

Understanding Biometric-based Systems for Detecting and Preventing Cyber-attacks: Current Trends, Emerging Technologies, and Synthetic Biometrics

Abstract. Today, everyone is heavily dependent on computers, mobile devices, and digital systems/applications to store, access, and transmit their data and personal information. On the other hand, cybersecurity threats, exploitation of digital systems, and new, complex cyberattacks are evolving daily. This requires a growing need for innovative approaches to protecting data beyond traditional methods. The study explores the use of biometric systems in cybersecurity for the prevention and detection of cyberattacks by integrating them for authenticating and authorizing individuals. Biometric authentication is used to verify an individual's identity and grant them access based on their roles or authorizations. The paper focuses on understanding current trends and emerging technologies in biometric systems, while recognizing that these systems are not immune to cyberattacks. Can synthetic biometric data that is generated using virtual identities be an option to be considered to minimize the risk of exposing user identity in the event of a data breach, and as a means to preserve privacy, be explored as part of this research? A qualitative study is carried out using existing literature and analyzed based on the generated themes. The outcome of the study resulted in a multi-layered conceptual framework integrating the modalities of biometric systems with synthetic data and a model offering a feedback loop that can enhance operational efficiency and cultivate user trust and resilience. The study also provides insights relevant to businesses and researchers to build their systems and enhance research from a user perspective.

Keywords: Biometric systems, Cyber security, Synthetic biometric, Cyber-attack detection and prevention.

1 Introduction

1.1 Background

Biometric technology is used to recognize individuals based on their biological, including physical and behavioural, characteristics, and is used in numerous applications, including Government systems, to confirm and verify an individual's identity [12]. These systems are widely adopted in banking, border control, and airport systems, e-commerce, Government sectors, and physical/logical access control, thus providing a robust defense against unauthorized access [7].

The benefits offered by biometric technology are not limited to only individual identity but also to preventing fraud, enabling physical access control for institutions or even automobiles, tracking time and attendance, and application and device authentication. These biological characteristics of individuals can include fingerprints, iris/retina scans, hand geometry, facial features/image, DNA images, voice patterns, signatures, keystroke rhythms, and mouse navigation, as shown in Figure 1 [7, 12]. Traditional authentication methods like passwords or tokens can be easily

compromised, lost, or stolen, and biometrics provides an advantage in this aspect since it's quite intrinsic to individuals and it's quite challenging to replicate or falsify [20]. Today, in comparison to the traditional authentication methods, biometric-based systems, due to their unique and advantageous offerings, are now an integral part of cybersecurity. Although these are not without vulnerabilities or immune to the various cyber-attacks, thereby compromising their effectiveness. When using a biometric system for authentication, it is essential to ensure that data is protected both at rest and in transit, with a trusted process to identify threats and implement countermeasures at each point [12].

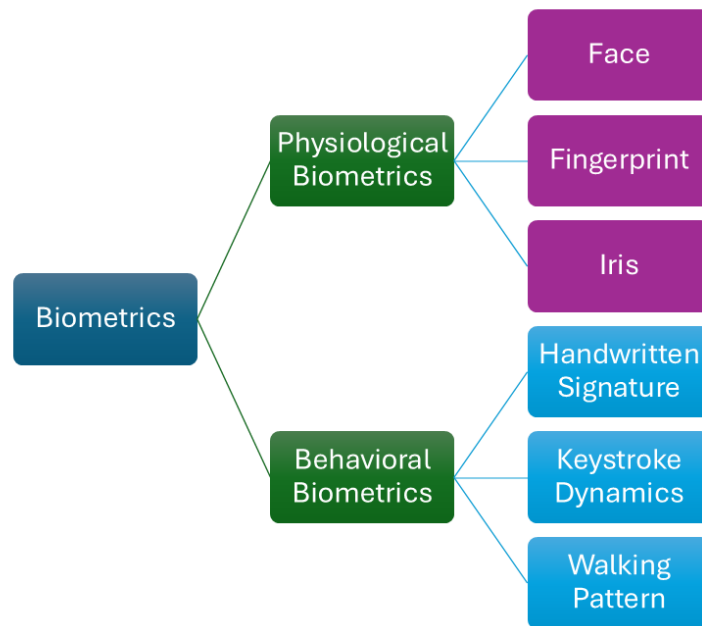


Fig. 1: Categorization of Biometrics System

1.2 Problem Statement

In today's digital era, the usage of digital systems, the internet, and the rise in cyber-attacks are going hand-in-hand [7]. Usage of traditional security means like passwords and firewalls is no longer sufficient to protect against the cyber threats that compromise the security and integrity of sensitive information. Biometric-based systems have become significantly popular in cybersecurity for verifying an individual's identity, with the help of their unique physical or behavioral characteristics, and offering an enhanced, promising solution that can prevent fraud and is quite convenient for users. Despite the commendable advantages offered by these systems, there are concerns about privacy and the risk of data breaches, leading to unauthorized access, identity theft, and impersonation [20]. These data privacy concerns arise in conjunction with one of the major risks associated with biometric systems, i.e., storing and processing

the sensitive data, which becomes multifold to comply with regulatory standards like GDPR (General Data Protection Regulation). Though the biometric systems present a promising avenue for enhancing cybersecurity, their vulnerability to various attacks and systems not being completely foolproof necessitate more ongoing research and development to understand their effectiveness, proactive measures, security, and emerging trends, especially on the privacy-preserving feasibilities with strategies to strengthen the systems against evolving threats.

Research Objective (RO). The objective of this research is to study the current state of biometric-based systems for detecting and preventing cyber-attacks, including the feasibility of privacy-preserving biometric techniques to address the concerns related to privacy, and to explore their potential applications and limitations as follows:

1. To analyze the potential applications and limitations of biometric-based systems in detecting and preventing cyber-attacks.
2. To examine the current trends and emerging technologies in biometric-based systems for cybersecurity.
3. To understand the use of synthetic biometrics as a privacy-preserving technique.

Research Questions (RQ).

The research question associated with this study, to align with the research objectives, is:

RQ1. What are the potential applications and limitations of biometric-based systems in detecting and preventing cyber-attacks?

RQ2. What are the latest trends and technologies emerging in biometric-based systems for cybersecurity?

RQ3. How can synthetic biometrics be used to address concerns related to data privacy and reduce the risk of data breaches in biometric systems?

2 Literature Review

A biometric system uses distinctive human features, captured and analyzed, to verify a person's identity. These distinct human traits includes the unique ridges, minutia points [4], and patterns as seen on the fingertips captured via fingerprints, scanning the iris which is the colored part of one's eye that has intricate patterns, capturing the contours and accurate face measurements, recognizing the unique voice patterns based on the sounds generated and one's rhythmic voice, and analyzing one's behavioural traits such as walking/typing/signature style etc. [24].

2.1 Biometrics Systems Applicability in Cybersecurity

The integration of biometric technology into cybersecurity frameworks was a significant technological achievement that reduced the risk of unauthorized access and strengthened security. While there are lots of applications for biometric systems, the most used are:

a. Access Control and Authentication

One of the basic uses of biometric systems in cybersecurity is to make sure that only authorized users can access sensitive systems, devices, networks, and even physical premises or facilities. On the other hand, ***biometric authentication*** provides greater security because it uses unique individual traits to confirm a person's identity. This is achieved by comparing individuals' biometric data, such as fingerprints, facial patterns, and retinal scans, with their previously enrolled biometric data [4]. Passwords and PINs, one of the traditional authentication methods, are no longer secure as they used to be in the past and are susceptible to cyberattacks such as social engineering, phishing, and credential theft, as well as the risk of being forgotten or, in the case of access cards, getting lost or stolen [20]. With biometric authentication, these challenges are addressed, and an additional advantage of using biometric technology for physical access control by organizations is its use as a time-and-attendance system to clock in and out of office time, along with identity verification, which also addresses the issue of proxy attendance [4].

- Facial recognition systems - To unlock devices and identify users in public spaces.
- Iris scans - To provide a high level of security for access control in high-risk areas, such as government buildings or financial institutions.
- Fingerprint-based systems - To secure office environments via usage in smartphones, banking apps [24].

In banking, access and transaction authorizations for customer accounts, and criminal identification to control access across borders, are used in law enforcement, with advanced biometric systems.

b. Insider Threat Detection

As the world advances in digital and artificial intelligence (AI) technology, there is a significant surge in global cyber threats across businesses and governments. Although the top three threats are phishing, social engineering, malware/ransomware, and AI-driven attacks, a significant challenge for organizations and businesses is insider threats. There is a significant risk associated with insiders due to the high level of trust and access to systems and devices they have, which can be misused by them or through stolen/compromised credentials [5].

Insider threat detection thereby becomes one of the critical applications of biometric systems, though often overlooked. Even with security systems in place to monitor network traffic and user behavior, it is difficult to determine whether any malicious activity occurs, as legitimate system access and subtle activities carried out by insiders can mimic malicious behavior. With biometric systems, a user's unique behavior when typing is difficult to replicate, thereby protecting system access [5]. Keystroke or mouse movements can identify anomalies or deviations from an individual's regular interaction style. Organizations can combine traditional authentication with behavioral biometrics to detect real-time suspicious activities post user identity verification.

c. *Continuous Authentication*

Continuous authentication, one of the applications of biometric systems, focuses on verifying a user's identity on a continuous basis throughout their interaction with the system, instead of verifying just at the access point [24]. Continuous authentication is used to monitor users' identity continually via context-based, biometric, and behavioral real-time information and detect any anomalies [22]. Leveraging AI technology can further enhance the process to determine the perceived threat level by dynamically providing real-time assessments for any unusual activity and requesting additional verification methods for the user's authorized access or automatically logging out the user [24]. Usage of this approach enhances security by detecting **session hijacking**, where an attacker is likely to steal a user's session once they have logged in, or **piggybacking and spoofing**, where someone tries to gain access using another user's credentials [22]. It is particularly useful in sensitive environments, where any kind of unauthorized access to systems can lead to serious repercussions [24].

Continuous biometric verification helps in reducing such vulnerabilities by monitoring the user's behavior and building a profile of the user's normal behaviors to be compared with a standard reference for any future activities. The behavioral pattern check includes checking **gait** (walking patterns), **typing patterns**, **location of access**, **voice patterns**, or **facial recognition** over time, to ensure that the person interacting with the system is the one who initially logged in.

2.2 Cyber Crimes/Challenges/Cyber-attack Preventive Strategies related to Biometric Systems

Biometric systems have been in use since ancient civilizations. In recent years, technological advances have enabled advanced layers of security, but they are not resistant to cyberattacks. The risk associated with these attacks is quite high, as biometric data is private and permanent for an individual.

a. *Types of cyberattacks on biometric systems*

- **Data Breaches and Identity Theft** - Biometric data once stolen or leaked cannot be reversed, as fingerprints, faces, etc., cannot be reset unless the system uses template protection or cancelable biometrics to allow the storage of transformed data. In 2015, the U.S. Office of Personnel Management (OPM) experienced a major data breach compromising the personal data of 21.5 million individuals, including SSNs (social security numbers), fingerprints, interview records, and login credentials. [23].

Prevention – Such attacks can be prevented through **secure, encrypted storage** methods to protect biometric data [16].

- **Impersonation Attacks** using fake biometric traits of individuals and pretending to be that specific person, and gain unauthorized access [16]. Data is often obtained via social engineering and user manipulation.

- **Spoofing Attacks** using fake biometric information like photographs for facial recognition systems, fake fingerprints, 3D masks, or deepfakes to fool the system [19]. Obtaining these fake data to attackers is made easier by users, for example, by leaving fingerprints on doorknobs, posting personal photos on social media, and images captured in cameras being made available in public places [26]. Spoofing attacks have become quite common with the advent of AI and easy access to AI and machine learning (ML) tools to generate deepfakes, like the researchers at New York University developed "DeepMasterPrints" synthetic fingerprints mimicking individuals' prints to deceive fingerprint sensors [21]. Another type of spoofing attack is a **Wolf attack**, where biometric samples are matched with the registered templates and used to fool the biometric authentication system [26].

Germany's Chaos Computer Club in 2013 hacked the latest model of iPhone, then released using a fingerprint, which was photographed from a glass surface, to authenticate the user and access the phone [6]

- **Replay Attacks** by reuse of captured biometric data obtained indirectly, either via secretly recording the voice or from photos in a public forum/social media, to authenticate as the legitimate user and gain access control of the system [16, 26].
Prevention – Enabling **multi-factor authentication (MFA)** by combining biometric authentication with other modes such as **time-sensitive tokens** or **secured sessions using token expiration** like OAuth can further enhance security [16].
- **Inverse Biometrics** by reverse engineering of stored biometric templates to reconstruct the original biometric data, thereby compromising user privacy and security, which can potentially generate data to successfully authenticate the user [18].
- **Hill climbing attack** targets physiological biometrics systems stored as a template by constructing a biometric input and gradually refining until it is falsely accepted and authenticated into the system [4].
Prevention - A countermeasure to prevent this attack is to **restrict the number of authentication attempts** and reduce the likelihood of false acceptance and successful iterative exploitation [4].

b. Other cyber-attack prevention strategies on biometric systems

Other cyber-attack prevention strategies to address the cyber-attacks on biometric systems include:

Intrusion Detection Systems (IDS) – IDS implementation can help prevent potential attacks by identifying suspicious activity and alerting system or application administrators to respond immediately [16]. Quick actions can help minimize the risk of escalated attacks or compromised systems.

Vulnerability Analysis – Identifying potential attack vectors and fixing vulnerabilities, using methods such as attack trees, and informing the need for designing better, more secure systems [19]. Regular vulnerability assessments and penetration testing to understand system weaknesses, and address these weaknesses through patch management, keeping systems and applications up to date with critical version upgrades or service packs, and deploying vulnerability fixes can help minimize attacks before attackers can exploit them.

Liveness Detection – Facial spoofing with high-resolution photographs or video clips can bypass facial recognition systems if they lack proper liveness detection mechanisms powered by ML algorithms. Liveness detection verifies whether the captured biometric sample is from a live person rather than a spoofed source by looking for specific behavioral or biological cues, such as eye movements, heartbeat detection, facial expressions, and variations in skin texture [26]. For example, dynamic facial recognition systems can verify a user's identity based on their smile, eye blink, and other facial cues.

c. Challenges of biometric systems

Environmental and Sensor Limitations – Environmental factors can affect how accurately the biometric systems works, like facial recognition systems can potentially give a false negative while identifying individuals under poor lighting conditions, or fingerprint scan can fail if the captured data of the user's hands were dirty, wet, or injured. Iris scanning can also be affected by individuals wearing glasses or contact lenses, glare or lighting, or by critically ill patients [10, 24]. These can make biometric systems less reliable in real-world scenarios, underscoring the need for regular user training to ensure appropriate interaction with the system.

Privacy Concerns and Data Breaches – Though biometric systems provide enhanced security, there are lots of **privacy concerns**, as these systems deals with personal & permanent information of an individual which can be compromised [20, 24]. Identify theft or malicious activities on an individual's biometric data due to data breach or loss cannot be reset. This is a major concern due to the growing trend of centralized biometric databases and the likelihood of potential breach. The risks associated with informed consents provided by individuals to collect, store, process, or potentially getting exposed due to breach of biometric data are not fully understood. It would be deemed important for organizations to adhere to stringent **data protection regulations** for how biometric data should be handled, processed, and stored, like the **EU General Data Protection Regulation (GDPR)**, California Consumer Privacy Act (CCPA) etc. [24]. In India, Aadhaar, used for personal identification, is integrated with multiple apps and services to verify users' identities. Although this integration is quite convenient, there is a good amount of uncertainty for individuals whose data is shared, as they are unaware of how secure their data is and for what purposes the platforms or services that use their biometric information are being used.

Cost and Integration Challenges – The cost associated with implementing and maintaining biometric systems is quite high due to the initial infrastructure investments,

subsequent maintenance, training, and business needs, which require a cost-benefit analysis before implementing and deploying these systems [24]. The infrastructure required includes high-resolution sensors, software for capturing/ storing/ processing/ matching biometric data, and secure storage systems, which are expensive.

These systems and applications, which need to switch to biometric authentication, must be integrated with existing IT infrastructures. In such situations, especially with legacy systems, biometric system compatibility [24] can pose a challenge for infrastructure setup and management.

2.3 Trends and Emerging Technologies in Biometric-based Systems

Technological advancements in the digital era also include biometric system enhancements to make the system more reliable, usable, accurate, and convenient [10]. These include:

a. Multi-Modal Biometric Systems

To address the ever-evolving threats, a combination of different biometric modalities like facial/palm recognition, iris scans, fingerprint, and voice recognition potentially offers a reliable, accurate, and higher level of security. An increased authentication accuracy resulting from a multi-modal biometric system would be less negative or false positives/acceptance rates [10]. Such systems thereby become more suitable where there is a need for highly secure environments like banking, healthcare, government services such as law enforcement, military, and border access [24]. Multimodal biometric systems offer significant advantages over unimodal systems by addressing various limitations such as noisy data, questionable sample size, intra-class variations, low error rate, non-universality, poor robustness, and spoof attacks associated [8, 9]. The value additions of multimodal biometric systems include reducing the acceptance or rejection rates, being a means of verification, identification, and resilience against attempts to spoof biometric systems [8].

b. Artificial Intelligence (AI) and Machine Learning (ML) in biometrics

AI algorithms can reduce false positives/negatives in user verification and in detecting patterns/ anomalies in a biometric system, thereby enhancing the system's accuracy and reliability. This is achieved due to the seamless integration of AI into biometric systems and its ability to learn/train itself from available data, thereby improving decision-making and the ability to identify individuals [24]. AI/ML advancement, such as Convolutional Neural Networks (CNNs), adapts to changes of an individual's physical appearance due to aging, environmental/lighting variations, or any other style/pose changes, thus ensuring long-term accuracy, making the system smarter and quicker to respond based on user behavior [26].

c. Integration with IoT devices

One of the latest trends in biometric systems is its integration with the Internet of Things (IoT) to secure everything from smart home devices to wearable technology, such as user authentication to access smart locks, personal health devices, and fitness trackers [24]. This also helps to address privacy concerns as the biometric data template and hashes can be stored, processed, and secured on IoT devices locally [2]. Continuous,

secure, and real-time authentication can be done with biometric sensors using heart rate or ECG liveness detection for wearable devices. In the healthcare industry, IoT-based solutions help with remote patient monitoring, and their integration with AI-powered biometrics ensures reliable access control and enhanced privacy to patient data, in addition to patient identification and provisioning them with appropriate treatment. The transportation industry and smart cities with biometric implementation benefit due to secure vehicle access and improved urban security, with user privacy, respectively, while military and government organizations are considering an additional authentication layer with DNA technologies.

d. Gait analysis – behavioral biometrics

Gait recognition is one of the behavioral biometrics that analyzes how a person walks by performing image analysis to extract unique walking features or collect walking data such as duration and number of steps, and is also used to assess whether an individual has musculoskeletal injuries and arthritic disorders [13]. In the context of a biometric system for cybersecurity, gait analysis can identify and authenticate an individual based on their unique walking style captured by sensors, machine vision, or wearable devices [13]. Though this method is accepted and includes non-invasive data collection, it faces challenges due to environmental factors and potential security vulnerabilities.

Table 1: A Comparative view of the various biometric authentication approaches

Authentication Approaches	Security Strength	Spoof Resistance	Deployment Cost	Key Limitations
Unimodal Biometrics	Moderate	Low–Moderate	Low	Vulnerable to spoofing & noise [7], [8], [26]
Multi-Modal Biometrics	High	High	High	Complexity, scalability [8], [9], [24]
Liveness Detection	High	High (varies)	Medium	Challenged by deepfakes [19], [26]
Biometric + MFA	Very High	Very High	Medium–High	Usability overhead [16], [26]
AI-based Continuous Auth.	High	Moderate–High	High	Resource intensive [2], [5], [22]

Comparative View

Various studies have consistently shown that multimodal biometric systems perform better than unimodal systems for authentication [26]. Integrating multiple biometric modalities with other biometric authentication approaches reduces FAR (False Acceptance Rate), FRR (False Rejection Rate), and ERR (Equal Error Rate), not only provides accurate results under different environmental conditions but is also quite robust [9, 14, 26]. Overall system reliability is enhanced with multimodal fusions, thus compensating for weaknesses in individual modalities [8], which is further confirmed

by studies carried out on a fingerprint and facial recognition multimodal system that achieved 98.2% accuracy with 1.0% EER, outperforming fingerprint-only (96.7%, EER 1.5%) and face-only systems (94.8%, EER 2.2%) [14].

With recent studies on AI-enhanced and continuous authentication approaches, it has been demonstrated that AI-powered biometrics for IoT security has improved accuracy and liveness detection [2, 22], and deep learning-based authentication can detect insider threats in critical infrastructure by analyzing behavioral patterns [5]. User authentication in real time with continuous authentication frameworks leverages multimodal signals and AI monitoring, moving towards a future with multi-factor biometric systems that are intelligent and adaptive, complementing the traditional multimodal fusion with AI, liveness detection, and behavioral monitoring [2, 5, 14, 22].

Given emerging technologies and the cybercrimes associated with biometric systems, Table 1 provides a critical comparative overview of biometric authentication approaches, including their strengths, resistance to spoof attacks, and implementation costs.

2.4 Synthetic Biometrics

When handling sensitive personal data, there are challenges in preserving privacy when using the data for analysis or mining to extract details. Other associated challenges include preventing data misuse to ensure fair and impartial decisions, avoiding community discrepancies, and improving data quality for better data mining and decision-making. Any dataset used for analysis that cannot be extracted for utility purposes with minimal effort to obtain the required knowledge or take appropriate decisions is considered to be of poor quality. Having a complete representative and diverse dataset with appropriate anonymity is considered to be of good quality and can be utilized to address the challenge associated with handling privacy vs. utility of data, and misuse of personal data [17]. Techniques like synthetic data, encryption, obtaining informed consents from individuals, legal measures, and other privacy-enhancing technologies are used to prevent data misuse.

Synthetic biometrics is all about generating artificial biometric data, often referred to as synthetic data, which mimics the characteristics of real biometrics and can be used to prevent data misuse. Another application of synthetic biometrics is training the users and testing the biometric systems, thereby enhancing system performance [28]. Over the period synthetic biometrics evolved from mathematical modeling to data-driven neural generative models, conditional generative adversarial (CTGAN) models enabling the creation of synthetic data and improving their realistic properties to help address privacy concerns, minimize any biases associated with dataset, and reduce the efforts required to obtain the diverse samples for large-scale evaluations that can include various modalities like iris scans, facial patterns, fingerprints, and vascular patterns [17, 18]. The most important aspect to be considered is the quality of data generated and models such as CTGAN have components like conditional vectors, which guarantee the data quality that is diverse and can be modelled to address potential security threats [17, 18].

Another advantage of using synthetic biometrics is addressing the anonymity aspect, which is a limitation with real biometric data. Synthetic biometrics creates data samples of virtual individuals that can be exposed to public databases without any legal

concerns. This enables synthetic biometric datasets to be used for research purposes, training, testing, and evaluation of systems with diverse samples and attributes like gender, age, ethnicity, etc., thus protecting the exposure of real biometric data for mining or analysis [18]. Other security-enhancing mechanisms include privacy-enhancing technologies such as cancelable biometrics, which transform real biometric data into a secure form that, even if stolen, will not compromise the original data and can be transformed again to safeguard the data. The stolen data cannot be restored to its original state without the transformation key.

Advancements in Synthetic Biometric Data

The use of synthetic biometric data is found to be viable for realistic authentication use, implying gains in terms of data privacy, availability, and efficiency. The study conducted in 2022 by Grosz and Jain, called SpoofGAN [11], demonstrated the utility of both live and spoof synthetic fingerprints to detect spoofing by training the data set with synthetic data and proving that in most scenarios, only 25% of real data was required to obtain the required detection. Few studies have generated fingerprints based on architectures with a conditional GAN. Use of CGAN showcased a 99.47% acceptance rate, preserving privacy and identities with no significant data leakage [1]. Healthcare applications leverage adversarial network techniques to generate biometric synthetic data from faces, irises, and fingerprints that minimizes the risk of data leakage by protecting sensitive information [15]. UserBoost – a system in the behavioural biometric domain demonstrated that synthetic data specific to user gestures can ease the operational overhead and limit the need for real user data by around 40% without impacting the system performance [27].

Research Gap

Despite the availability of solid empirical evidence on the use of synthetic biometric data providing better performance for preserving privacy using fingerprints, other biometric domains, and behavioral biometrics, which can support spoof detection, there is no literature available that integrates synthetic biometric data with the different modalities of biometric systems' to offer enhanced security and mechanisms with which the system can continuously learn and improve itself, to enable detection and prevention of cyber-attacks.

Although each component is validated by prior research, the combination of these components provides an opportunity to address the study's scope and offers a timely contribution to research and business.

3 Research Methodology

3.1 Research Design and Data Collection

This research adopted a qualitative, analytical, and exploratory research approach, with an aim to understand the biometric systems utilization in cybersecurity, data privacy, synthetic biometrics, and privacy-preserving authentication. Due to the exploratory nature of the study, insights are obtained from existing literature [25] and highly credible industry reports and sources online to identify the latest trends,

emerging technologies, opportunities, challenges, and verifiable evidence of real-world incidents associated with the use of biometric-based security systems.

Data Collection and Search Strategy

Secondary data used for this research were collected online from academic databases, including Google Scholar, ResearchGate, IEEE, Scopus, ScienceDirect, and reputed professional and government portals such as Wired, Financial Crime Academy, OPM, Ping Identity, and Chaos Computer Club. The search was conducted by combining multiple keywords to ensure complete coverage, including the following:

- Biometric systems: “biometric systems in cybersecurity”, “behavioral biometrics”.
- Synthetic biometrics: “synthetic biometrics”, “synthetic data”, “inverse biometrics”, “privacy-preserving biometrics”.
- Security threats: “spoofing attacks”, “cyber-attacks”, “adversarial attacks”.
- Trends and applications: “biometric systems trends in cybersecurity”, “cybersecurity threats in biometric systems and authentication”.

The news articles were selected based on their publication years, limited to 2024-2025, to capture current trends, developments, and emerging real-world threats. The search criteria included publication years set from 2005 to 2025 for peer-reviewed journals, books, and conference proceedings to include the foundational literature and recent studies.

Inclusion and Exclusion Criteria

The sources reviewed included studies based on the keyword clusters provided in the search criteria and relevant information available in the context of standards, regulatory guidance, and highly credible incident reports. The sources were screened in a staged process, inspired by PRISMA guidelines, with the initial relevance screening conducted by reviewing the titles and abstracts of the returned results. The next stage involved evaluating the full text of the contents to review their quality, methodology, and thematic contribution in alignment with the study scope, and finally identifying and coding the relevant themes emerging from the study.

Contents related to studies on medical biometrics (except for synthetic data) with no relevance to cybersecurity and non-technical articles with opinions from experts, and marketing-related content were excluded. Publications with duplicated information and those that were incomplete were also excluded.

3.2 Thematic Analysis

The selected literature was analyzed using Braun and Clarke’s six-phase thematic analysis [3], starting with getting familiar with the data sources from data collection to identify initial patterns, followed by initial coding and grouping them into themes. Initial coding was conducted based on key ideas extracted from the literature, including spoofing, cyberattacks, AI-related threats, vulnerabilities of biometric modalities, liveness detection techniques, continuous and behavioral authentication, privacy regulations, ethical considerations, and synthetic biometric generation and use. The grouped themes were further reviewed and finalized during the final synthesis step for integration into the proposed conceptual framework.

4 Analysis, Findings and Discussions

Thematic analysis was carried out by identifying themes from the findings, including the threat landscape in biometric-authentication systems, security mechanisms and countermeasures, emerging technology applications of biometric systems, policies and compliance, and synthetic biometrics. In conjunction with the research questions, Table 2 summarizes the study's findings.

Table 2: Data analysis - Theme mapping to research questions

Theme	Mapped to RQs	Key Findings
Threat Landscape in Biometric-Authentication Systems	RQ1: Applications and limitations in detecting / preventing cyber-attacks	<ul style="list-style-type: none"> • Spoofing, AI-driven impersonation, breach of data, and identity theft are common threats. • Biometric systems, though effective, are vulnerable to evolving attack vectors like deepfakes and AI/ML technologies.
Security Mechanisms and Countermeasures	RQ1: Limitations & Prevention and RQ2: Trends/Technologies	<ul style="list-style-type: none"> • Use of liveness detection, anti-spoofing, encryption, and multi-modal biometrics • Cloud storage and real-time anomaly detection systems are becoming more common.
Emerging Technology Applications of Biometric Systems	RQ2: Latest trends and technologies in biometric-based cybersecurity	<ul style="list-style-type: none"> • AI, and cloud platforms are reshaping biometric systems. • Integration with other digital infrastructures (e.g., IoT, mobile apps) is expanding biometric authentication scope.
Policy and Compliance Implications	RQ1 & RQ3: Data Privacy, Limitations, and Breach Risk	<ul style="list-style-type: none"> • Regulatory frameworks (GDPR, BIPA) are becoming stricter. • Ethical concerns around surveillance, consent, and fairness.
Synthetic Biometrics	RQ3: Use of synthetic biometrics to protect privacy and reduce breaches	<ul style="list-style-type: none"> • Use of AI to generate synthetic biometric data reduces breach impact. • Protects actual biometric traits while enabling authentication.

Threat Landscape in Biometric-Authentication Systems

While biometric authentication provides a strong, reliable, and secure method of protection against unauthorized access, it remains a target for attackers who are rapidly

evolving their techniques, threats such as spoofing, data breaches, identity theft, and by adapting to technological advancements like AI and deep-fake technologies, to exploit vulnerabilities in these systems. As biometric systems are now being integrated into sensitive areas such as finance, healthcare, and government services, the impact of cyber-attacks on these systems is greater, and the likelihood of escalation is higher, underscoring the need for robust, adaptive security measures.

Table 3: Comprehensive view of the various attack types, countermeasures and their effectiveness

Attack Type	Description	Countermeasures	Effectiveness	Limitations
Spoofing	Use of fake biometric traits (photos, masks, recordings)	Liveness detection	High	Can be challenged by advanced deepfakes
AI/Deepfake Attacks	AI-generated biometric impersonation	AI/ML-based anomaly detection, Liveness detection	Medium–High	Requires continuous model updates
Data Corruption (Storage/Transmission)	Tampering with biometric data in transit or at rest	Encryption, secure storage	High	Key management complexity
Identity Theft	Unauthorized use of stolen biometric data	Cancelable biometrics, multi-modal biometrics	Medium	Increased system complexity
Unauthorized Access to Sensitive Systems	Attacks on finance, healthcare, and government platforms	Multi-modal biometrics, real-time monitoring	High	Higher processing and usability overhead

Security Mechanisms and Countermeasures

The threats and attack vectors associated with biometric systems require layered security, the major ones including liveness detection, anti-spoofing technologies, AI/ML-based anomaly detection, cancelable/multi-modal biometrics, and secure, encrypted storage. While the attackers are evolving with the technologies, organizations should also ensure they implement security measures and be ready to swiftly adapt to the evolving technologies and have real-time monitoring and adaptive systems that can self-learn/self-heal/self-protect from each attack. While significant technological advances help detect and prevent, there is a need to consider the balance required for security and ease of use of these systems, to avoid processes and systems getting slowed down. Table 3 summarizes the effectiveness of these countermeasures against key attack vectors.

Emerging Technology Applications of Biometric Systems

AI, ML, Cloud solutions, blockchain, etc., are the emerging technologies that can enhance biometric systems and the authentication/authorization process. User recognition/verification accuracy can be improved with AI/ML models, given the large datasets available for training. With blockchain technology, biometric data can be decentralized and securely stored, thereby minimizing the risks of data breaches or theft associated with centralized databases. However, the new technologies, such as cloud-based and AI-driven systems, present new attack surfaces, challenges associated with technical scalability, and ethical concerns around informed consent, profiling, surveillance, and algorithmic bias, which must be addressed via governance and ethical frameworks.

Policy and Compliance Implications

Biometric data being highly sensitive, must focus on data privacy-related regulations and be compliant with data protection frameworks such as the EU GDPR, BIPA (Illinois Biometric Information Privacy Act), etc., in terms of data storage and transmission policies. Moreover, the difference in privacy laws and data protection requirements across borders necessitates the biometric designs to follow guidelines as per international standards and ensure compliance. Regulatory and compliance bodies should also ensure that the policies are refined and reviewed regularly to address the potential scope for cyber-attacks with the rapidly growing technological advancement, and also to address ethical adoption across to ensure issues around bias, data ownership, and consent are taken care of.

Synthetic Biometrics

Synthetic biometrics is definitely one of the futuristic approaches to protect biometric data from privacy-related risks. The two distinct purposes of using synthetic data are to support the training and testing of AI models in the event of a system or data breach, to protect individuals' identities, and to enable privacy-preserving authentication, which can revolutionize secure authentication. Considering that the data is created from virtual or non-existent individuals, synthetic biometrics is useful.

- ***Training and Testing for AI models:*** Synthetic biometric data is an alternative to limited real-world datasets, enhancing the robustness and generalizability of AI-based models [17,18,21,28]. The generation of diverse and distinct biometric variations with the synthetic datasets helps prevent overfitting, improve model accuracy, and minimize data scarcity issues, thus reducing dependency on sensitive personal data. DeepMasterPrints [21] demonstrated how AI-generated fingerprints could be used to train models for improved recognition performance. Although it is an effective approach for model development, synthetic data should be mimicked to reflect real-world scenarios, considering all aspects of real-world scenarios, to minimize biases, glitches, and unrealistic patterns that could degrade system performance or model outcomes.
- ***Privacy-Preserving Authentication:*** Synthetic biometrics enable systems to authenticate users without storing or exposing individuals' personal and sensitive biometric templates [17,18], which can be used to verify user

identity. Organizations can use this technique to reduce the risk of biometric templates being leaked or stolen, thereby addressing key privacy and compliance concerns. Although integration challenges such as avoiding false rejections and maintaining realistic information exist. Synthetic templates must be secured and maintained to prevent attackers from exploiting and predicting the synthetic patterns generation process [18,19].

Although synthetic biometrics technology is still emerging, it has its own advantages, and any implementation using it is not without risks. Over-reliance on synthetic data could reduce system resilience if real-world variations are not completely represented. Additionally, there are risks posed by adversaries targeting AI systems with synthetic data through adversarial attacks [26]. Considering the advancements in technology and the need for standardization, validation, and clarity regarding compliance/regulatory aspects, this approach ensures greater trust and adoption. Successful adoption of the technology requires careful integration with real biometric modalities, robust liveness detection, and secure handling protocols to ensure both accuracy and privacy, although there are downsides resulting from the evolutions in AI/ML, which can be used to generate data in bulk and trigger spoofing attacks or for malicious purposes. Additionally, the distinctions between training/testing uses and operational privacy-preserving applications must be accounted for and implemented appropriately to avoid any confusion with stakeholders regarding system capabilities and limitations. Care should be taken to ensure that frameworks are incorporated that can detect bias and can also be used for audit.

5 Proposed Conceptual Framework

As part of the study, a high-level conceptual framework (depicted in Figure 2) has been proposed to guide future research incorporating user perspectives.

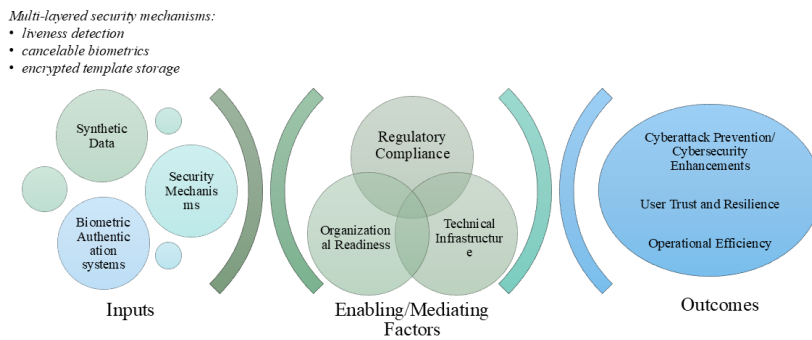


Fig. 2: Proposed Conceptual Framework

The framework concludes that this has been part of the findings and conceptualizes biometric authentication systems (fingerprint, facial/iris/voice recognition, gait, etc.) and synthetic data (virtual user identities) as multi-layered security mechanisms. With the multi-layered security approach, the physiological and behavioral biometric modalities interact with liveness detection, synthetic data, and security mechanisms

used to detect threats, ensuring regulatory compliance, organizational readiness, and availability of infrastructure as an enabler. The framework specifies the contribution of each component towards resilience and does not assume that biometrics alone can increase user trust. The biometric inputs provided by users are first verified for liveness to prevent spoofing attacks, while synthetic biometric templates support privacy-preserving authentication, ensuring no real biometric data is exposed to the outside world or attackers.

The interactive components in the framework depicted in figure 3, entails the use of AI/ML models for continuous monitoring to detect anomalies, adversarial attacks, and insider threats, in compliance with regulatory policies and data privacy standards, to provide a feedback mechanism and carry out system configuration updates by learning on a continuous basis, in case any attacks or incidents are detected. The holistic integration and interactions of the framework, based on the thematic analysis outcomes, explain how biometric systems can enhance security, improve user trust, and provide privacy safeguards that are also visible to users, thereby improving organizational resilience and operational efficiency. The policy and governance framework is horizontal across the entire framework, and the feedback mechanism primarily supports retraining the AI models, updating the generation of synthetic data parameters, and the thresholds for liveness detection.

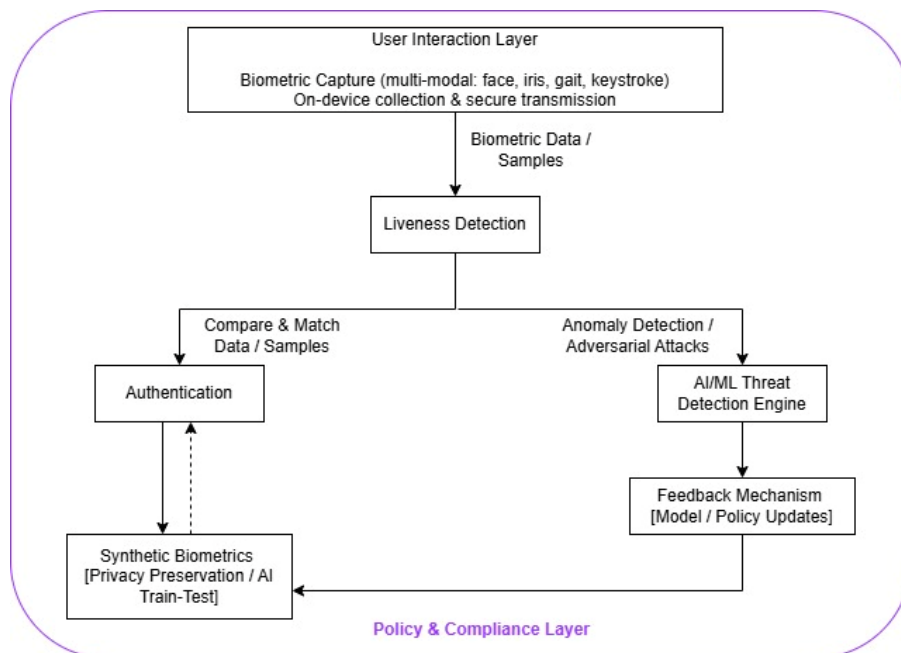


Fig. 3: Interactive components entailed in the proposed conceptual framework

The model proposed in this study provides a foundation for designing the system and for future empirical research that can enable researchers to derive testable hypotheses based on the propositions listed below:

Propositions for future research based on the proposed conceptual framework:

- P1: Biometric systems that are set up with multilayered security mechanisms, such as liveness detection, threat modeling, and continuous feedback, are more effective at detecting and preventing cyber threats than single-layer systems.
- P2: The use of privacy-preserving synthetic biometric templates increases user trust by reducing concerns about biometric misuse and identity theft.
- P3: Biometric systems with multilayered security mechanisms with explicit user-facing visual indicators and data privacy safeguards increase user trust and acceptance rates
- P4: The combined use of synthetic biometrics and multilayered security enhances security, trust, and efficiency compared to traditional biometric systems.

These would also help practitioners and businesses understand how to integrate biometric components securely, responsibly, and in compliance with global regulatory standards.

6 Conclusion and Research/Business Contributions

The research started with an objective to study the current state of biometric-based systems for detecting and preventing cyber-attacks and to understand the privacy-preserving biometric techniques that can be leveraged to address privacy concerns. As part of the study, it was revealed that biometric-based systems are one of the most powerful systems due to their inherent uniqueness to defend systems from cyberattacks and also provide preventive measures to address password breaches. These systems, though, are inherently used to prevent unauthorised access, are not immune to cyber-attacks and evolving threats like spoofing, identity theft, or template inversions and thus need to be resilient enough to adapt to the evolving technological advancements and incorporate protection mechanisms. Some of the challenges arising from technical vulnerabilities can be addressed by ensuring the systems have robust multi-modal and behavioural biometrics implemented, though any kind of implementation should also consider the trade-off required in terms of ease of use/operation of the system and enabling security. Some of the strategic implementations that can be considered to enable multi-layered security mechanisms include liveness detection with tracking eye/body movement, heartbeats, etc., cancelable biometrics, and encrypted template storage. These defence mechanisms, if clubbed with strong governance and regulatory compliance in alignment with the data privacy and protection laws, can lead to growth in the use of biometric systems in all of the modern cybersecurity landscapes. One important aspect to be considered is infrastructure scalability, and adaptation to the latest technological advancements should be one of the key determining/enabling factors.

While technologies such as AI/ML, edge computing, blockchain, and cloud architectures are transforming all business operations, integrating with biometric systems can enhance protection against cyberattacks. AI/ML technologies revolutionize synthetic biometrics, generating virtual data as required across different modalities for testing and training various systems. These generated data serve as a privacy-preservation technique, as they don't reveal individual identity, thereby

offering a privacy-first design approach, and can be integrated with biometric encryption.

The existing literature provides insights into components such as biometric and different layered authentication architectures, synthetic biometric data generation, and privacy-preserving learning. However, the research gap in the absence of an integrated approach across these components remains, especially given that applications and organisations are opting for biometric technologies and that there is a huge demand for biometric systems, thereby creating high-risk, data-sensitive environments.

The study proposes a conceptual framework to address the gap, integrating the major aspects of this research, offering a novel theoretical foundation of biometric systems with a focus on balancing security and privacy without degrading the performance:

- ***Synthetic biometric data*** to reduce privacy risk, address data scarcity, and support scalable system development.
- ***Multilayered biometric security*** systems for a resilient system to detect and prevent cyber-attacks.
- ***Feedback mechanisms*** for continuous learning and system improvement, to build user trust, and enhance operational efficiency.

Overall, while biometric systems used for authentication and authorization are one of the powerful frontiers in cyber defense, the effectiveness of this system totally depends on having innovative approaches on a continuous basis to enhance the systems ethically to safeguard an individual's personal identity data, while in alignment with all the government, regulatory and privacy-focused policies. The conceptual model thereby offers a theoretical foundation with propositions for future innovations and research in this technologically evolving field. It is a pretext to ensure that biometric security systems become among the sought-after, secure, robust, trustworthy, and adaptable systems in the complex cyber landscape.

6.1 Contributions to Business and Research

Business Contribution

The study provides insights into the use of biometric systems like fingerprint, facial recognition, voice, etc., as single or multi-modal options, synthetic biometrics and how these can be used for cybersecurity to detect and prevent cyber-attacks, which can be leveraged by businesses to strengthen their defence mechanisms against threats such as spoofing, identity theft, etc. Businesses adopting biometric authentication and integration of the same with IoT devices, AI/Cloud, which can detect threats in real-time and smartly prevent any misuse of the devices, can enhance their customer experience. Study emphasises that organizations should not limit the usage of these systems only for compliance and security, instead, leverage the aspects of sensitive information protection and focus on building user trust, improving operational efficiency, and being resilient by adapting and adopting to the ever-changing technology and threats. Further organizations building systems and products utilising synthetic biometrics in privacy preservation with the latest technologies can be a differentiator in the market and obtain a competitive advantage, due to strong authentication and data privacy offerings.

Research Contribution

In the context of research, the study provides an ample amount of information with respect to biometric systems, current trends in this technology, and how it can be leveraged in cybersecurity. The literature review conducted collates a good amount of information on various threat landscapes, including the latest technological ones like AI-based deepfakes, prevention mechanisms, including the various means to protect individual identity data and user privacy, with the integration of synthetic biometrics. It also identifies emerging gaps in existing literature in terms of privacy-preservation of user identity and provides avenues for future research scope. The study also covers the latest emerging technological trends, such as AI/ML, blockchain, edge computing, etc., and enhances biometric-based cyber defense mechanisms.

6.2 Limitations of the study and Future scope

The current study is based on secondary data sources, looking at the available papers and articles online, so the insights obtained are predominantly based on their accuracy and currency. No primary data via surveys or interviews were collected since this study is based solely on secondary data. There would have been additional hands-on research, experiments, and technical implementations that were conducted in a lab environment, which are not considered or for which the results are not available on public forums.

Future Scope

From a future perspective, research can be carried out to prove the theories proposed as part of the study in conjunction with the proposed framework, and additionally, in the following areas, apart from including the demographic, inclusivity, and accessibility aspects, the results of which are likely to differ and provide actionable insights for business and researchers to provide a secure solution in terms of biometric devices and processes.

- To study the perceptions of users on their trust in AI-made decisions based on deep-learning biometric systems that analyze behaviors/gait
- To understand user comfort in operating/accessing the biometric systems that conduct continuous authentication/monitoring, and to understand
- To study user awareness on the use of synthetic data, either as part of training or security, and understand their perceptions on the trust in the usage of the system and its impact on privacy preservation.
- To experiment with integrating multimodal approaches with synthetic data and enable researchers to compute FRR, FAR, and ERR comprehensively and in a structured manner, thereby helping simulate, analyze, and prevent potential cyberattacks.
- The study can be further expanded as interdisciplinary research for biometric authentication, converging legal in the context of privacy laws, ethical in the context of data surveillance and usage, and social dimensions in the context of how the users use the systems and what they perceive or have experience in terms of trusting or continuing to use these systems.

Acknowledgments

The authors would like to express their sincere gratitude to the University and their supervisor for providing the opportunity to conduct this research and for their continuous guidance, insights, and encouragement throughout the study.

Funding

The authors have received no funding for this research study, and this is an academic project.

Conflicts of interest

The authors declare no conflict of interest in this research study.

Data availability statement

No data has been collected from any users as part of this study.

Author contribution statement

Author 1 has conceptualized the study, research methodology, and conducted the analysis.

Author 2 has provided their guidance, review feedback, and inputs at each stage of the study.

References

- [1] Abbas, S. K., Purnapatra, S., Murshed, M. G. S., Miller-Lynch, C., Igene, L., Dey, S., Schuckers, S., & Hussain, F. (2025). *Conditional Synthetic Live and Spoof Fingerprint Generation*. arXiv preprint arXiv:2510.17035. <https://arxiv.org/abs/2510.17035> (arXiv)
- [2] Awad, A. I., Babu, A., Barka, E., & Shuaib, K. (2024). AI-powered biometrics for Internet of Things security: A review and future vision. *Journal of Information Security and Applications*, 82, 103748.
- [3] Braun, V., & Clarke, V. (2006). *Using thematic analysis in psychology*. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- [4] Boonkroong, S. (2021). Authentication and Access Control. *Berkeley, CA: Apress*, 133-162.
- [5] Budžys, A., Kurasova, O., & Medvedev, V. (2024). Deep learning-based authentication for insider threat detection in critical infrastructure. *Artificial Intelligence Review*, 57(10), 272. <https://doi.org/10.1007/s10462-024-10893-1>
- [6] Chaos Computer Club. (2013, September 22). *Chaos Computer Club breaks Apple TouchID*. <https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid>
- [7] Debas, E. A., Alajlan, R. S., & Rahman, M. M. H. (2023). Biometric in cyber security: A mini review. In 2023 International Conference on Artificial Intelligence in

Information and Communication (ICAIC) (pp. 570–574). IEEE.
<https://doi.org/10.1109/ICAIC57133.2023.10067017>

[8] Dargan, S., & Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Systems with Applications*, 143, 113114. <https://doi.org/10.1016/j.eswa.2019.113114>

[9] Farik, M. (2016). A review of multimodal biometric authentication systems. *International Journal of Scientific & Technology Research*, 5(4), 5–9.

[10] Financial Crime Academy. (2025, March 14). *Game-changing technology: The advancements in biometric authentication systems*. Financial Crime Academy. <https://financialcrimeacademy.org/biometric-authentication-systems/>

[11] Grosz, S. A., & Jain, A. K. (2022). *SpoofGAN: Synthetic Fingerprint Spoof Images*. arXiv preprint arXiv:2204.06498. <https://arxiv.org/abs/2204.06498> (arXiv)

[12] Gupta, H., & Chauhan, K. (2015). Role of biometric security for the enhancement of data security. *International Journal of Computers & Technology*, 14(10), 6184–6189. <https://doi.org/10.24297/ijct.v14i10.1832>

[13] Gupta, P., Singh, R., Katiyar, R., & Rastogi, R. (2011). Biometrics system based on human gait patterns. *International Journal of Machine Learning and Computing*, 1(4), 389–392.

[14] K. Varshney, A. Chelse, A. Parasher, S. K. Tomar, and R. Paul, “Digital identity management using biometric systems: BioTrace,” *Journal of Information Systems Engineering and Management*, vol. 10, no. 51s, 2025. [Online]. Available: <https://www.jisem-journal.com/>

[15] Khadidos, A. O., Manoharan, H., Khadidos, A. O., Selvarajan, S., & Singh, S. (2025). *Synthetic healthcare data utility with biometric pattern recognition using adversarial networks*. *Scientific Reports*. <https://doi.org/10.1038/s41598-025-94572-3> (PMCID: PMC11928505) (Nature)

[16] Kumar, S. (2024). *Biometric Systems Security and Privacy Issues*. 68–91. <https://doi.org/10.1201/9781032614663-4>

[17] Majeed, A. (2023). Attribute-centric and synthetic data based privacy preserving methods: A systematic review. *Journal of Cybersecurity and Privacy*, 3(3), 638–661.

[18] Makrushin, A., Uhl, A., & Dittmann, J. (2023). A survey on synthetic biometrics: Fingerprint, face, iris and vascular patterns. *IEEE Access*, 11, 33887–33899. <https://doi.org/10.1109/ACCESS.2023.3250852>

- [19] Marasco, E., Shehab, M., & Cukic, B. (2016). A Methodology for Prevention of Biometric Presentation Attacks. *Latin-American Symposium on Dependable Computing*, 9–14. <https://doi.org/10.1109/LADC.2016.13>
- [20] Nebreda, P. (2023, March 21). The role of biometrics in cybersecurity: Threats and solutions. Alice Biometrics
- [21] Newman, L. H. (2018, November 17). Machine learning can create fake ‘master key’ fingerprints. *Wired*. <https://www.wired.com/story/deepmasterprints-fake-fingerprints-machine-learning/>
- [22] Ping Identity. (n.d.). *What is continuous authentication?* <https://www.pingidentity.com/en/resources/identity-fundamentals/authentication/continuous-authentication.html>
- [23] U.S. Office of Personnel Management. (n.d.). *Cybersecurity Resource Center*. Retrieved April 20, 2025, from <https://www.opm.gov/cybersecurity-resource-center/#url=Cybersecurity-Incidents>
- [24] Ughade, N. (2025, February 26). *Future of biometrics: Trends, innovations, and challenges ahead*. HyperVerge. <https://hyperverge.co/blog/future-of-biometrics/>
- [25] Ugwu, C. N., & Eze, V. H. U. (2023, January 18). *Qualitative Research*. *ResearchGate*. https://www.researchgate.net/publication/367221023_Qualitative_Research
- [26] Wang, X., Yan, Z., Zhang, R., & Zhang, P. (2021). Attacks and defenses in user authentication systems: A survey. *Journal of Network and Computer Applications*, 188, 103080.
- [27] Webber, G., Sturgess, J., & Martinovic, I. (2024). *UserBoost: Generating User-specific Synthetic Data for Faster Enrolment into Behavioural Biometric Systems*. arXiv preprint arXiv:2407.09104. <https://arxiv.org/abs/2407.09104> (arXiv)
- [28] Yanushkevich, S. (2006). Synthetic biometrics: A survey. In *2006 International Joint Conference on Neural Networks* (pp. 676–683). IEEE. <https://doi.org/10.1109/IJCNN.2006.246749>