A ES
ISSN: 2096-3246
Volume 58, Issue 02, June, 2026

BIOMETRIC AUTHENTICATION USING GENERATIVE AI TECHNIQUES

Shanthi Pannala,
Research Scholar, Department of CSE, JNTUH, Hyderabad, Telangana,India. Mail-ID: Shanthi.pannala@gmail.com
Dr. B. Sateesh Kumar,
Professor, Department of CSE, JNTUH College of Engineering, Jagtial, Telangana, India. Mail-ID: sateeshbkumar@jntuh.ac.in

Abstract
Biometric authentication systems have become essential in modern security applications due to their ability to provide reliable and user-specific identification using physiological and behavioral traits such as face, fingerprint, iris, palmprint, voice, and vein patterns. Recently, generative artificial intelligence (AI) techniques, particularly Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), diffusion models, and transformer-based architectures, have significantly transformed biometric authentication by improving biometric data synthesis, spoof detection, privacy preservation, and multimodal authentication. This survey presents a comprehensive review of generative AI techniques applied in biometric authentication systems, covering major research areas including biometric data augmentation, deepfake detection, privacy-preserving authentication, multimodal biometric fusion, liveness detection, and anti-spoofing mechanisms. The survey is from 2020-2026.The study analyzes recent advancements in GAN-based synthetic biometric generation, adversarial attack detection, explainable AI integration, blockchain-enabled privacy protection, and quantum-resistant biometric frameworks. Furthermore, a detailed classification framework and comparative literature analysis are presented to identify current methodologies, datasets, algorithms, strengths, and limitations of existing approaches. The survey also highlights critical research gaps related to scalability, cross-database generalization, adversarial robustness, computational complexity, explainability, and real-time deployment challenges. Finally, future research directions are discussed, emphasizing the development of secure, lightweight, privacy-aware, and robust generative AI-driven biometric authentication systems for next-generation intelligent security applications.

1.Introduction

Biometric authentication has emerged as one of the most reliable approaches for identity verification in modern digital environments. Biometric systems offer robust security, convenience and protection against traditional attacks using credentials, with unique physiological and behavioural attributes like facial features, iris patterns, fingerprints, voice signals and vein patterns. As a result, these technologies are already in use at banks, in healthcare, border control, smart devices and in digital identities. While there are pros to biometric authentication systems, they still have many challenges to overcome, such as the ability to manufacture presentation attacks, generate deepfakes, create synthetic identity, leak privacy, and manipulate an individual. These threats can influence the accuracy of the authentication and erode the trust of users in the biometric security infrastructure. With the advent of new generative AI technologies, new solutions to these challenges have emerged. Generative models, and specifically Generative Adversarial Networks (GANs), have shown to be very successful in the generation of biometric data, the protection of privacy, the prevention of spoofering and the enhancement of recognition. By generating realistic biometric samples and improving feature learning processes, these models contribute to more robust and scalable authentication systems. Significant progress has been reported in face spoof detection, facial anti-spoofing, privacy-preserving biometric authentication, synthetic voice attack detection, and realistic iris image generation through the application of GAN-based architectures and domain generalization techniques (Ge et al. 2024) (Mjachky and Homoliak 2025) (Li et al.

2024). Furthermore, advanced approaches have enabled the generation of high-quality synthetic iris images while preserving distinctive biometric characteristics, thereby supporting secure data augmentation and recognition performance improvements (Kordas et al. 2024) (Yadav and Ross 2023). These developments highlight the growing role of generative AI in strengthening biometric authentication, improving privacy protection, enhancing data availability, and increasing resistance against sophisticated spoofing attacks.

2. Background and Foundations

Biometric recognition systems have gained considerable capability with the development of deep learning and generative artificial intelligence. Deep neural networks allow for automatic extraction of features from complex biometric patterns and generative models can help to generate realistic synthetic biometric samples that enhance model training and generalization. The advent of recent models, such as GANs, VAEs, diffusion models, and transformer-based architectures, has paved the way for groundbreaking advancements in biometric data synthesis, augmentation, privacy protection, and spoof detection. Recent developments have seen the emergence of models like GANs, VAEs, diffusion models, and transformer-based architectures, which have enabled significant progress in biometric data synthesis, augmentation, privacy protection, and spoof detection. To overcome this, synthetic sample generation has been used for vein recognition systems (VRS) to create more training data, and the integration of GAN-based data generation and transfer learning (TL) has improved recognition performance in finger vein biometrics (Mathew and Amudha 2024) (Qin et al. 2023).

Likewise, hybrid feature engineering and self-learning have enhanced the scalability and resilience of iris recognition systems (Kavitha, Sankari, and Shalini 2024) with the help of generative AI. With the advent of voice replay attacks and AI-generated deep fake speech, there has been a growing need for more secure voice authentication systems (Kamel et al. 2025). Moreover, the development of self-supervised transformer architectures has improved anti-spoofing and liveness detection of faces by learning from discriminative facial representations that require fewer labeled datasets, which in turn improves the accuracy of facial anti-spoofing and liveness detection (Keresh and Shamoi 2024). In addition, deep learning methods have shown promising results in hand vein biometric recognition, enhancing the system's reliability and security across various operational conditions (Simaiya et al. 2026). The progress of these technologies collectively creates the groundwork for next-generation biometric authentication systems, combining generative AI, comprehensive security measures, and smart identity verification capabilities.

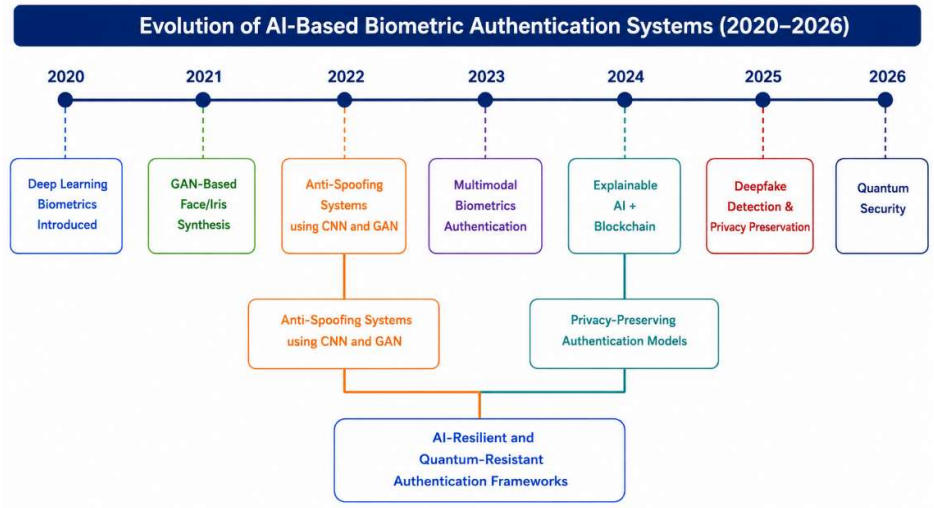

Figure.1 Evolution of AI-Based Biometric Authentication Systems

Figure.1 represents the time-dependent development trend of biometric authentication systems using artificial intelligence from the year 2020 up to 2026, demonstrating important technological progress in biometric authentication security. In 2020, deep learning algorithms were developed to enhance the accuracy of biometric authentication. In 2021, GANs used to synthesize faces and irises came into practice to facilitate biometric data generation and improvement. Anti-spoofing methods using CNN and GAN models were developed to detect fakes based on the biometric authentication data in 2022. Multimodal biometric authentication combining various types of biometric features like face, fingerprint, and voice was proposed in 2023. During 2024, explainable AI technology combined with blockchain technology was implemented to make the process more transparent and trustful. Deepfake detection and privacy preserving authentication models became an important research issue in 2025. Finally, in 2026, there will be a shift towards developing AI and quantum resistant biometric authentication systems that will be capable of standing up against sophisticated cyber threats and attacks in the post-quantum world.

3. Classification Framework:

The proposed taxonomy framework is structured in accordance with the biometric modality, AI architecture, use case, attack types, and learning paradigm. The taxonomy comprises biometric modalities like facial images, fingerprints, irises, palm prints, and vasculatures wherein the use of generative AI models is applied to perform biometric authentication and spoofing attacks. The AI techniques included in the taxonomy framework comprise GAN, DCGAN, StyleGAN, and VAE, which are employed in biometrics to create synthetic faces or other biometrics for anti-spoofing purposes. Other categories in the framework include anti-spoofing, data augmentation, synthetic biometrics creation, privacy-preserving biometrics, and PAD attacks.

3.1 Generative AI for Biometric Data Synthesis & Augmentation

The concept of generative AL has gained prominence as a revolutionary way of dealing with issues of data insufficiency and inconsistencies within biometric authentication schemes. Under this approach, ML algorithms like GANs, VAEs, and diffusion methods are used extensively in generating realistic features of biometrics such as fingerprint, facial image, iris scan, and voice samples. While such techniques offer significant potential for overcoming data insufficiencies and inconsistency problems, several issues arise when trying to ensure that generated data are representative and not susceptible to being spoofed or faked. As a result, recent research emphasizes the need for balance between data generation and security.

Mustafa et al. (2023) explore the use of generative models for fingerprint generation and authentication in biometrics in order to overcome issues related to data scarcity and privacy in the field. The paper suggests a framework based on an adaptive deep convolutional GAN trained on the Socofing database, which not only generates realistic fingerprints but also enables authentication tasks. The framework takes advantage of feature learning using GANs, improving the quality of representations and matching performance. An accuracy rate of 92% shows the success of the suggested method in biometric authentication. Nevertheless, the study may be constrained by possible synthetic artifacts and does not consider cross-database generalization and spoofing attacks.

Raouf et al. (2024) have introduced a more effective user authentication system by using keystroke dynamics, thereby offering protection from any potential imposter attack. In the process, they make use of Quantile transformation as a technique for handling outliers in their analysis, while Conditional Tabular Generative Adversarial Networks (CTGAN) is used to augment their data. Multiple Transfer Learning Models like VGG19, ResNet50, and EfficientNetB0 have been used to extract the features of the data sets, whereas LIME is employed as a method for making Explainable Artificial Intelligence. Their experimental analysis using CMU benchmark data set proves that their approach outperforms current

approaches.

Rao et al. (2024) investigate the escalating problem of face spoofing attacks on biometric authentication systems by introducing a model based on DCGAN for improving spoofing detection accuracy. In their study, they implement Deep Convolutional Generative Adversarial Networks in order to create virtual facial images to increase the training data set. The discriminator part of the model is able to efficiently differentiate between true and fake images through adversarial training. Evaluation conducted on CelebA dataset shows very high accuracy with 99.1%, which is superior to other methods. But the method heavily depends on the properties of the data set and cannot be validated elsewhere.

Natarajan et al. (2025) design a multi-modal behavioral biometric authentication system that can overcome limitations related to privacy, scalability, and data availability in continuous authentication systems. Natarajan et al. (2025) present a hybrid generative adversarial network–variational autoencoder (GAN-VAE) architecture for generating artificial datasets using formal differential privacy constraints (ε=1.0, δ=10^{-5}). This method preserves the correlation between different types of behaviors through nine behavioral attributes. Researchers have applied several models like CNN, LSTM, and hybrid CNN-LSTM. Among all these models, the hybrid model provides the best average accuracy of 96.04%, and its maximum value is 99.12%. The proposed model achieves a 5.47% improvement in performance compared to existing benchmarks and 75% reduction in enrollment data.

Chowdhury et al. (2024) investigate the application of generative models in synthesizing palmprint biometric information without contact. The authors utilize sophisticated StyleGAN frameworks to train models based on H-PolyU and IIDT databases to synthesize 4,839 palmprint images. The uniqueness features are assessed through SIFT, with the palm region achieving 16.12% similarity score and the finger region scoring 17.85%, with the model achieving FID of 16.1. This study proves that StyleGAN is effective in biometric generation. Nevertheless, the authors fail to assess its performance in practical authentication applications.

Pushpakumar (2022) presents a combined technique for behavioral biometrics authentication that is designed to address the shortcomings of existing methods regarding capturing dynamic interaction behavior of the users. This includes integrating VAEs for representation of hidden features and GNN modeling of the relationships between different behavioral signals such as typing patterns and gestures, and optimizing the technique using Ant Colony Optimization (ACO). Results show a performance improvement of 15–20% as well as decreased false acceptance and rejection rates of the proposed technique compared to traditional approaches. Still, there are no studies conducted on a large real dataset.

Farooq et al. (2023) introduce the ChildGAN model, which is based on StyleGAN2, and uses domain adaptation techniques to generate huge databases of child faces. The research focuses on overcoming the issue of limited availability of child facial images and their ethical collection problems by creating realistic images that contain controlled changes in expressions, poses, lightings, and demographic factors. The proposed model generates more than 300,000 samples and evaluates their realism with the help of CNN-based gender recognition, face landmarks recognition, ArcFace identity similarity, and eye aspect ratio analysis. It provides high-quality synthetic data useful for various computer vision applications, but the performance of the method is not evaluated in biometric authentication and spoofing cases. The summary of Generative AI for Biometric Data Synthesis & Augmentation shown in Table.1

Table.1 Generative AI for Biometric Data Synthesis & Augmentation

S.No	Paper	Dataset Used	Key Attributes / Features	Algorithms / Models	Methodology Used	Limitations
1	Mustafa et al. (2023)	SOCOFing	Fingerprint ridge	Adaptive DCGAN	GAN-based fingerprint	Synthetic artifacts, no

			patterns, synthetic biometric features		generation and authentication using feature learning	cross-database validation, no spoofing analysis
2	Raouf et al. (2024)	CMU Keystroke Dataset	Keystroke timing, typing behavior	CTGAN, VGG19, ResNet50, EfficientNetB0, LIME	Quantile transformation, data augmentation using CTGAN, transfer learning for authentication	Limited generalization, dependence on benchmark dataset
3	Rao et al. (2024)	CelebA	Facial biometric features, spoofing patterns	DCGAN	Synthetic face generation and spoof detection using adversarial learning	Dataset dependency, lack of external validation
5	Natarajan et al. (2025)	Synthetic behavioral biometric dataset	Nine behavioral biometric attributes	GAN-VAE, CNN, LSTM, CNN-LSTM	Differential privacy-based synthetic data generation and hybrid authentication	Limited real-world deployment validation
6	Chowdhury et al. (2024)	H-PolyU, IIDT	Palmprint texture, finger region features	StyleGAN, SIFT	Synthetic palmprint generation and uniqueness analysis	No practical authentication evaluation
7	Pushpakumar (2022)	Behavioral biometric datasets	Typing patterns, gestures, interaction graphs	VAE, GNN, ACO	Feature extraction using VAE and graph modeling with optimization	No large-scale dataset validation
8	Farooq et al. (2023)	Child face datasets	Facial expressions, pose, lighting,	StyleGAN2, ArcFace	Child face synthesis with domain adaptation	No biometric authenticati

			demographics			on evaluation

3.2 Deepfake Attacks & Threats in Biometric Authentication

The rapid development of generative ALhas contributed immensely towards making deepfake attacks more advanced, hence presenting great risks for biometric authentication systems. The advanced nature of deepfake attacks is attributed to the application of techniques involving deep neural network architectures like generative adversarial networks (GAN) and diffusion networks that can create realistic artificial characteristics for face, voice, and behavior. The risks posed by such deepfakes make traditional methods of authentication vulnerable to attacks since they are designed to detect natural characteristics. Recently, several studies have been conducted concerning deepfake detection techniques, mainly involving robust feature learning and liveness detection.

He et al. (2025) explores the evolving problem of attacks via deepfakes enabled by AI generation techniques on biometric authentication, with the intention of narrowing the gap between expert knowledge and public perceptions. The research uses a mixed-methods design that features the completion of a survey questionnaire involving 408 participants and an interview involving 37 participants. Specifically, a new Deepfake Kill Chain model is formulated by the researchers to evaluate attack strategies, and they further put forward a multi-layered strategy for mitigation, with an emphasis on dynamic biometrics and data governance. The research finds substantial differences in terms of awareness and trust among the experts.

Khan & Khan (2025) examine the new threat from deepfake attacks on biometric authentication mechanisms that use generative models of AI such as GANs and VAEs. The objective is to review the existing mechanisms for detecting deepfake attacks and identifying weaknesses in these mechanisms as a result of growing realism in artificial identities created using such approaches, including cross-modal attacks. Nevertheless, while discussing different methods and their effectiveness, the authors point to the necessity of implementing more advanced methods of protecting privacy and applying multiple layers of security in order to combat these threats.

Pakina et al. (2023) investigate the increasing danger of AI-generated synthetic identities in FinTech, specifically attacks on KYC/AML frameworks using deepfakes to perform fraud. This paper presents a behavioral biometrics-based identification scheme by leveraging a variety of multimodal traits, which include keystroke timing, mouse behavior, speech characteristics, and facial micro expressions. Machine-learning-based detection models along with temporal modeling techniques are used to classify authentic user behavior versus fake ones in a live environment. Results on a simulated set of data show an extremely high detection rate of 98.7% while outperforming existing verification approaches. Nevertheless, this research is based on synthetic data and needs validation using practical banking datasets.

Zen et al. (2025) discuss the problem of identifying deepfakes in biometric authentication applications, specifically in terms of generalization. They present an ensemble method that uses multiple DL-based classifiers to identify a wide range of deepfake attacks on the biometric system. In addition to individual classifier performance comparison, the findings show increased accuracy of detecting deepfakes in terms of identification deception and identity fraud through a more consistent performance pattern. In the findings, it is shown that the ensemble model has a strong detection capability across multiple deepfake data sources. On the other hand, the work does not provide specific evaluation parameters.

Park et al. (2024) present a complete risk analysis scheme designed to analyze adversarial attacks on biometric authentication schemes that employ DL technologies. This research is intended to address deficiencies in previous work related to module-specific or attack-specific analysis approaches. In the proposed approach, adversarial attacks are simulated within

interconnected system components, determining which surfaces are weak and how modules are dependent on each other – such as modules responsible for liveness detection or identity verification. The authors developed evaluation criteria to determine risks related to security vulnerabilities, testing their approach via a practical example involving face recognition. Nevertheless, the proposed study does not deal with defensive measures against adversarial attacks and lacks benchmarking.

Alghamdi et al. (2024) study the susceptibility of multimodal biometric systems for authentication purposes to the impact of adversarial attacks with the aim of determining the optimal fusion mechanism. The research considers input level fusion, feature level fusion, and score level fusion in combination with FGSM technique to produce adversarial perturbation within behavioral and physiological biometric modalities. Accuracy, precision, recall, and attack success rate performance measures have been used in the evaluation of adversarial attacks. The findings revealed that input level fusion is more secure with low attack success rate of 16.62% and 32.30% in DenseNet201 and Arc Face respectively.

Dudykevych et al. (2024) suggest the design of an artificial neural network framework to identify the modification of deepfakes in biometric images for improving information system security. This research paper presents a module-based detection model designed through various processing levels such as pre-processing, feature extraction, and classifier training, which are incorporated into the multi-level security framework that includes assets, information systems, and processes. The proposed model uses the concept of neural network analysis and decision support systems to detect and classify modified facial biometric images. This research model proves to be effective in enhancing the performance of detection and classification.

Tak et al. (2022) analyze the problem of deepfake and spoofing detection in ASV applications with the help of self-supervised learning through a wav2vec 2.0-based architecture. This research seeks to enhance the generalization capability of ASV algorithms in situations where training data is restricted and not representative of real-life spoofing attempts. This work uses a wav2vec 2.0 pre-trained front-end with fine-tuning that has been first trained on bona fide voice samples without any inclusion of spoofing attacks. The system was further improved through data augmentation techniques. State-of-the-art results were obtained on ASVspoof 2021 Logical Access and Deepfake databases, with an increase of almost 90% over the baselines. Nevertheless, the solution is still mainly oriented towards audio inputs. Summary of Deepfake Attacks & Threats in Biometric Authentication shown in Table.2

Table.2 Summary Of Deepfake Attacks & Threats in Biometric Authentication

S.No	Paper	Dataset Used	Key Attributes / Features	Algorithms / Models	Methodology Used	Limitations
9	He et al. (2025)	Survey data (408 participants), interviews	User trust, awareness, attack strategies	Deepfake Kill Chain Model	Mixed-method analysis and multi-layered mitigation framework	No implementation framework
10	Khan & Khan (2025)	Review-based	Deepfake characteristics, cross-modal attacks	GANs, VAEs	Review of deepfake detection and privacy-preserving strategies	No experimental validation

11	Pakina et al. (2023)	Simulated multimodal dataset	Keystroke timing, speech, mouse movement, micro-expressions	ML classifiers, temporal models	Behavioral biometric-based fraud detection	Requires real banking dataset validation
12	Zen et al. (2025)	Multiple deepfake datasets	Deepfake visual features	Ensemble DL classifiers	Ensemble-based deepfake detection framework	Missing detailed evaluation metrics
13	Park et al. (2024)	Face recognition attack simulations	Adversarial vulnerability metrics	DL adversarial analysis models	Risk assessment of interconnected biometric modules	No defense mechanisms proposed
14	Alghamdi et al. (2024)	Multimodal biometric dataset	Physiological and behavioral modalities	DenseNet201, ArcFace, FGSM	Fusion-based adversarial attack analysis	Limited real-world robustness testing
15	Dudykevych et al. (2024)	Facial biometric datasets	Image manipulation patterns	ANN, Decision Support Systems	Multi-level deepfake detection architecture	No benchmark comparison
16	Tak et al. (2022)	ASVspoof 2021, Deepfake DB	Audio spoofing features	wav2vec 2.0	Self-supervised anti-spoofing learning	Restricted to audio modality

3.3 Privacy-Preserving Biometric Authentication using Generative AI

Biometric authentication techniques have received much interest due to the implementation of generative AL algorithms in order to solve security and confidentiality issues. The conventional technique for biometric authentication involves storing sensitive data, which makes them susceptible to breach and exploitation. However, generative models like Generative Adversarial Networks (GANs) and Variational Auto-encoders (VAEs) provide methods for generating biometric data that contain discriminative traits while masking identities. Generative models contribute to secure data exchange, federated learning, and differential privacy algorithms. Current literature has focused on finding the right trade-offs between authentication efficiency and privacy.

Ghani et al. (2024) suggest a decentralized system of face recognition that improves privacy and security in biometrics-based systems. This study presents a blockchain-enabled system whereby facial attributes are divided and dispersed among different nodes in the network and GANs are used to obfuscate data to safeguard biometric information. The encrypted data is stored on the blockchain, which ensures authenticity and makes the system immutable. A test was conducted on the CelebA database, which showed a precision rate of 99.80%, surpassing other models currently available. Nonetheless, the model requires considerable computing and

memory resources.

Byeon et al. (2024) suggest a DL approach using AI that enables multimodal biometrics authentication to increase accuracy and generalize beyond a unimodal framework. This research employs both pixel-level, feature-level, and score-level fusion techniques under one single deep neural network design. Simulated multimodal data set is generated for assessment purposes. Feature level fusion increases accuracy by 2.2% and score-level fusion generates highly accurate retrievals up to 99.6%. Enhanced accuracy and robustness were observed in this approach towards identity verification. On the other hand, limitations include the lack of real data sets for training and testing purposes, and absence of privacy protection measures in the model.

Brown et al. (2020) develop a multimodal biometric authentication framework to improve the performance of user identity verification by combining various biometric features, namely fingerprints, facial recognition, age, and gender, along with a supervised ML technique based on the Decision Tree algorithm to make predictions on verification outcomes and obtain a score that represents confidence levels. Blockchain technology is also employed to provide accountability and ensure data integrity. Although experiments show enhanced robustness and accuracy than those from unimodal authentication methods, the scheme entails high system complexity, demands the use of multiple biometric characteristics, and lacks testing using large-scale data and sophisticated adversarial environments like deepfakes.

Mehar (2022) examines the use of generative AL in securing cloud-based systems involved in video and media processing operations. In particular, the objective of the paper is to utilize the power of AI to protect against the emergence of new threats, including deepfakes, piracy, and cyber-attacks leading to data leakage. Generative AI is employed for threat intelligence prediction, behavioral analysis, anomaly detection, and improving the security of biometric authentication and multi-factor authentication techniques. The integration of generative AI with Zero Trust Architecture and blockchain technology is also discussed. Nonetheless, no experimental approach or quantification of results is provided in the paper.

Aslam et al. (2025) have developed a method that makes use of Generative Adversarial Networks to enable occluded face recognition. The paper highlights the implementation of a framework involving multiple stages including the classification of gender, detection of facial landmarks, and mask segmentation to facilitate landmark-aware inpainting. A generator based on an encoder-decoder architecture with composite loss functions ensures visual perceptual quality, structural consistency, and identity preservation during the process. This model was trained on a dataset containing 70,000 images of masked and non-masked faces, obtaining impressive results like SSIM = 0.95 and PSNR = 33.3 dB Reconstruction bias and vulnerability to attacks remain potential concerns.

Wang et al. (2025) suggest a privacy-preserving MAP-GAN that is designed to preserve facial data privacy but maintain the ability for identification. In particular, the researchers use a GAN-based approach in combination with a unique privacy protection loss function and attribute probability score mechanism to overcome problems related to attribute leaking and binary flipping. An information loss limitation function guarantees the maintenance of image utility during the process, while residual architecture improves the quality of generated images. The experiments conducted show that the proposed solution performs better at preserving multiple attributes and keeping recognition efficiency in comparison with previous methods. Nevertheless, the model has not been tested against adversarial attacks and in real-time conditions.

Khadidos et al. (2025) examine the application of adversarial neural networks for generating synthetic medical data that can be used in conjunction with biometric pattern recognition systems. The main objective is to minimize the dependency on actual data by ensuring security during data transfer and leakage minimization. The proposed method uses a deep convolutional

adversarial neural network with conditional measurements in order to ensure consistency and quality of the data under various operating conditions. The effectiveness of the method in generating the synthetic data has been proven through experiments conducted under four different scenarios and two cases, with less than 5% data loss. Summary of Privacy-Preserving Biometric Authentication using Generative AI shown in Table.3

Table.3 Summary of Privacy-Preserving Biometric Authentication using Generative AI

S.NO	Paper	Dataset Used	Key Attributes / Features	Algorithms / Models	Methodology Used	Limitations
17	Ghani et al. (2024)	CelebA	Facial attributes, blockchain security metadata	GANs, Blockchain	Decentralized privacy-preserving face recognition	High computational and storage cost
18	Byeon et al. (2024)	Simulated multimodal dataset	Pixel-level, feature-level, score-level fusion	Deep Neural Networks	Multimodal fusion-based authentication	No privacy-preserving mechanism
19	Brown et al. (2020)	Multimodal biometric dataset	Fingerprint, face, age, gender	Decision Tree, Blockchain	Multimodal biometric verification with blockchain	Complex architecture, no adversarial testing
20	Mehar (2022)	Conceptual study	Threat intelligence, anomaly patterns	Generative AI, Blockchain, Zero Trust	AI-assisted cloud security framework	No quantitative results
21	Aslam et al. (2025)	70,000 masked/non-masked face images	Facial landmarks, mask regions	GAN encoder-decoder	Landmark-aware inpainting for occluded face recognition	Vulnerable to attacks and reconstruction bias
22	Wang et al. (2025)	Facial privacy dataset	Attribute privacy, identity retention	MAP-GAN	Privacy-preserving face synthesis with attribute protection	No adversarial attack evaluation
23	Khadidos et al. (2025)	Synthetic medical biometric data	Medical biometric consistency	Conditional DCGAN	Synthetic biometric medical data generation	Limited real-time validation

4. Multimodal Biometric Authentication with Generative AI

Multimodal biometric authentication integrated with generative AL represents an advanced paradigm for enhancing identity verification systems through the fusion of multiple biometric traits such as face, fingerprint, iris, voice, and behavioral signals. Generative models, including GANs and VAEs, are increasingly utilized to synthesize complementary biometric data, address missing modality issues, and improve dataset diversity. This integration strengthens

recognition accuracy, robustness, and resistance to spoofing attacks compared to unimodal systems. However, challenges persist in effective fusion strategies, inter-modality consistency, computational complexity, and privacy preservation. Recent research focuses on optimizing DL-based fusion architectures while ensuring security, scalability, and real-time applicability in authentication systems.

William et al. (2022) investigate AI-driven adaptive authentication systems for enhancing multi-modal biometric security in cybersecurity applications. The study aims to integrate multiple biometric modalities, including facial recognition, fingerprint, voice, and behavioral biometrics, within a unified adaptive framework. ML algorithms are employed to dynamically adjust authentication strength based on contextual risk factors such as user behavior, device characteristics, and geolocation. The approach enhances both security and usability by continuously learning from user interactions. However, the study remains conceptual in nature, lacking experimental validation, quantitative performance evaluation, and implementation on standardized biometric datasets, limiting its practical applicability in real-world systems.

Kolluri et al. (2024) analyze the role of AL and ML in enhancing multimodal biometric authentication systems. The study aims to overcome limitations of unimodal biometrics, such as spoofing vulnerability, environmental variability, and reduced accuracy. It reviews neural network-based architectures including CNNs, RNNs, and GANs, and evaluates different fusion strategies such as early, late, hybrid, and deep fusion for integrating multiple biometric traits. The findings highlight improved accuracy and robustness against adversarial attacks in multimodal systems. However, the study is survey-based, lacking experimental validation and quantitative benchmarking of proposed architectures in real-world authentication scenarios.

Javid and Kollwitz (2025) investigate AI-based behavioral biometrics for next-generation digital identity verification to address limitations of traditional authentication mechanisms such as passwords and static biometric traits. The study proposes the use of dynamic behavioral patterns including keystroke dynamics, mouse movements, touchscreen gestures, and navigation behavior for continuous and passive authentication. ML techniques such as neural networks, decision trees, and ensemble models are applied to learn and adapt to user-specific behavioral signatures, enabling real-time anomaly detection. The approach enhances security while reducing user friction and spoofing risks. However, the work remains conceptual and lacks empirical validation and benchmarking on standard behavioral biometric datasets.

Salami et al. (2025) explore AI-based behavioral biometric techniques for detecting frauds in online banking systems with an emphasis on addressing the shortcomings of traditional approaches for detecting frauds using rule-based and statistical approaches. Salami et al. [28] leverage ML and DL algorithms such as Random Forest, CNN, and LSTM on datasets such as PaySim, Credit Card Fraud Detection, and HMOG to detect suspicious patterns in transactions and behaviors. The experimental results indicate that LSTM attains the highest accuracy at 97.9%, precision at 95.6%, and recall at 93.4%, thus indicating high potential in detecting frauds in real-time. However, there are some limitations related to dataset dependency and live testing of banking systems.

Khairnar et al. (2024) present a novel biometric authentication scheme that concentrates on face liveness detection for combating any spoofing attempts made against the facial recognition system. The method involves employing DL pre-trained models such as VGG16, ResNet50, DenseNet201, and InceptionV3, which are then optimized using the SiWMv2 database involving various spoofing attacks. In order to make the system more interpretable, XAI technique through LIME is utilized for understanding the working principles behind the decision-making process. The system shows good results in handling replay attacks, mask attacks, and even makeup-based attacks. Yet, it requires heavy computations and no evaluation is done in real-time implementation and cross-database generalizability.

Gayathri and Malathy (2022) have introduced a two-level security system that utilizes intrusion

detection along with multimodal biometrics for better information security. This research makes use of the Improved Recurrent Neural Network with Bi-directional LSTM network model (I-RNN-BiLSTM) for intrusion detection as well as multimodal authentication. While intrusion detection uses NSL-KDD datasets, multimodal authentication takes into account face, iris, and fingerprint features by making use of Gabor, Canny Edge Detection, and minutiae methods. Shuffling fusion method is used before classification. The intrusion detection model demonstrates a very high level of accuracy (98.94%), while multimodal authentication shows a good level of accuracy (98%). Still, no DL models are used in this research.

Salturk and Kahraman (2024) present a biometric authentication system that combines dynamic signatures along with facial biometrics to boost security in the absence of expensive biometric equipment in online applications. The authors use computer cameras and signatures to build a database of 1,750 samples from 25 subjects. The CNN, LSTM, GRU, and TCN DL models are used to learn the time-series and spatial features of the biometric data. The combination of dynamic and static biometrics substantially boosts biometric accuracy. The experiment is limited in scope due to the use of small-sized data and testing on adversarial attacks.

Sengar et al. (2020) present a multimodal biometric authentication technique in order to address limitations in unimodal approaches, including high false acceptance rate and false rejection rate. This research combines both fingerprints and palmprints as biometric features using DNN for feature extraction such as detection of minutiae features. In addition, Euclidean distance is used as matching algorithm. Although multimodal techniques enhance the identification efficiency as well as increase the robustness of the system in the presence of noise and spoof attacks, this technique utilizes conventional feature-matching method without generative methods for dealing with changes in biometrics.

Tarek et al. (2025) suggest keyless multimodal biometrics authentication scheme that uses generative adversarial networks for better security and privacy purposes. The purpose of the research was to avoid using of classical encryption keys, substituting them by using generative models to convert raw input from biometric sources to no reversible templates synthesized by using GAN modeling. Fusion takes place at three different levels: feature level, GAN-based, and decision level in order to make system more resistant to attacks and to exclude any data leakage. The results of the work prove low error rates for different kinds of data fusion as well as high resistance to pre-image and correlation attacks. Still, the solution requires large amounts of computational resources. Summary of Multimodal Biometric Authentication with Generative AI is shown in Table.4

Table.4 Summary of Multimodal Biometric Authentication with Generative AI

S.NO	Author	Method	Advantage	Limitation
24	William et al. (2022)	AI-driven adaptive multimodal biometric authentication using ML algorithms with facial, fingerprint, voice, and behavioral biometrics.	Dynamically adjusts authentication strength based on contextual risk factors, improving security and usability.	Conceptual study without experimental validation, quantitative evaluation, or testing on standard biometric datasets.
25	Kolluri et al. (2024)	Review of AI and ML techniques including CNN, RNN, GAN, and multimodal fusion strategies	Enhances authentication accuracy, robustness, and resistance to adversarial attacks	Survey-based study lacking practical implementation and quantitative benchmarking.

		(early, late, hybrid, deep fusion).	through multimodal fusion.	
26	Javid and Kollwitz (2025)	AI-based behavioral biometrics using keystroke dynamics, mouse movements, touchscreen gestures, and navigation behavior with ML models.	Enables continuous authentication, anomaly detection, and reduced spoofing risks.	Lacks empirical validation and evaluation on benchmark behavioral biometric datasets.
27	Salami et al. (2025)	Fraud detection using behavioral biometrics with Random Forest, CNN, and LSTM on banking datasets.	Provides effective real-time fraud detection with strong predictive performance.	Performance depends on specific datasets and lacks deployment in live banking environments.
28	Khairnar et al. (2024)	Face liveness detection using VGG16, ResNet50, DenseNet201, InceptionV3, and LIME-based explainability.	Effectively detects replay, mask, and makeup spoofing attacks while improving interpretability.	Requires high computational resources and lacks real-time and cross-dataset evaluation.
29	Gayathri and Malathy (2022)	Intrusion detection and multimodal biometric authentication using I-RNN-BiLSTM with face, iris, and fingerprint fusion.	Achieves strong security through integration of intrusion detection and multimodal authentication.	Does not utilize advanced deep learning architectures for biometric feature learning.
30	Salturk and Kahraman (2024)	Dynamic signature and facial biometric authentication using CNN, LSTM, GRU, and TCN models.	Improves authentication accuracy by combining dynamic and static biometric traits.	Limited dataset size and absence of adversarial attack analysis.
31	Sengar et al. (2020)	Multimodal fingerprint and palmprint authentication using DNN-based feature extraction and Euclidean distance matching.	Improves identification accuracy and robustness against noise and spoofing attacks.	Relies on conventional feature matching and does not incorporate generative AI techniques.
32	Tarek et al. (2025)	GAN-based keyless multimodal biometric authentication with	Enhances privacy, security, and resistance to pre-	Requires substantial computational resources and

		feature-level, GAN-level, and decision-level fusion.	image and correlation attacks through irreversible biometric templates.	complex model training.

5.Liveness Detection & Anti-Spoofing using Generative AI

Presentation attacks have become serious concerns in the field of biometric authentication due to their vulnerability to spoofing attacks like photos, video replay attacks, masks, and deep fake-based attacks. Generative AI has had an enormous impact in this field by facilitating the generation of advanced spoof attacks and defences against these attacks. The DL algorithms such as GANs and CNN models play a key role in identifying real biometric characteristics based on texture features, temporal dynamics, and physiology of subjects. Modern research is directed towards enhancing robustness and generalizability under different attack scenarios.

Zia et al. (2025) suggest a scalable face recognition anti-spoofing solution by enhancing the model with the use of GANs in order to address vulnerabilities caused by photo, video, or replay attacks. The research applies Generative Adversarial Networks to implement unsupervised learning and enables automatic classification of real facial samples and those that are subject to fraud, without the need for additional training or labelling. The face verification stage is achieved through the use of a supervised classifier, thus minimizing the storage of biometric information. The evaluation conducted on CASIA-FASD and CelebA-Spoof proves improved scalability and security.

Dash et al. (2025) introduce an optimized GAN-based biometric authentication model that can be used in real-time scenarios to authenticate deepfake manipulations on faces. This research aims at addressing security threats posed by the widespread development of deepfake technologies through adversarial learning algorithms that can detect any incongruities within the synthetic content. The model relies on integrating the capabilities of GAN models in feature learning and DL algorithms in classification to differentiate between authentic and manipulated faces. The model is assessed in terms of detection accuracy, processing speed, and resistance to adversarial attacks. It is worth noting that the model is restricted by the diversity of the data available.

Yousif (2024) evaluates the effectiveness of deepfake face detection algorithms under attacks using GAN fingerprint elimination. This paper discusses the high frequency Fourier and spatial features of real vs. generated faces, emphasizing inherent vulnerabilities in DL algorithms for detecting fakes. In particular, the research indicates that an adversary could easily tamper with or eliminate the GAN fingerprint from faces, resulting in lower accuracy in detecting them. Experiments carried out on a dataset consisting of 140,000 real vs. generated faces indicate that the detection rate of fake faces is lowered by 50%.

Keerthi et al. (2025) have presented an effective DL technique that can detect deepfake images of palmprints for improving the safety of biometric authentication processes. They have developed the problem of deepfake palmprint spoofing within financial applications and identity verification systems through the use of a hybrid DL model using CNN and ResNet. In order to test their approach, they have created their own dataset using ridge-based synthesis techniques and data augmentation methods, including rotating, adjusting contrast, introducing noises, and creating distortions. Metrics such as accuracy, precision, recall, and F1-Score were used to measure the effectiveness of the model in detecting deepfakes, which performed effectively.

Adami et al. (2024) present a novel unsupervised DL architecture for contactless fingerprint anti-spoofing. In their research, emphasis has been made towards improving the capability of generalization, where an autoencoder model augmented with a convolutional block attention

system was trained exclusively with legitimate fingerprints without using any spoof samples. The technique was tested for multiple kinds of presentation attacks, including photo paper and display attack spoofs. The proposed method yielded excellent results with an average BPCER and APCER values of 0.96%, and 1.6% respectively. There might be some restrictions in dealing with highly sophisticated attacks and scalability issues in practical application.

Spinoulas et al. (2021) explore the possibility of PAD of multi-modal fingerprints utilizing advanced sensor technologies that would enhance robustness to spoof attacks. This research explores multiple imaging sensors such as short-wave infrared imaging sensors, near-infrared imaging sensors, and front/back illuminated laser imaging sensors combined with the classification algorithm of fully convolutional deep neural network. In their analysis, they explore both known and unknown cases of attack, along with intra-dataset and inter-dataset performance evaluation. The authors reveal that the utilization of multi-modal sensors increases significantly the performance of PAD when compared to conventional fingerprint datasets. However, the requirement of advanced hardware limits its applicability.

Abdulbaqi et al. (2023) present a multimodal biometric anti-spoofing scheme based on face detection and ECG signals for improving the security of biometrics-based authentication. The authors aim at overcoming shortcomings of face detection-based biometrics through inclusion of physiological signals in both decision-making and scoring phases. The ECG signals are used in combination with wavelet transform for feature extraction. Experiments have confirmed improved accuracy (94%) and low rejection errors for the proposed multimodal scheme. However, the scheme has relatively higher false acceptance error rates and is also restricted by the necessity of employing specialized sensors.

Alashik and Yildirim (2021) present a framework using DL-GANs for verifying the biometric identities using dorsal hand veins. In this study, the combination of DL along with Generative Adversarial Networks is utilized to improve feature representation for enhanced authentication. A multi-step pre-processing step has been adopted for extracting features from the dorsal hand vein images, which are then classified using GANs-based learning. The effectiveness of the proposed method was verified on the datasets from Jilin University as well as the 11K hands database, obtaining accuracy rates of 98.36% and 96.43%, respectively. Nevertheless, the method lacks generality and scalability, apart from robustness against adversarial attacks.

Koshy & Mahmood (2020) propose DL-based approaches to detect face liveness to counter face liveness spoofing attacks on biometrics. As stated in the paper, a hybrid pipeline using non-linear anisotropic diffusion along with texture enhancement of face images is used while specific CNN models such as SCNN and Inception v4 and CNN-LSTM model architecture is proposed to classify static face images and videos respectively. The experiments performed show very high accuracy in face liveness detection, achieving 96.21% accuracy in the case of static face images and 98.71% in the case of videos, whereas HTER is very low in both cases. However, the approach needs pre-processing and lacks an analysis of deepfake attacks. Liveness Detection & Anti-Spoofing using Generative AI shown in Table.5

Table.5 Liveness Detection & Anti-Spoofing using Generative AI

S.No.	Paper	Dataset Used	Key Attributes / Features	Algorithms / Models	Methodology Used	Limitations
33	Zia et al. (2025)	CASIA-FASD, CelebA-Spoof	Face spoofing patterns	GANs, supervised classifiers	GAN-based anti-spoofing and face verification	Requires large-scale deployment testing

34	Dash et al. (2025)	Deepfake face datasets	Manipulated facial features	GAN + DL classifiers	Real-time deepfake authentication	Limited data diversity
35	Yousif (2024)	140,000 real/generated faces	GAN fingerprint patterns	Fourier feature analysis	GAN fingerprint elimination attack study	Detection accuracy reduction
36	Keerthi et al. (2025)	Custom palmprint deepfake dataset	Ridge textures, spoof patterns	CNN, ResNet	Deepfake palmprint spoof detection	Limited public benchmark testing
37	Adami et al. (2024)	Contactless fingerprint datasets	Genuine fingerprint representations	Autoencoder + Attention CNN	Unsupervised anti-spoofing framework	Scalability concerns
38	Spinoulas et al. (2021)	Multi-sensor fingerprint datasets	SWIR, NIR, laser imaging features	FC-DNN	Multi-sensor presentation attack detection	Requires advanced hardware
39	Abdulbaqi et al. (2023)	Face + ECG datasets	Physiological ECG signals	Wavelet Transform	Multimodal anti-spoofing using ECG and face	Specialized sensors required
40	Alashik and Yildirim (2021)	Jilin University, 11K Hands	Dorsal hand vein patterns	DL-GAN	Hand vein biometric authentication	Limited scalability and robustness
41	Koshy & Mahmood (2020)	Face image/video datasets	Texture and temporal liveness features	SCNN, Inception-v4, CNN-LSTM	Face liveness detection pipeline	No deepfake attack analysis

6. Emerging Trends & Future Directions in Generative AI Biometrics

The incorporation of generative AI into biometric authentication has been contributing to many improvements in the field of security, adaptability, and data synthesis abilities. These trends are characterized by diffusion generative models, self-supervised representation learning, and multimodal fusion techniques for improved performance across different conditions. Much attention is being paid to privacy-preserving models, including federated learning and differential privacy, in order to address potential threats related to the use of sensitive biometric data. Moreover, there is increased interest in developing adversarial robust and explainable AI due to ongoing deepfakes and other biometric spoofing attacks.

Makrushin et al. (2023) present a thorough review regarding synthetic biometrics and focus on the generation of fingerprints, faces, irises, and vascular patterns using contemporary neural

generative models. This research seeks to examine how data-driven synthetic generation technology can be used to overcome issues of privacy, dataset bias, and sample scarcity. This paper classifies previous methodologies and their applications for testing on a large scale or creating an algorithm using synthetic data. However, this paper emphasizes the improvement of realism through the use of GANs and deep generative models but at the same time requires suitable quality metrics. Nonetheless, this paper is solely a review with no experiments involved.

Awodeyi et al. (2025) have developed a dynamic integration of liveness into a CNN-based system for the detection of spoofing attacks in multi-biometric face and iris identification. The research is intended to increase the level of security in authentication by integrating dynamic liveness features like eye blinks, pupil motion, and time texture into the recognition process. A dual branch of CNN is used to capture spatial and temporal features, which are then combined with liveness features to achieve higher efficiency of classification. An experiment was conducted using the modified ORL and CASIA-IrisV4 databases containing spoofed photo and video attacks. The method achieves a high-level detection rate of 98.9% with FAR and FRR values being 0% and 1.1%, respectively.

Gomez-Alanis et al. (2022) introduce GANBA, a framework for generative adversarial networks that aims to tackle the issue of biometric spoofing within automated speaker verification. The research tackles vulnerabilities within presentation attack detection by jointly learning anti-spoofing and ASV losses, which enable the generation of adversarial spoofing examples that can fool entire biometric chains. In parallel, the discriminator is being fine-tuned to improve resistance to both standard and generated attacks. The performance results based on the ASVspoof 2019 challenge dataset have shown that attacks generated using GANBA outperform current state-of-the-art adversarial approaches in both white-box and black-box attacks while increasing PAD resistance.

Kumar and Abbas (2025) offer a multimodal approach to AI and ML for next-generation digital ecosystems that ensures secure integration of biometric and fraudulent activity identification. The authors use facial recognition, voice biometric information, and behavioral patterns to verify users' identities and monitor any abnormal behaviors. Ensembles and anomaly detection models are utilized to analyze transactional and biometric data in real time, which helps in improving the accuracy rate and minimizing errors in identification. The model is intended to be implemented in cloud and edge computing environments. Unfortunately, Kumar and Abbas do not provide sufficient experimental details and lack benchmarking results on adversarial attacks.

Vel (2021) presents an AI-powered adaptive authentication scheme for multi-biometric authentication systems with the objective of increasing security and usability. This research work combines various biometrics such as fingerprint authentication, facial authentication, and voice authentication and uses ML techniques for adapting the authentication parameters according to context and behavior data. It reports a decrease in false acceptance rates by 27% and a decrease in false rejection rates by 35% when compared to static authentication schemes. Nevertheless, there are no details regarding the methodology used, the dataset employed, and the experiments conducted under current DL and generative AI attacks.

Jang et al. (2026) present a quantum-proof, machine-learning robust real-time keystroke protection mechanism incorporating blockchain-enabled decentralized identity for biometric behavioral authentication. This paper considers attacks using browser-based keyloggers, timing side channels, and potential quantum computer threats by employing ChaCha20-Poly1305 encryption, differential privacy-based noise addition, timing jittering, and post-quantum cryptographic algorithms (ML-KEM-768). Decentralized identity is maintained through the use of blockchain (Hyperledger Fabric) and decentralized identifier (DID). Experimental results reveal a dramatic decline in keystroke-based user recognition success rate

from 85.8% to 5.5% (synthetically generated) and 72.4% to 2% (CMU database). Nonetheless, there is no experimental evidence regarding side channels that target audio and EM emanations. Radanliev et al. (2025) present a quantum-resistant and privacy-focused system for digital identity which includes post-quantum cryptography, blockchain-based identifiers, and AL with transformers. This research seeks to overcome the security challenges that arise with the use of centralized identity schemes, especially issues such as quantum-based attack, data aggregation, and identity correlation. The technique used includes lattice cryptography compliant with NIST standards for key exchanges, zero-knowledge proofs for selective attribute release, and homomorphic encryption for privacy-preserving verification. Furthermore, blockchain oracles and decentralized identifiers ensure that there is no need for central authorities in terms of auditing and integrity.

Althobaiti et al. (2022) present a novel lattice cryptography model that is resilient to quantum computer attacks and suitable for secure face recognition in IoT systems as well as advanced communication networks. The paper combines facial biometric characteristics and uses them for dynamically generating key codes without any need for transmitting and storing such critical information. It should be noted that this lattice cryptography system is created to provide robustness to quantum computers while providing light-weight performance. Performance results achieved in the NB-IoT scenario show that there is an enhancement in delay, power consumption, throughput, and stability. Nevertheless, there is no performance analysis in relation to biometric authentication reliability. Emerging Trends & Future Directions in Generative AI Biometrics

Table.6 Emerging Trends & Future Directions in Generative AI Biometrics

S. NO	Paper	Dataset Used	Key Attributes	Models	Methodology Used	Limitations
42	Makrushin et al. (2023)	Review-based	Fingerprints, face, iris, vascular patterns	GANs, generative models	Review of synthetic biometrics	No experiments
43	Awodeyi et al. (2025)	ORL, CASIA-IrisV4	Eye blink, pupil motion, temporal texture	Dual-branch CNN	Dynamic liveness integration	Limited modality coverage
44	Gomez-Alanis et al. (2022)	ASVspoof 2019	Speaker spoofing features	GANBA	GAN-generated adversarial spoofing examples	Audio-focused only
45	Kumar and Abbas (2025)	Cloud-edge biometric systems	Face, voice, behavior patterns	Ensemble ML, anomaly detection	Real-time multimodal fraud detection	Missing benchmark results
46	Vel (2021)	Multi-biometric authentication framework	Fingerprint, face, voice	Adaptive ML	Context-aware adaptive authentication	Lack of methodological details

47	Jang et al. (2026)	CMU keystroke dataset	Keystroke timing, blockchain identity	ML-KEM-768, Differential Privacy	Quantum-resistant keystroke authentication	No audio/EM side-channel evaluation
48	Radanliev et al. (2025)	Decentralized identity systems	Selective attribute release	Transformers, Homomorphic Encryption	Quantum-resistant decentralized identity framework	No biometric benchmarking
49	Althobaiti et al. (2022)	NB-IoT face recognition environment	Facial biometric cryptographic keys	Lattice Cryptography	Quantum-resistant biometric encryption	No authentication reliability evaluation

8.Evolutionary Perspective of AI-Based Biometric Authentication

The chronology represents the development timeline of AI-powered biometric authentication systems from 2020 to 2026, highlighting the constant evolution of intelligent security systems. This timeline illustrates the evolution of biometric authentication systems from conventional systems using deep learning to those that have advanced to become more intelligent through the implementation of GANs, multimodal authentication, explainable AI, blockchain-based security, privacy protection measures, and quantum-resistance. Every phase in the timeline shows the gradual improvement and evolution of the technology as the need to develop highly secure, adaptive, and reliable authentication systems capable of combating contemporary cybersecurity threats such as spoof attacks and deepfakes becomes increasingly necessary.

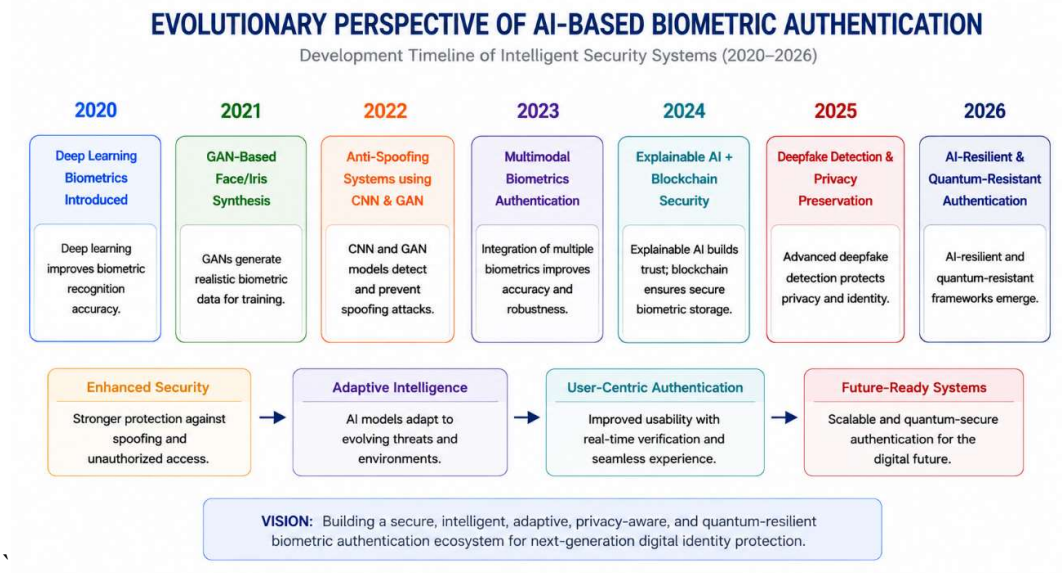

Figure.2 Evolutionary Perspective of AI-Based Biometric Authentication

Figure 2 illustrates the evolutionary approach to the development of AI-based biometric authentication technologies between 2020 and 2026, showing how intelligent solutions develop progressively. Figure 2 starts with introducing deep learning models for biometric recognition as the first evolutionary step in 2020, allowing for efficient feature extraction and authentication accuracy improvement. Following that, GAN-based face and iris generation appeared as a part of machine learning models used to generate realistic biometric data in 2021 to train algorithms. In 2022, the evolution was connected with the development of anti-spoofing

solutions with CNN and GAN algorithms used to detect and stop presentation attacks. Biometric authentication using several biometric modalities became common practice in 2023 to increase the reliability of intelligent algorithms and security of such systems. In 2024, AI solutions became explainable and secure with blockchain integration allowing biometric data storage more effectively. 2025 was marked with deepfake detection tools and privacy protection technologies that allowed avoiding synthetic identities and preserving users' information safety. Finally, in 2026, AI-resilient and quantum resistant authentication frameworks became essential components of the future biometric ecosystem.

8.1 Comparative Discussion and Research Outlook

Biometric Authentication Using Generative AI Technology has seen significant advancements in its development with respect to GAN, VAE, diffusion model, and multimodal learning architectures. GAN-based methods have shown high efficiency in terms of synthesizing biometric samples and spoofing attacks, but are hampered by increased computational costs and low generalization capability. The multimodal approach improves authentication accuracy and robustness, yet has a higher level of difficulty in implementation. Privacy-preserving methods such as blockchain, federated learning, and differential privacy ensure better security while facing scalability issues. The future direction includes explainable AI technology, diffusion-based biometric sample generation, edge computing, post-quantum cryptography, and privacy-aware authentication systems.

9.Conclusion and Future Perspectives

The use of generative artificial intelligence in biometric authentication systems has led to enhanced performance and security of contemporary biometric identity verification systems. In this study, we examined the latest innovations in the areas of biometric data generation, multimodal biometric authentication, fake detection, anti-spoofing, privacy-preserving, and liveness detection in biometric systems utilizing cutting-edge AI technologies like GANs, VAEs, diffusion, transformer, and hybrid deep learning systems. From our review, it is evident that generative AI approaches have been able to overcome the inherent shortcomings associated with conventional biometric authentication approaches. These include inadequate training data, spoofing attacks, adversarial attacks, and privacy issues. Multimodal biometric systems using facial recognition, fingerprints, iris scanning, voice recognition, vein recognition, and behavioral recognition offer better authentication capabilities than conventional unimodal systems. Moreover, innovative solutions such as blockchain, federated learning, explainable AI, and quantum cryptography further enhance the security and privacy of biometric authentication systems. Nevertheless, various issues have yet to be addressed by researchers, such as high computational complexity, lack of generalization to other databases, real-time application, weak adversarial robustness, and no privacy-preserving approach at all. It is suggested that future studies should be directed toward the creation of low-complexity, scalable, explainable, and privacy-preserving multimodal biometric systems that are resilient against both deepfakes and adversarial attacks. Self-supervised learning, diffusion-based generation, edge-AI implementation, blockchain-based decentralized identity management, and post-quantum security technologies will be vital in creating new-age intelligent biometric authentication systems.

References

Abdulbaqi, Azmi Shawkat, Nawfal Ahmed Turki, Ahmed J. Obaid, Soumi Dutta, and Ismail Yusuf Panessai. 2023. “Spoof Attacks Detection Based on Authentication of Multimodal Biometrics Face-ECG Signals.” Pp. 507–26 in *Artificial intelligence for smart healthcare*. Springer.

Adami, Banafsheh, MohammadReza Hosseinzadehketilateh, and Nima Karimian. 2024. “Contactless Fingerprint Biometric Anti-Spoofing: An Unsupervised Deep Learning

Approach." Pp. 1–10 in *2024 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE.

Alashik, Khaled Mohamed, and Remzi Yildirim. 2021. "Human Identity Verification from Biometric Dorsal Hand Vein Images Using the DL-GAN Method." *IEEE Access* 9:74194–208.

Alghamdi, Shaima M., Salma Kammoun Jarraya, and Faris Kateb. 2024. "Enhancing Security in Multimodal Biometric Fusion: Analyzing Adversarial Attacks." *IEEE Access* 12:106133–45.

Althobaiti, Ohood Saud, Toktam Mahmoodi, and Mischa Dohler. 2022. "Intelligent Bio-Latticed Cryptography: A Quantum-Proof Efficient Proposal." *Symmetry* 14(11):2351.

Aslam, Fatima, Adil Afzal, Muhammad Rizwan, Adel Sulaiman, Mana Saleh Al Reshan, and Asadullah Shaikh. 2025. "Enhancing Security and Privacy in Occluded Face Recognition: A Human-Centered GAN-Based Approach for Masked Identities in High-Security Environments." *IET Image Processing* 19(1):e70256.

AWODEYI, AFOLABI, PHILIP ASUQUO, and BLISS STEPHEN. 2025. "Dynamic Liveness-Integrated CNN Architecture for Face-Iris Spoof Detection." *Detail* 6:10.

Brown, Richard, Gueltoum Bendiab, Stavros Shiaeles, and Bogdan Ghita. 2020. "A Novel Multimodal Biometric Authentication System Using Machine Learning and Blockchain." Pp. 31–46 in *International Networking Conference*. Springer.

Byeon, Haewon, Vikas Raina, Mukta Sandhu, Mohammad Shabaz, Ismail Keshta, Mukesh Soni, Khaled Matrouk, Pavitar Parkash Singh, and TR Vijaya Lakshmi. 2024. "Artificial Intelligence-Enabled Deep Learning Model for Multimodal Biometric Fusion." *Multimedia Tools and Applications* 83(33):80105–28.

Chowdhury, AM Mahmud, Md Jahangir Alam Khondkar, and Masudul Haider Imtiaz. 2024. "Advancements in Synthetic Generation of Contactless Palmprint Biometrics Using StyleGAN Models." *Journal of Cybersecurity and Privacy* 4(3):663–77.

Dash, Manoranjan, A. Mallikarjuna Reddy, Deekshitha Pulapa, Varshini Kodakandla, and Kavya Gavini. 2025. "Optimizing the Biometric Authentication Scheme to Detect the Deepfake in Real Time Using GAN." Pp. 1–6 in *2025 IEEE International Conference for Women in Innovation, Technology & Entrepreneurship (ICWITE)*. IEEE.

Dudykevych, Valeriy, Serhii Yevseiev, Halyna Mykytyn, Khrystyna Ruda, and Hennadii Hulak. 2024. "Detecting Deepfake Modifications of Biometric Images Using Neural Networks." *Cybersecurity Providing in Information and Telecommunication Systems 2024* 3654:391–97.

Farooq, Muhammad Ali, Wang Yao, Gabriel Costache, and Peter Corcoran. 2023. "Childgan: Large Scale Synthetic Child Facial Data Using Domain Adaptation in Stylegan." *IEEE Access* 11:108775–91.

Gayathri, M., and C. Malathy. 2022. "A Deep Learning Framework for Intrusion Detection and Multimodal Biometric Image Authentication." *Journal of Mobile Multimedia* 18(2):393–419.

Ge, Xinxu, Xin Liu, Zitong Yu, Jingang Shi, Chun Qi, Jie Li, and Heikki Kälviäinen. 2024. "Difffas: Face Anti-Spoofing via Generative Diffusion Models." Pp. 144–61 in *European conference on computer vision*. Springer.

Ghani, MANU, Kun She, Muhammad Arslan Rauf, Shumaila Khan, Masoud Alajmi, Yazeed Yasin Ghadi, and Hend Khalid Alkahtani. 2024. "Toward Robust and Privacy-Enhanced Facial Recognition: A Decentralized Blockchain-Based Approach with GANs and Deep Learning." *Math. Biosci. Eng* 21(3):4165–86.

Gomez-Alanis, Alejandro, Jose A. Gonzalez-Lopez, and Antonio M. Peinado. 2022. "GANBA: Generative Adversarial Network for Biometric Anti-Spoofing." *Applied Sciences* 12(3):1454.

He, Shijing, Yaxiong Lei, Zihan Zhang, Yuzhou Sun, Shujun Li, Chi Zhang, and Juan Ye. 2025. "Identity Deepfake Threats to Biometric Authentication Systems: Public and Expert Perspectives." *arXiv Preprint arXiv:2506.06825*.

Jang, Yeojin, Harin Jang, and Sangkeum Lee. 2026. "A Quantum-Resistant and AI-Resilient Real-Time Keystroke Protection Framework with Blockchain-Backed Decentralized Identity." *IEEE Access*.

Javid, Umair, and Elbert Kollwitz. 2025. "AI-Based Behavioral Biometrics for Next-Generation Digital Identity Verification."

Kamel, Kamel, Keshav Sood, Hridoy Sankar Dutta, and Sunil Aryal. 2025. "A Survey of Threats against Voice Authentication and Anti-Spoofing Systems." *arXiv Preprint arXiv:2508.16843*.

Kavitha, AR, C. Sankari, and T. Shalini. 2024. "Deep Learning-Enhanced Iris Biometrics: Integrating Gan-Generated Synthetic Data, Hybrid Feature Engineering, and Iterative Self-Learning for Robust and Scalable Recognition Systems." Pp. 1–6 in *2024 International Conference on Advancement in Renewable Energy and Intelligent Systems (AREIS)*. IEEE.

Keerthi, Guttikonda, Devarakonda Uma Katyayani, Balla Naga Durga, Boddu Snehitha, Chinta Durga Rahul, and UG Naidu. 2025. "TOWARDS SECURE BIOMETRICS: DEEP FAKE PALMPRINT DETECTION WITH ADVANCED CNN-RESNET MODELS." *Journal of Nonlinear Analysis and Optimization* 16(1).

Keresh, Arman, and Pakizar Shamoi. 2024. "Liveness Detection in Computer Vision: Transformer-Based Self-Supervised Learning for Face Anti-Spoofing." *IEEE Access* 12:185673–85.

Khadidos, Adil O, Hariprasath Manoharan, Alaa O Khadidos, Shitharth Selvarajan, and Subhav Singh. 2025. "Synthetic Healthcare Data Utility with Biometric Pattern Recognition Using Adversarial Networks." *Scientific Reports* 15(1):9753.

Khairnar, Smita, Shilpa Gite, Kashish Mahajan, Biswajeet Pradhan, Abdullah Alamri, and Sudeep D. Thepade. 2024. "Advanced Techniques for Biometric Authentication: Leveraging Deep Learning and Explainable AI." *IEEE Access* 12:153580–95.

Khan, Farrukh Aslam, and Muhammad Khurram Khan. 2025. "Generative AI and Deepfake Detection in Biometric Systems." *Cognitive Computation* 17(3):112.

Kolluri, Venkateswaranaidu, Souratn Jain, Manjeet Malaga, and Jyotipriya Das. 2024. "Advancing Biometric Security through AI and ML: A Comprehensive Analysis of Neural Network Architectures for Multimodal Authentication Systems." *International Journal of Communication Networks and Information Security* 16(5):487–505.

Kordas, Adrian, Ewelina Bartuzi-Trokielewicz, Michał Ołowski, and Mateusz Trokielewicz. 2024. "Synthetic Iris Images: A Comparative Analysis between Cartesian and Polar Representation." *Sensors* 24(7):2269.

Koshy, Ranjana, and Ausif Mahmood. 2020. "Enhanced Deep Learning Architectures for Face Liveness Detection for Static and Video Sequences." *Entropy* 22(10):1186.

Kumar, Wajid, and Fakhar Abbas. 2025. "Securing Next-Gen Digital Ecosystems: Integrating Biometric Authentication and Fraud Detection through Multimodal AI and ML Models."

Li, Fan, Yanxiang Chen, Haiyang Liu, Zuxing Zhao, Yuanzhi Yao, and Xin Liao. 2024. "Vocoder Detection of Spoofing Speech Based on GAN Fingerprints and Domain Generalization." *ACM Transactions on Multimedia Computing, Communications and Applications* 20(6):1–20.

Makrushin, Andrey, Andreas Uhl, and Jana Dittmann. 2023. "A Survey on Synthetic Biometrics: Fingerprint, Face, Iris and Vascular Patterns." *Ieee Access* 11:33887–99.

Mathew, Amitha, and P. Amudha. 2024. "Improved Finger Vein Recognition Using Generative Adversarial Network and Transfer Learning." *Journal of Nanoelectronics and Optoelectronics* 19(10):1042–52.

Mehar, Tariq. 2022. "Advanced Cyber Security Measures in Cloud Computing for Video and Media Processing Using Generative AI."

Mjachky, Lubos, and Ivan Homoliak. 2025. "Generative Adversarial Networks Applied for Privacy Preservation in Biometric-Based Authentication and Identification." *arXiv Preprint arXiv:2509.20024*.

Mustafa, Syed Muhammad Nabeel, Syeda Sundus Zehra, Alina Baber, and Maria Andleeb Siddiqui. 2023. "Fingerprint Generation and Authentication Though Adaptive Convolution Generative Adversarial Network (ADCGAN)." Pp. 1–5 in *2023 7th International Multi-Topic ICT Conference (IMTIC)*. IEEE.

Natarajan, Sathish Kumar, Azween Abdullah, Sukhminder Kaur, and Prabhu Natarajan. 2025. "Advancing Multi-Modal Behavioral Biometric Authentication: A Deep Learning Approach With Synthetic Data Generation." *IEEE Access*.

Pakina, Anil Kumar, Deepak Kejriwal, Anshul Goel, and Tejaskumar Dat-tatray Pujari. 2023. "AI-Generated Synthetic Identities in Fin Tech: Detecting Deep Fakes KYC Fraud Using Behavioral Biometrics." *IOSR Journal of Computer Engineering* 25(3):26–37.

Park, Seong Hee, Soo-Hyun Lee, Min Young Lim, Pyo Min Hong, and Youn Kyu Lee. 2024. "A Comprehensive Risk Analysis Method for Adversarial Attacks on Biometric Authentication Systems." *IEEE Access* 12:116693–710.

Pushpakumar, R. 2022. "Hybrid Variational Autoencoders and Graph Neural Networks for Behavioural Biometric Authentication." *Environment* 18(2).

Qin, Huafeng, Haofei Xi, Yantao Li, Mounim A. El-Yacoubi, Jun Wang, and Xinbo Gao. 2023. "Adversarial Learning-Based Data Augmentation for Palm-Vein Identification." *IEEE Transactions on Circuits and Systems for Video Technology* 34(6):4325–41.

Radanliev, Petar, Carsten Maple, and Omar Santos. 2025. "Complying with the NIST Post-Quantum Cryptography Standards and Decentralizing Artificial Intelligence: Methodology for Quantum-Resistant and Privacy-Preserving Digital Identity Systems." *Frontiers in Blockchain* 8:1702066.

Rao, Vuda Sreenivasa, Shirisha Kasireddy, Annapurna Mishra, R. Salini, Sanjiv Rao Godla, and Khaled Bedair. 2024. "Unveiling Spoofing Attempts: A DCGAN-Based Approach to Enhance Face Spoof Detection in Biometric Authentication." *International Journal of Advanced Computer Science & Applications* 15(4).

Raouf, Hussien Abdel, Mostafa M. Fouda, and Mohamed I. Ibrahem. 2024. "Revolutionizing User Authentication Exploiting Explainable AI and CTGAN-Based Keystroke Dynamics." *IEEE Open Journal of the Computer Society* 6:97–108.

Salami, Isaac Adinoyi, Anuoluwapo Deborah Popoola, Michael Olayinka Gbadebo, Faith Hauwa Oluwapamilerin Kolo, and Temilade Oluwatoyin Adesokan-Imran. 2025. "AI-Powered Behavioural Biometrics for Fraud Detection in Digital Banking: A next-

Generation Approach to Financial Cybersecurity." *Asian Journal of Research in Computer Science* 18(4):473–94.

Salturk, Serkan, and Nihan Kahraman. 2024. "Deep Learning-Powered Multimodal Biometric Authentication: Integrating Dynamic Signatures and Facial Data for Enhanced Online Security." *Neural Computing and Applications* 36(19):11311–22.

Sengar, Sandeep Singh, U. Hariharan, and K. Rajkumar. 2020. "Multimodal Biometric Authentication System Using Deep Learning Method." Pp. 309–12 in *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)*. IEEE.

Simaiya, Sarita, Vivek Singh, Praveena Challa, Kapil Kumar Sharma, Sathish Kuppan Pandurangan, Lidia Gosy Tekeste, Ehab Seif Ghith, Shimaa A. Hussien, and Umesh Kumar Lilhore. 2026. "AI Driven System for Enhancing Consumer Electronics through Maintenance Personalization and Security." *Scientific Reports*.

Spinoulas, Leonidas, Hengameh Mirzaalian, Mohamed E. Hussein, and Wael AbdAlmageed. 2021. "Multi-Modal Fingerprint Presentation Attack Detection: Evaluation on a New Dataset." *IEEE Transactions on Biometrics, Behavior, and Identity Science* 3(3):347–64.

Tak, Hemlata, Massimiliano Todisco, Xin Wang, Jee-weon Jung, Junichi Yamagishi, and Nicholas Evans. 2022. "Automatic Speaker Verification Spoofing and Deepfake Detection Using Wav2vec 2.0 and Data Augmentation." *arXiv Preprint arXiv:2202.12233*.

Tarek, Mayada, Eslam Hamouda, Amjad Alsirhani, Abdullah Alomari, and Ayman Mohamed Mostafa. 2025. "A Keyless Multimodal-Based User Authentication Scheme Using Generative Adversarial Networks." *PeerJ Computer Science* 11:e3360.

Vel, Thulasi. 2021. "Ai-Driven Adaptive Authentication for Multi-Modal Biometric Systems." *J. Electrical Systems* 17(1):75–88.

Wang, Yue, Meng Yue, Zhiqiang Yao, Zheyu Chen, Renyuan Hu, and Biao Jin. 2025. "MAP-GAN: Multi-Attribute Facial Privacy Protection Model without Losing Identification." *Cybersecurity* 8(1):112.

WILLIAM, BRUCE, ADEYEMO AFEEZ, and AKANDE OLAMIDE. 2022. "AI-Driven Adaptive Authentication: Revolutionizing Multi-Modal Biometric Security."

Yadav, Shivangi, and Arun Ross. 2023. "Iwarpgan: Disentangling Identity and Style to Generate Synthetic Iris Images." Pp. 1–10 in *2023 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE.

Yousif, Jabar H. 2024. "Evaluating the Effectiveness of a Gan Fingerprint Removal Approach in Fooling Deepfake Face Detection." *Journal of Internet Services and Information Security*.

Zen, Hilary, Rohan Wagh, Miguel Wanderley, Gustavo Bicalho, Rachel Park, Megan Sun, Rafael Palacios, Lucas Carvalho, Guilherme Rinaldo, and Amar Gupta. 2025. "Ensemble-Based Biometric Verification: Defending Against Multi-Strategy Deepfake Image Generation." *Computers* 14(6):225.

Zia, Ayesha, Syeda Ravia Ejaz, Sabeerah Ahmad, and Farrukh Hasan Syed. 2025. "GAN-Enhanced Scalable Anti-Spoofing Framework for Facial Recognition Systems."