security, healthcare and financial services.

Although these biometric authentication systems offer a number of benefits, there are major security and privacy issues raised by the system. Biometric characteristics cannot be revoked and reissued once violated as it is permanent unlike a password or cryptographic key. This is irreversible and therefore biometric data is very sensitive and appealing to the adversaries. The recent cases of biometric data breach, spoofing and unwarranted surveillance has also highlighted the importance of better protection measures. Besides, the sensitive data on biometric information that are collected and stored in large numbers is subject to some grave issues regarding user privacy, misuse of information, and adherence to laws [2].

Traditional biometric studies have mainly been interested in enhancing the recognition accuracy, strength and efficiency. These aspects are still crucial. The current biometric systems are being used in a distributed and networked environment frequently with cloud platforms, mobile devices, and third-party service providers. These environments pose a high risk to biometric systems by increasing the size of the attack surface to presentation attacks, template inversion, replay attacks, database compromise, and insider threats [3]. Simultaneously, the development of artificial intelligence and deep learning has made possible advanced spoofing methods, such as face and voice attacks based on deepfakes, that are additionally effecting biometric authentication.

Another important aspect is privacy. Sensitive personal information can be exposed to the biometric data in addition to identity like ethnicity, health conditions, and behavioural patterns. Without proper authorization or inter-matching of biometric databases, mass surveillance, profiling, and individual loss of autonomy may occur. Rules like the General Data Protection Regulation (GDPR) or standards like ISO/IEC standards have highlighted the fact that privacy-by-design principles ought to be considered when designing biometric systems. However,

there is little and uneven application of privacy-saving mechanisms into practical biometric uses [4]. Over the past few years, a number of privacy preservation methods have been suggested to deal with these issues. Efforts like cancellable biometrics, biometric cryptosystem, homomorphic encryption; secure multi-party computation, privacy-aware machine learning, etc. are designed to defend biometric data under storage, transmission and processing. Although these methods hold potential solutions, they all tend to carry trade-offs in computation complexity, system accuracy and compatibility. In addition, the existing body of research usually examines these measures separately and does not provide a systematic association with the threats they are aimed to address.

The current review papers on biometric authentication have a performance-based categorization. Despite its utility, these methods do not help to give detailed information of security threats and privacy risks at various points on the biometric pipeline. In order to overcome these shortcomings, this paper includes a threat-based analysis of biometric authentication systems with a concentration on privacy-preserving methods. The proposed work analytically examines the security risks in the biometric lifecycle, such as data collection, feature extraction, template storage, transmission, and matching. Privacy risks related to each of the threat categories are detected and mapped to the current protection mechanisms. The paper also compares the state-of-the-art privacy preserving techniques based on their security, privacy and computing ability and implementation feasibility.

The significant contributions are highlighted as follows:

- An in-depth categorization of security attacks on biometric authentication systems.
- A detailed discussion of privacy concerns of biometric data processing and storage.
- An overview of privacy preserving mechanisms, such as cancellable biometrics, biometric cryptosystems, as well as cryptographic protection mechanisms.
- An organized map on the threats/solutions that identifies the strengths and weaknesses of the current methodologies.

The rest of the paper is structured in the following way. Section 2, gives an overview of the traditional biometric authentication systems and the mechanism of operation. Section 3, talks of security threats and related privacy risks. Section 4, is an overview of the state of the art privacy preserving methods. Section 5, contains threat to solution mapping. Lastly, Section 6, indicates conclusion and the future research directions.

2. Traditional Biometric System for identity verification and Security threats

Biometric authentication system is used to verify or identify people through their distinguishing physiological or behavioural characteristics [3]. Biometric systems are based on inherent human characteristic rather than on traditional methods of knowledge-based or token-based authentication systems and therefore are more convenient and less forgeable. In this section an overview of biometric modalities, the overall architecture of biometric authentication systems, and the stages of the work where security and privacy vulnerabilities can occur are discussed.

2.1 Biometric Traits Classification

Biometric characteristics are generally divided into two, namely, physiological and behavioural. Physical characteristics of human body are the basis of physiological biometrics. This may be fingerprints, facial features, iris scan, retina scan, and hand geometry. These characteristics tend to be resistant to changes and are very accurate in recognition, and hence can be applied in situations where a high level of security is needed (like in border controls as well as national identity systems).

Behaviour biometrics is based on human behaviour patterns which include voice, signature dynamics, keystroke dynamic and gait. Such characteristics are conditioned by environment and psychological factors, and can change with time. However, behavioural biometrics has benefits of constant authentication and non-invasive data capture making it very helpful in remote authentication and mobile authentication [5].

Each biometric modality has its own distinct benefits and drawbacks with respect to the accuracy, usability, permanence, and spoofing resistance. In turn, multimodal biometrics that unites several traits together to enhance

the reliability and security are widely used by modern authentication systems. Table 1, demonstrates comparison of various biometrics modalities.

Table 1 Comparison of various biometrics modalities

Biometric Traits	Advantages	Limitations	Typical Applications
Physiological Traits			
Fingerprint	High accuracy Low cost	Susceptible to spoofing, wear and tear	Mobile devices Access control
Face	Non-intrusive Contactless	Sensitive to lighting, spoofing, deepfakes	Surveillance Smartphone authentication
Iris	Very high accuracy Stable over time	Expensive sensors, user discomfort	Border control National ID
Retina	Extremely accurate	Intrusive High cost	High-security environments
Behavioural Traits			
Voice	Hands-free User friendly	Noise sensitive Voice spoofing	Call centres, remote authentication
Gait	Non-intrusive Continuous	Low accuracy, affected by environment	Surveillance, continuous authentication
Signature	Socially accepted	High intra-class variation	Banking Document verification

2.2 Biometric Authentication System Architecture

A standard biometric authentication system is based on a sequence of processing steps, which include many steps as shown in Fig. 1 [6].

1. Data Acquisition: Some sensor like a fingerprint scanner, camera or microphone captures the biometric trait. Acquired data quality has a great impact on system performance and can be attacked through a presentation attack, which attacks that can be spoofed include those based on artificial fingerprints or facial images.
2. Pre-processing and Feature Extraction: Raw biometric information is improved and changed into discriminative features. The objective of this step is to eliminate noise, regularize variations and come up with a small feature representation. Algorithms of feature extraction are important in the determination of the recognition accuracy and system robustness.
3. Template Generation and storage: Features that have been extracted are turned into a biometric template and are stored in database or secure module. Biometric templates security is a huge security issue since they cannot be reissued like passwords. Storage of templates can be built centrally, dispersed or cloud-based based on system architecture.
4. Matching: In authentication, the input biometric sample is matched with the template stored using a comparable algorithm. Compared to a predetermined threshold, a similarity score is produced and compared to reject or accept it.

Such pipeline architecture presents several attack points, which the attackers can use to violate the security of the systems or privacy of the users.

2.3 Operational Modes of Biometric Systems

Biometrics authentication systems work in two major modes:

- Verification (1:1 matching): The system authenticates the identity by contrasting the biometric sample typed in with one stored template.
- Identification (1: N matching): This system identifies an individual by matching the input sample with all the templates present in the database.

The access control systems usually involve verification mode and an application of identification mode is in surveillance and forensics. While biometric authentication provides strong identity assurance, it remains vulnerable to a range of security threats targeting different system components. Section 3 examines these threats in detail and highlights their implications for system security and user privacy.

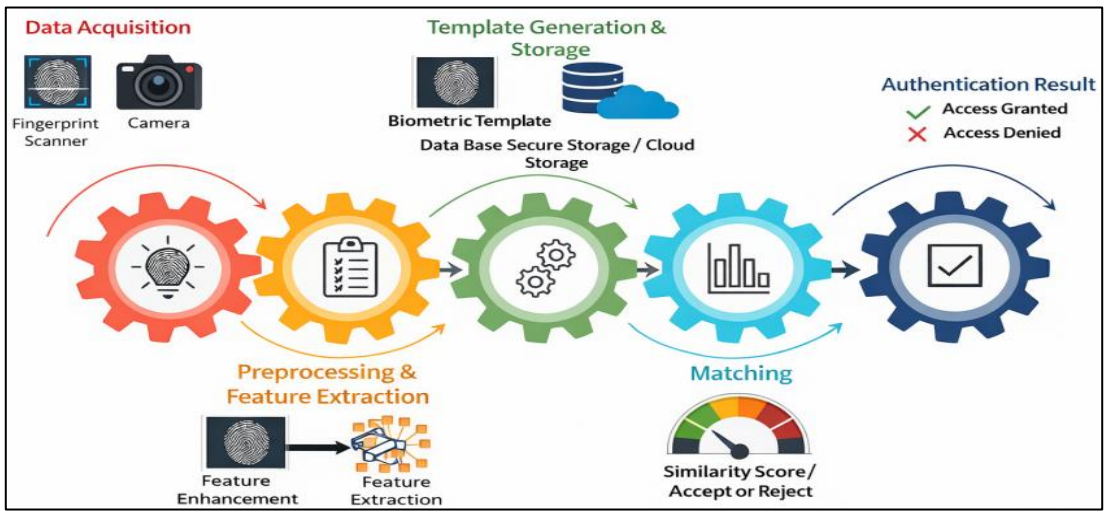

Figure 1. Biometric Authentication System Architecture

3. Security Threats in Biometric systems

Although biometric authentication systems provide a better identity verification method than conventional methods used in authentication, they are vulnerable to numerous security threats in the lifecycle of operation. These risks may be against various components of the systems such as biometric sensors, channels of communication, the storage of templates and decision modules. These vulnerabilities can be used to develop strong and privacy sensitive biometric systems [7].

3.1 Sensor-Level Attacks

One of the most prevalent attacks at the biometric systems is sensor level attacks that are carried out at the stage of acquiring biometric data. These attacks are designed to defraud the sensor providing false or modified biometric characteristics. This can be described as the use of artificial fingerprints, printed facial photos, recordings of voices replayed or contact lenses that are made to replicate the iris patterns. Unless good liveness detection and sensor integrity measures are undertaken, such spoofing attacks can circumvent authentication measures. Bad light, noises or sensor deterioration are additional environmental factors which make biometric sensors susceptible to real world application [8].

3.2 Replay Attacks

Replay attacks are a form of data theft attack whereby a biometric information or feature representations are recorded in an authorized authentication process and then resubmitted to get unauthorized access in future. Injection attacks take the advantage of the weaknesses in the communication channel by directly injecting into the system pipeline pre-recorded biometric signals or feature vectors [9]. Such attacks are very harmful especially in networked biometric systems where data is sent between sensors, processing and servers. The biometric systems are susceptible to these threats unless they are implemented with secure communication protocols and data integrity verification.

3.3 Template Compromise and Database Attacks

Biometric templates that are stored in centralized or distributed databases constitute a high security asset. By accessing such templates without permission, one might end up being an identity thief, inverting templates, or cross-matching between different systems. In comparison to passwords, biometric templates are not easily revoked or replaced, so the security of templates is a significant issue. Sensitive biometric data can be compromised by attackers because of weak access controls, insider threats or database vulnerabilities and the long-term privacy consequences can be experienced by the users [9].

3.4 Matcher and Decision-Level Attacks

Hacking into the matcher or decision-making component is intended to alter similarity measure or authentication parameters. On changing matching scores, attackers would be able to generate false high acceptance rates or induce denial-of-service states. Such attacks can be done by altering the classifier parameters or by hacking decision thresholds, or by using software weaknesses in the matching algorithm. Such threats may compromise the reliability of the system and result in authorization and service interruption.

3.5 Man-in-the-Middle and Communication Attacks

In distributed biometric systems there is normally data transmission between sensors, edge devices and central servers. The man-in-the-middle (MitM) attacks are attacks on biometrics data in transit that allow attackers to intercept, modify, and/or replay authentication messages. Poor encryption, poor key management, or poor network protocols can greatly create the likelihood of communication based attacks.

3.6 Insider Threats

Insider threats involve the trusted employees who abuse their access privileges in order to steal biometric information or disrupt system operations. These are also especially difficult to track down since insiders might be granted access to biometric databases, system configuration, or authentication logs. Unauthorized template modification, data leakage, or system sabotage can be the outcomes of insider attacks, and it is a serious threat to the security and privacy.

3.7 Privacy and Linkability Attacks

Privacy-related attacks involve using biometric information with non-authentication purposes. Linkability attacks enable the attacker to match biometric templates in multiple databases or applications, and track users without their permission. These attacks compromise the privacy of the users and the security of trust in biometric systems particularly at mass scale where there is the use of a number of service providers [10].

This part underscores the fact that biometrics are vulnerable to a wide range of threats that are in the process of acquisition, transmission, storage, and decision-making. To solve these vulnerabilities, it is needed to have an integrated security strategy that involves liveness detection, secure communication, template protection, access control and trust-conscious system design.

4. Privacy Preservation Techniques in robust biometric systems

Although biometric authentication systems offer great assurance of identity, the irrevocability of biometric data is a major cause of concern in terms of privacy. Biometric traits cannot be easily substituted once compromised as compared to passwords or tokens; therefore, privacy preservation is a significant design consideration. The section addresses some of the critical methods that are used in securing biometric information during its lifecycle such as acquisition, storage, transmission and matching [11].

4.1 Protecting Biometric Templates

The protection techniques based on biometric templates are utilized to keep the stored biometric representations safe against hacking. Rather, transformed or protective templates are stored to eliminate inversion of templates and identity theft. The general methods of template protection are:

- Template Encryption: To secure privacy at the time of storage and transmission of biometric templates, cryptographic algorithms are applied to encrypt the templates [12]. The management of keys should be secure so as to avert unauthorized decryption.
- Cancellable Biometrics: Here, deliberate, non-invertible manipulations on biometric templates are used. In the case that a template is compromised, then it can be revoked and a reconstruction of it can be performed by applying an alternate transformation, which is like resetting a password [13].

- Biometric Hashing: Secure hashing functions transform the length of feature vectors to hash representations of fixed length. This approach prevents privacy invasion at the expense of similar accuracy because of sensitivity to within-class variations.

4.2 Secure Biometric Transmission of Data

Biometric systems are frequently deployed in distributed contexts whereby data is sent across sensors, processing devices and servers. Secure communication protocols will be required to avoid eavesdropping, re-play attacks and manipulation of data. There are encryption protocols like Transport Layer Security (TLS) and secure key exchange protocols that guarantee data confidentiality and data integrity over the network [14]. Also, the system components mutually authenticate, which also minimizes the risk of unlawful access.

4.3 Cryptographic Privacy-Preserving Methodology

There have been advanced cryptography methods that have been pursued to make biometric operations possible without the need to expose sensitive data.

4.3.1 Homomorphic Encryption

Homomorphic encryption enables calculation of the encrypted biometric data and thus the matching of the encrypted biometric data can be done privately without disclosing the templates. The technique has a high privacy guarantee and it is mostly handy in bypassed or clouded biometric systems [15]. Nonetheless, the computational complexity and a higher latency of homomorphic encryption are too high to make it practical in real-time and resource-intensive applications.

4.3.2. Secure Multi-Party Computation

Secure multi-party computation allows two or more parties to combine their efforts to execute a biometric matching/verification without sharing their personal inputs with each other. This technique works in the distributed setting, whereby trust between entities is minimal [16]. Secure multi-party computation can be costly with a substantial overhead in communication and implementation despite its high level of privacy protection.

4.4 Decentralized and On-Device Storage

In order to curb such risks posed by centralized biometric databases, there has been an interest in decentralized storage methods. Local storage Local biometric templates are stored in user devices or secure hardware modules, including trusted execution environments (TEEs) or secure elements, in such systems [17]. On-device storage eliminates the mass-breach of data and improves user's control of biometric data [18].

4.5 Access Control and Audit Authority

Access control policies are very rigid in order to restrict access by persons to biometric information and system configurations. Role-based access control (RBAC) along with audit logging and audit monitoring assists in identifying the presence of unauthorized access and insider threats. Accountability and compliance with the data protection regulations are also facilitated by audit trails [19].

4.6 Regulatory and Ethical Reconsiderations

The biometric systems should also observe the legal and ethical standards of privacy preservation. Laws like data protection act focus on principle like user consent, minimization of data, limit purpose and transparency. When these are implemented in the system design, it improves the user confidence and promotes responsible biometric implementation [20].

4.7 Strengths and Weaknesses of Existing Techniques

The currently used methods of privacy preservation offer inconsistent levels of security against data theft involving biometrics. The mechanisms of template protection are revocable and simple and can potentially affect recognition performance. Cryptographic solutions provide high-security levels of privacy, but at a high price of overloading computation and communication costs. Privacy-conscious machine learning methods open up opportunities of decentralized and trust-oriented systems but are still quite young and need additional standardization [21]. In general, none of the privacy preservation techniques meets the security, privacy, usability and-scalability needs to the full extent. This constraint makes it clear that it needs to be analysed in structured forms and combined solutions, which are further discussed in the scope of comparative analysis and threat-to-solution maps in the following section.

5. Threats-to-solution mapping of privacy mitigation techniques

A systematic mapping of threats-solution allows a better insight into how current privacy preservation methods deal with particular threats to security in biometric systems [22]. Modifications at the sensor level, including spoofing attacks and presentation attacks are usually addressed through the liveness mechanisms of detection and the multimodal authentication. Threats at the communication level such as replay attacks, man-in-the-middle attacks are handled by the implementation of secure transmission protocols and encryption.

The cancellable biometrics, biometric cryptosystems, and secure template storage mechanisms are the most common mechanisms used in mitigating template-level threats like template inversion, cross-matching and database leakage [23]. Threats at the system level such as insider threats, unauthorized access need strong access control policies, audit mechanisms and decentralized storage methods. Additional cryptographic techniques like homomorphic encryption and secure multi-party computation are even more beneficial in improving privacy since they allow a secure matching process without disclosing the raw biometric information [24]. The analysis of this mapping is that proper protection of privacy can only be done through a layered approach that is a combination of many measures and not a mono solution. Figure 2 is a heat map that represents the level of privacy risk in the various layers of the biometric authentication systems. The heat map classifies threats as low-risk, medium-risk and high-risk depending on the extent to which they may affect user privacy, data irreversibility and widespread misuse.

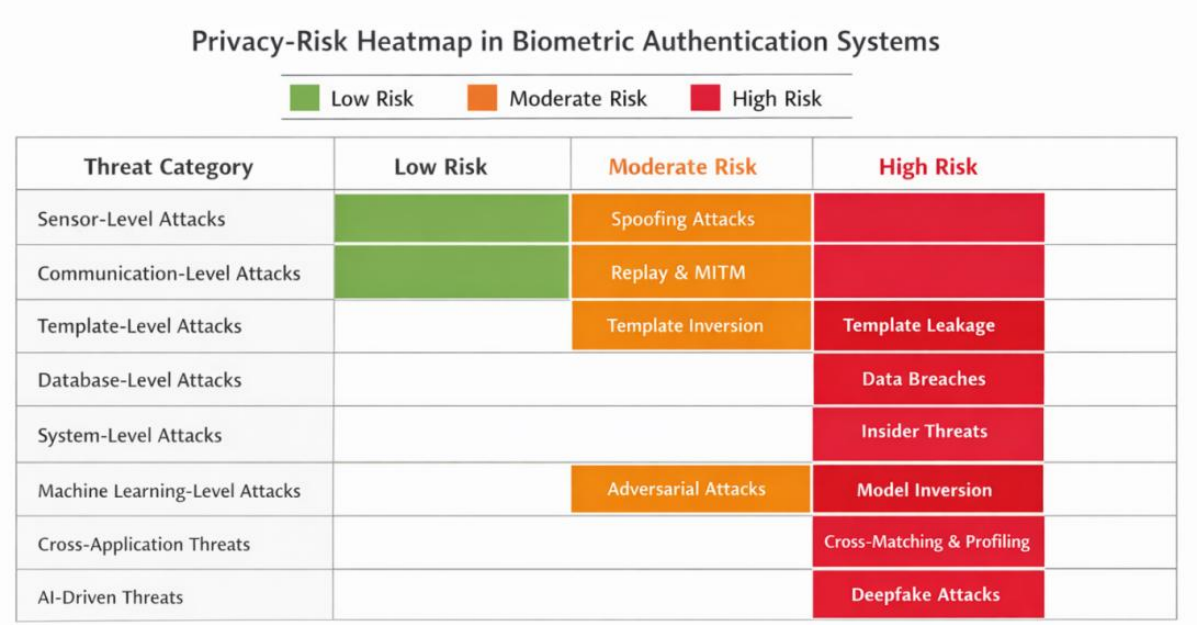

Figure 2. Privacy-risk heat map in Biometric Authentication Systems

Table 2 has provided a systematic mapping of typical security threats of biometric authentication systems and privacy-protective weakness mitigation strategies. The discussion indicates that the majority of effective defences are based on a layered combination of cryptographic, system-level and machine learning-based solutions, as opposed to individual ones.

6. Conclusion and Future Scope

This paper has introduced a threat based survey of biometric authentication system with significant consideration of privacy protection. The study has identified the strengths and weakness of the existing methods by examining biometric modalities, security threats, and maximum privacy preserving methods. Threat-to-solution mapping and privacy-risk heat map is in place to identify the critical weaknesses and gaps in research. The results indicate that successful biometric authentication will entail a concerted and layered model which will all address security, privacy, scalability and confidence. The knowledge and research avenues presented in this work will inform future research of creating secure, privacy-yielding, and trustful biometric authentication systems applicable to large-scale and networked setups. Future studies must be aimed at creating trust-based biometric models where privacy protection becomes the design principle instead of a feature. It involves the incorporation of cancellable biometrics, cryptographic protection and privacy conscious machine learning into unified architectures that are security conscious, performance conscious and usability conscious. Decentralized and user-controlled biometric

systems with the help of technologies like federated learning and edge computing are becoming a good direction in order to decrease centralized data exposure. Moreover, the adaptive and multimodal biometric systems also require further understanding to increase resilience to adaptable attack vectors, as well as reliability. Privacy evaluation metrics and frameworks also need to be standardized so that privacy preserving methods can be compared uniformly. There should also be research aimed at explaining and transparent biometric which will be more acceptable to users and meet regulatory standards. The problem of solving AI-based spoofing attacks with the help of a strong liveness detection and cross-modal verification is a valuable field of further investigation.

Table 2. Threat-to-Solution Mapping in Biometric Authentication Systems

Threat Category	Specific Threats	Security & Privacy Impact	Privacy-Preserving Solutions	Trade-offs
Sensor-Level Attacks	Presentation attacks (spoofing), fake biometric traits, sensor tampering	Unauthorized access, identity impersonation, trust degradation	Liveness detection, challenge–response mechanisms, multimodal biometrics	Increased hardware cost, user inconvenience, partial spoof resistance
Communication-Level Attacks	Replay attacks, man-in-the-middle (MITM), eavesdropping	Biometric data leakage, session hijacking	Secure channels (TLS), encryption, secure key exchange protocols [28]	Computational overhead, latency in real-time systems
Template-Level Attacks	Template inversion, template reconstruction, cross-matching [27]	Permanent privacy breach, identity misuse across databases	Cancellable biometrics, biometric cryptosystems, secure hashing	Accuracy degradation, revocation complexity
Database-Level Attacks	Database leakage, insider misuse, unauthorized access	Mass biometric compromise, loss of user trust	Encrypted template storage, access control, decentralized storage [29]	Storage overhead, system complexity
System-Level Attacks	Trojan horse, backdoor attacks, privilege escalation	System manipulation, covert data exfiltration	Trusted execution environments (TEE), secure system design	Platform dependency, limited scalability
Machine Learning-Level Attacks	Adversarial examples, model inversion, membership inference	Privacy leakage, reduced system robustness	Privacy-aware ML, federated learning, differential privacy [25]	Reduced model accuracy, complex training
Cross-Application Threats	Cross-database matching, profiling, surveillance misuse	Loss of anonymity, function creep	Cancellable templates, policy-driven access control	Requires strong governance and regulation
Emerging AI-Driven Threats	Deepfake attacks, synthetic biometric generation [26]	High-fidelity spoofing, large-scale impersonation	Multimodal fusion, AI-based liveness detection	Arms-race with attackers, training data bias

References

1. Jain, A. K., Ross, A., & Nandakumar, K. (2023). Introduction to biometrics and security trends: 2023 update. *IEEE Transactions on Biometrics, Behavior, and Identity Science, 5*(2), 123–145.
2. Alrawili, R., AlQahtani, A. A. S., & Khan, M. K. (2023). A comprehensive survey on biometric authentication systems: Security and privacy issues. *Computers & Electrical Engineering, 104*.
3. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*.
4. Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. *EURASIP Journal on Advances in Signal Processing*.
5. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition* (2nd ed.). Springer.
6. Kumar, S. . (2023). Qualitative Analysis of Religious Drama in Hindi Cinema: A Study of Movie "Dharam Sankat Mein". *MediaSpace: DME Media Journal of Communication*, *4*(01), 11–16. https://doi.org/10.53361/dmejc.v4i01.02
7. Li, S. Z., & Jain, A. K. (Eds.). (2011). *Handbook of face recognition* (2nd ed.). Springer.
8. Chingovska, I., Anjos, A., & Marcel, S. (2022). On the effectiveness of local binary patterns in face anti-spoofing. In *Proceedings of IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*.
9. Akhtar, Z., & Marcialis, G. L. (2022). Biometric system security: Attacks and countermeasures in the deep learning era. *IEEE Access, 10*, 98765–98790.
10. Wang, Y., Li, Q., & Xu, W. (2023). Adversarial attacks on deep biometric systems: A review. *IEEE Access, 11*, 45678–45701.
11. Rane, S., Wang, Y., Draper, S. C., & Ishwar, P. (2022). Secure biometrics: Concepts, authentication architectures, and challenges. *IEEE Signal Processing Magazine, 39*(5), 51–64.
12. Fierrez, J., Morales, A., Vera-Rodriguez, R., & Camacho, D. (2018). Multiple classifiers in biometrics. Part 2: Trends and challenges. *Information Fusion, 44*, 103–120.
13. Teoh, A. B. J., Ngo, D. C. L., & Goh, A. (2006). Biohashing: Two-factor authentication featuring
14. Kumar, S. ., & Hooda, S. (2023). An Analytical Review of Political Communication in India with Special Reference to the Social Media. *MediaSpace: DME Media Journal of Communication*, *3*(01), 8–15. https://doi.org/10.53361/dmejc.v3i01.02
15. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2023). Cancelable biometrics: Concepts and recent advances. *IEEE Transactions on Information Forensics and Security, 18*, 1123–1137.
16. Nandakumar, K., & Jain, A. K. (2022). Biometric cryptosystems: A review of recent advances. *IEEE Signal Processing Magazine, 39*(5), 52–63.
17. Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2022). Homomorphic encryption for arithmetic of approximate numbers. In *Advances in Cryptology – ASIACRYPT*.
18. Yao, A. C. (2022). Protocols for secure computations: Modern perspectives. In *Proceedings of Foundations of Computer Science*.
19. Kumar, S., & Hooda, S. . (2023). Healthcare and Hospital Promotions and Audience Reception. *MediaSpace: DME Media Journal of Communication*, *3*(01), 16–19. https://doi.org/10.53361/dmejc.v3i01.03

20. Deng, Y., Ren, Z., & Shan, S. (2025). Privacy-aware face recognition via adversarial learning. *IEEE Transactions on Pattern Analysis and Machine Intelligence* (Early access).
21. Ratha, S., & Patel, V. M. (2024). Next-generation biometric security: Trustworthy and explainable AI. *IEEE Security & Privacy, 22*(1), 45–53.
22. Deng, Y., Ren, Z., & Shan, S. (2025). Privacy-aware face recognition via adversarial learning. *IEEE Transactions on Pattern Analysis and Machine Intelligence* (Early access).
23. Chamikara, M. A. P., et al. (2020). Privacy-preserving face recognition using differential privacy.
24. Kumar, S., & Singh, P. (2023). Emotional Appeal in the Tweets: A Study on Indian National Political Parties. *Journal of Communication and Management*, *2*(02), 95–97. https://doi.org/10.58966/JCM2023223
25. Drozdowski, P., Stockhardt, F., Rathgeb, C., et al. (2021). Feature fusion methods for privacy-preserving biometric retrieval.
26. Gomez-Barrero, M., Rathgeb, C., & Busch, C. (2022). General framework for biometric template protection. *IEEE Transactions on Information Forensics and Security, 17*, 1234–1248.
27. Maiorana, E., Campisi, P., & Fierrez, J. (2023). Privacy protection in biometric systems: A structured overview. *IEEE Signal Processing Magazine, 40*(3), 97–109.
28. International Organization for Standardization. (2022). *ISO/IEC 24745: Information technology—Security techniques—Biometric information protection*.
29. Dr. Sudhir Kumar. Feminism in Indian Cinema: A Study of Characters in Kiran Rao's Laapataa Ladies. International Journal of Contemporary Research in Multidisciplinary. 2024: 3(6):206-209. https://doi.org/10.5281/zenodo.14939103
30. Liu, X., Feng, J., & Zhao, H. (2024). Deep privacy-preserving biometric recognition using transformers. *IEEE Transactions on Biometrics, Behavior, and Identity Science*
31. Deng, Y., Ren, Z., & Shan, S. (2025). Privacy-aware face recognition via adversarial learning. *IEEE Transactions on Pattern Analysis and Machine Intelligence* (Early access).
32. Ratha, S., & Patel, V. M. (2024). Next-generation biometric security: Trustworthy and explainable AI. *IEEE Security & Privacy, 22*(1), 45–53.
33. Yang, W., Wang, S., Cui, H., Tang, Z., & Li, Y. (2023). A review of homomorphic encryption for privacy-preserving biometrics. *Sensors, 23*(7).
34. Kumar, S., & Singh, P. (2023). Emotional Appeal in the Tweets: A Study on Indian National Political Parties. *Journal of Communication and Management*, *2*(02), 95–97. https://doi.org/10.58966/JCM2023223
35. Sharma, S., Mudgil, A., Dubey, R., et al. (2026). A bibliometric analysis of homomorphic encryption for privacy-preserving biometrics. *Computers & Electrical Engineering*.