Biometrics For User Authentication

Name: Mukesh Kumar [6893549]

COMM047 Secure Systems and Applications

1/15/25

DECLARATION OF ORIGINALITY

I confirm that the submitted work is my own work. No element has been previously submitted for assessment, or where it has, it has been correctly referenced. I have clearly identified and fully acknowledged all material that should be attributed to others (whether published or unpublished, and including any content generated by a deep learning/artificial intelligence tool, and have also included their source references where relevant) using the referencing system required by my course or in this specific assignment. I agree that the University may submit my work to means of checking this, such as the plagiarism detection service Turnitin UK and the Turnitin Authorship Investigate service. I confirm that I understand that assessed work that has been shown to have been plagiarised will be penalised.

UNI: 6893549

Abstract

Biometric authentication systems have gained significant attention due to their potential to enhance security and improve user experience by eliminating password management challenges. This paper presents a comprehensive in-depth analysis of biometric authentication techniques with a primary focus on privacy-preserving and secure identification. While existing systems employing static and dynamic biometric features demonstrate varying degrees of usability and accuracy, they remain influenced by various attacks, such as spoofing and replay attacks. Critical evaluation reveals that fingerprint and iris recognition methods excel in terms of accuracy, though iris recognition demands additional hardware and raises privacy concerns. Dynamic feature-based systems, despite offering continuous authentication and aliveness detection, suffer from lower accuracy and usability.

Balancing performance criteria, such as accuracy, efficiency, usability, privacy, and security, remains a significant challenge. High-accuracy systems tend to reduce efficiency due to longer processing times, while systems prioritizing usability may compromise security.

1.1. Introduction

User authentication is an important process it is used when someone wants to gain access to the protected system or service whether it is a system or a service online. This procedure aims to guarantee that whoever is trying to access is really the person they are pretending to be. There are three primary forms of authentication processes in today's known systems in the world today. The first is knowledge-based authentication that entails verifying the user's identity through something which includes a password or a PIN. This method as suggested earlier is a widely used one since it is simple and easily can be incorporated with different systems. The second type of the authentication is what you possess such as a smart card, an access key or token. This method is often applied in situations where the conditions of security are envisioned at a higher level. Third, we have biometric authentication where users are verified using features that are specific to them like fingerprints, face, or voice Biometrics.

Biometric authentication systems have steadily risen in popularity because of their capability to give user experience that is both easy and secure. This is unlike Knowledge based and possession-based methods which utilize attributes that can be erased, misplaced or even stolen while Biometrics affix the identification process to the user's genetic specifications. Such a difference established biometric system as less vulnerable to particular areas of security threats inclusive of theft or forging of the credentials. However, as it shall be noticed above, there are apparent benefits of using biometrics which also bring new and complex issues of privacy and security. Because biometrics data is a fixed and unchangeable that cannot be altered once it has been breached makes the proper handling and storage of this information to become a very difficult issue. Biometric databases based on centralized IT systems are most at risk of cyberattacks, and their violations may have critical consequences for privacy and may take years to resolve for victims.

2.1. BIOMETRIC AUTHENTICATION SYSTEM OVERVIEW

A biometric authentication system consists of three core components: the User Interface (UI), the Identity Provider (IdP) and the Relying Party (RP). It is through the UI that the user communicates to appeal for an authentication process, in the case of applications, and secured gadgets. Depending on the kind of biometric system, some of the features on the UI are capturing ones fingerprints, face or the iris of the eye. The function of the IdP is to confirm the authenticity of the user based on the biometric data captured in the hand-held device and compared with the templates kept in a database. The IdP processes the biometrical data, and if the match is found, the identity of the user is confirmed. Depending on the type of the authentication result the RP allows/denies the user access to the requested services or information.

Basically, this process starts when a user clicks on the button and demands an authentication process through the UI. The UI then triggers an authentication process by communicating and connecting securely with the IdP. On acceptance of the request, the IdP initiates a challenge that involves the collection of the user's biometric data by the UI sensor. The UI takes up the data activities such as removing noise and

quantization of data, as well as other operations, occur at this level – and engages the IdP in answering the challenge.

The IdP then processes the data submitted through application of the data processing techniques and matches it with records stored in the database. As a result of comparison, the IdP either verifies the identity of a user or denies it. As soon as the authentication decision is communicated to the RP optimum security measures to the resources are secured.

Biometric authentication systems can be developed in different modes.

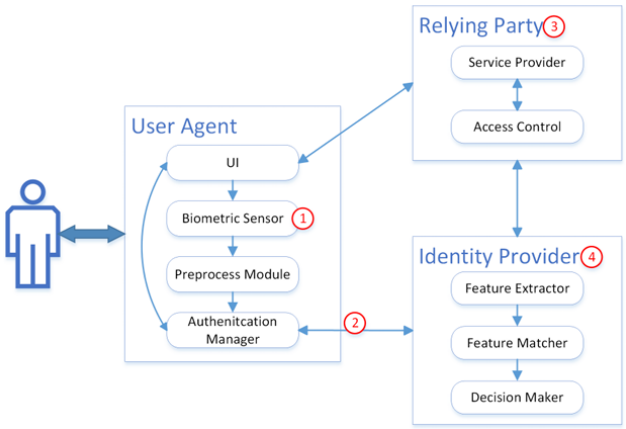
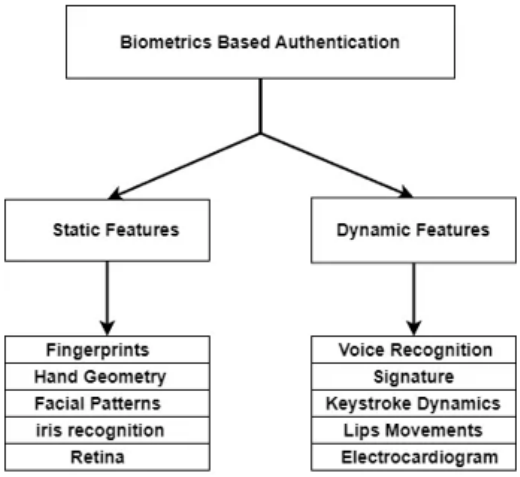


Figure 1: System workflow

While in other settings the RP and IdP are part of a local area to the extent that authentication can be done offline. Other systems work in the cloud when both the RP web service and the IdP web service reside on different web servers and use network connection with the user device. Furthermore, the RP and IdP can be controlled by different organization that benefits from having some of the aspects such as connection links that may be made weak, the exposure of data exchange that may be made vulnerable.

2.2. BIOMETRIC AUTHENTICATION TYPES

Figure 2.2: Types of Biometrics



Biometric authentication systems can be broadly classified into two categories, those based on static features and those based on dynamic features. Static features, such as fingerprints, facial patterns, and iris recognition, offer high stability over time, resulting in greater accuracy. However, they often susceptible to spoofing attacks. In contrast, dynamic features, including voice recognition, electrocardiogram (ECG) signals, and keystroke dynamics, allow for continuous authentication and exhibit improved resistance to forgery, as they depend on behavioural characteristics that are difficult to replicate. Nonetheless, the reliability of dynamic features can fluctuate due to environmental factors and variations in user behaviour.

Fingerprint recognition is one of the earliest biometric models to gain widespread adoption, particularly in law enforcement and consumer technology. It provides high accuracy and cost-effectiveness, making it a popular choice for mobile devices and security systems. Despite its widespread use, fingerprint authentication remains vulnerable to spoofing through the use of high-quality fake fingerprints. To address this vulnerability, modern systems have incorporated liveness detection, which verifies the presence of genuine, live skin. For instance, Apple's Touch ID employs capacitive sensors and machine learning algorithms to enhance detection accuracy.

Facial recognition, another prominent biometric technology, has gained popularity through smartphone applications like Apple's Face ID. This technology offers hands-free and rapid authentication, enhancing user convenience. However, it is prone to spoofing using photos, masks, or videos. To counteract these vulnerabilities, recent advancements have focused on integrating depth sensors and employing machine learning models capable of detecting live faces through subtle facial movements. Nonetheless, facial recognition raises significant privacy concerns, as facial data can be easily captured without user consent, potentially leading to misuse and unauthorized surveillance. Privacy-preserving approaches, such as differential privacy and homomorphic encryption, are being explored to safeguard user data while maintaining functionality.

Iris recognition, noted for its exceptional accuracy, is commonly employed in high-security environments such as government institutions and border control systems.

Unlike fingerprints and facial recognition, iris patterns are more resistant to spoofing due to their complexity and uniqueness. However, iris recognition systems require specialized hardware, such as near-infrared cameras, and controlled environmental conditions, limiting their applicability in everyday scenarios. To improve usability, research efforts are focusing on developing less intrusive hardware and more adaptable algorithms that function effectively under varying lighting conditions.

Behavioural biometrics, such as voice recognition and keystroke dynamics, offer alternatives to static methods, particularly for continuous authentication. Voice recognition provides hands-free convenience but is vulnerable to spoofing through recorded playback. Security can be improved using multi-factor authentication and challenge-response protocols. Keystroke dynamics analyse typing patterns based on timing and rhythm, offering a non-intrusive form of verification. However, its accuracy may vary due to factors like fatigue or stress. Despite these limitations, it remains a promising, cost-effective solution for enhancing security in online platforms and remote work.

Multi-modal biometric systems, which combine multiple biometric models, have emerged as a powerful solution to the limitations of single-modal systems. By integrating different biometric traits, such as fingerprints and facial recognition, multi-modal systems enhance accuracy, usability, and spoof resistance. For example, systems combining fingerprint and face recognition offer improved security by requiring verification through two distinct modalities, making it significantly harder for attackers to bypass both simultaneously.

2.3. POTENTIAL RISKS IN BIOMETRIC AUTENTICATION

Faking the Sensor

One of the primary vulnerabilities in biometric authentication systems is the potential for faking the sensor. This type of attack involves substituting the real biometric feature with a forged one, such as a fake fingerprint, a photo for face recognition, or a recorded voice sample. Unlike traditional network security attacks, this form of attack does not require technical skills for breaching the system’s network but instead relies on physical manipulation of the biometric input. The ease with which attackers can fabricate biometric data poses a significant security risk, especially in user terminals, which are often less protected than server-side systems.

Resubmitting Biometric Signals

Another critical threat to biometric authentication is the risk of resubmitting previously captured biometric data. In this type of attack, the attacker intercepts biometric signals such as a fingerprint or a facial image during the registration or authentication process. Once the data is obtained, the attacker can replay it during a subsequent authentication attempt, bypassing the system's verification process. This type of attack highlights the need for robust protection during both the transmission and storage of biometric data to prevent unauthorized reuse.

Common Network Attacks on Servers

Biometric authentication systems often depend on centralized servers where the identity provider (IdP) and relying party (RP) are housed. These systems are vulnerable to traditional network attacks, such as hijacking, SQL injection, and privilege escalation. In these cases, attackers gain unauthorized access to the server, potentially compromising biometric data or obtaining additional sensitive information about legitimate users. If attackers manage to access a user’s biometric information, they could use it maliciously in other contexts, increasing the overall risk of identity theft and fraud.

Attacks on Face Recognition

Face recognition systems are particularly vulnerable because face images and videos can be easily obtained, even from publicly accessible platforms such as social media. In some cases, attackers do not need to steal photos directly from users, they can capture images from the internet or use photos taken without the

user's knowledge. This accessibility makes face recognition systems highly susceptible to impersonation attacks.

Attacks on Iris Recognition

While iris recognition systems are generally more secure due to the difficulty in replicating the unique patterns in an individual's iris, they are still vulnerable to attacks. With the advancement of high-resolution cameras, it is possible to capture an image of an iris from a distance and use it to deceive the system. However, such attacks are typically more expensive due to the specialized optical equipment required, making them less common than attacks on other biometric systems.

Attacks on Fingerprint and Palm-print Recognition

Fingerprint and palm-print recognition systems are among the most commonly used biometric methods, but they are also highly vulnerable to spoofing. Fake fingers can be made using materials such as silica gel, latex, or even gelatin. Additionally, attackers can collect fingerprint data from surfaces that users have touched, making it relatively easy to reproduce biometric information without the user's consent.

Attacks on Electrocardiographic (ECG) Signals

While ECG-based biometric systems are relatively difficult to spoof, they are not immune to attack. ECG signals must be collected using specific electrodes or sensors, making it harder for attackers to intercept these signals without the proper equipment. However, since ECG signals are not as commonly used in mainstream biometric systems, the risks associated with them are lower compared to other biometric systems.

Attacks on Voice Recognition

Voice recognition systems are another biometric method that is vulnerable to attacks. Because voice data is relatively easy to collect, attackers can record a user's voice and replay it during an authentication attempt. This type of attack, known as a spoofing attack, can often bypass voice recognition systems, particularly if the system does not incorporate features like liveness detection.

Attacks on Keystroke and Touch Dynamics

Keystroke and touch dynamics are behavioural biometrics that rely on the user's typing or touch patterns. While these methods can be difficult to imitate due to the individual nature of each person's typing rhythm and touch behaviour, they are still vulnerable to statistical attacks. These attacks can involve analysing typing patterns over time to identify and mimic the user's behaviour.

3.1. EVALUATION CRITERIA

Biometric authentication systems are becoming essential in contemporary security frameworks, particularly in sectors demanding strong identity verification. These systems hold unique biological and behavioural traits to ensure that access is restricted to legitimate users. The expansion of biometric systems across industries, including mobile devices, banking, healthcare, government identification, and border security, highlights their expanding role in modern society. While they provide superior security and user convenience, biometric systems present inherent challenges in terms of accuracy, reliability, usability, privacy, and vulnerability to spoofing.

Accuracy

The accuracy of a biometric authentication system is a critical factor in its performance evaluation. Several metrics are used to measure accuracy, including the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). FAR represents the likelihood of an impostor being falsely accepted as a legitimate user, while FRR reflects the probability of a legitimate user being incorrectly rejected. The EER is the point where the FAR and FRR are equal, and a lower EER generally indicates a more accurate system. A biometric system's accuracy is crucial because it directly impacts its reliability and effectiveness in authenticating users.

Efficiency

Efficiency measures how quickly a biometric authentication system can perform the entire authentication process, including data collection, processing, feature extraction, and decision-making. Systems with high efficiency are able to provide quick responses, ensuring that users do not experience delays during authentication. Efficiency is particularly important in real-time applications, such as mobile devices or access control systems, where speed is a key factor for user satisfaction and system performance. The faster the system can authenticate users without compromising accuracy, the better its overall usability.

Usability

Usability in biometric authentication systems refers to how effortlessly users can engage with the technology, highlighting user experience, accessibility, and adaptability across a diverse user base. It encloses several critical factors, such as universality (UV), which ensures that the biometric method is applicable to a wide range of users by guaranteeing that most individuals possess the required traits. Uniqueness (UQ) is crucial for accurately distinguishing one individual from another, while permanence (PM) ensures that biometric traits remain stable over time to maintain consistent system accuracy. Acceptability (AC) involves user willingness to adopt the system, considering how biometric data is collected and used. Moreover, systems should not require additional equipment (EE) beyond commonly available devices. A system that scores highly on usability can be widely adopted, ensuring smooth operation, convenience, and practicality in everyday use.

Security

Security is a critical evaluation standard for biometric authentication systems. A system should be able to resist various types of attacks, such as spoofing or replay attacks, where an attacker tries to impersonate a legitimate user by presenting forged biometric data. The system must be designed to protect against such vulnerabilities and ensure that only legitimate users can gain access. A secure biometric system should employ techniques like liveness detection, encryption, and secure data storage to prevent unauthorized access to sensitive biometric information. The system's ability to withstand attacks without compromising user privacy or data integrity is vital for its success.

Privacy

Privacy protection is a critical aspect of biometric authentication systems due to the highly sensitive nature of biometric data. Key factors in ensuring privacy include mission success rate (MSR), which refers to the system's ability to safeguard biometric information against unauthorized access or exposure. Non-invertibility (NI) is essential to prevent stored biometric data from being reverse-engineered or reconstructed, ensuring that attackers cannot recover original biometric traits even if the database is compromised. Revocability (RV) allows users to revoke or replace compromised biometric templates and register new ones, ensuring that stolen data cannot be reused. Unlinkability (UL) ensures that users' biometric data cannot be linked to their real identity across different platforms or services, enhancing anonymity. Effective privacy measures are necessary to secure biometric data throughout its lifecycle, including during collection, storage, and transmission, thereby minimizing the risk of unauthorized access or exposure, even in case of a breach.

Table 3.1: EVALUATION CRITERIA

Biometric Feature	FAR	FRR	EER	Performance	Accuracy	Efficiency	Usability	Security	Privacy
Fingerprints	L	L	L	H	H	H	H	H	M
Hand Geometry	M	M	M	M	M	M	M	M	L
Facial Patterns	M	M	M	M	M	M	H	M	L
Iris Recognition	L	L	L	H	H	L	M	H	M
Retina	L	L	L	H	H	L	L	H	M
Voice Recognition	M	M	M	M	M	M	H	M	M

Signature	M	M	M	M	M	M	H	M	M
Keystroke Dynamics	M	M	M	M	M	M	M	M	M
Lips Movements	H	H	H	L	L	L	M	M	L
Electrocardiogram	L	L	L	H	H	M	M	H	M

4.1. Relationship between features (such as conflicting to, complementing and supporting to)

Accuracy Vs Efficiency

Accuracy and efficiency are two essential yet occasionally conflicting features in biometric authentication systems. While high accuracy ensures precise identification, it often results in slower processing, thereby reducing efficiency. This trade-off is particularly evident in systems such as iris recognition, where achieving maximum precision requires high-resolution image capture and complex analysis, leading to increased computational demands and reduced responsiveness. Similarly, in ECG-based authentication, maintaining high accuracy involves sophisticated signal processing and extended data analysis, which can slow down the system's real-time performance. As higher accuracy typically requires more detailed data and complex algorithms, efficiency may suffer, especially in time-sensitive applications.

Despite these conflicts, accuracy and efficiency can complement each other when advanced technologies and optimization strategies are applied. Fingerprint recognition systems illustrate this complementarity, as they achieve both high accuracy and efficiency through well-developed algorithms that deliver quick and reliable results. Machine learning and deep learning methods further help bridge the gap, enabling high accuracy with reduced processing times through optimized feature extraction and parallel processing. These technological improvements demonstrate how the relationship between accuracy and efficiency can evolve from conflict to complementarity.

In specific contexts, accuracy and efficiency can support and rely on each other. Multi-modal biometric systems, which combine different biometric traits, improve both accuracy and efficiency by reducing re-authentication attempts and minimizing errors. This integration streamlines the authentication process and enhances system performance. Furthermore, in high-security environments, where real-time authentication is crucial, systems that can quickly and accurately verify users not only ensure operational efficiency but also prevent delays and bottlenecks, proving that these two features, when properly balanced, can work in harmony.

Security Vs Privacy

Security and privacy are two intertwined yet distinct features in biometric authentication systems, each serving to protect users and their sensitive data. Despite their shared objective, these features can sometimes conflict. Enhancing security often involves centralizing biometric data in databases for better control, yet this centralization increases the risk of privacy violations if a breach occurs. Similarly, robust security measures like encryption and access control may require more detailed processing and storage of biometric data, potentially compromising user privacy. Multi-modal biometric systems, which combine different biometric traits for improved security, exemplify this trade-off by increasing the volume of sensitive data collected, thereby heightening privacy concerns.

Nevertheless, security and privacy can also complement one another. Strong security mechanisms such as encryption safeguard the privacy of biometric data by preventing unauthorized access during transmission and storage. Additionally, privacy-enhancing technologies (PETs), including template protection and cancellable biometrics, allow systems to achieve both privacy and security. These methods ensure that even if biometric data is compromised, it remains unusable to attackers, thus balancing both objectives. Moreover, techniques like de-identification reduce identifiable information, thereby supporting privacy without weakening security.

In practice, security and privacy often rely on each other in environments that require stringent data protection. Privacy by design frameworks, for example, ensure that systems are inherently secure by minimizing data exposure and anonymizing sensitive information. User-consent models further reinforce this relationship by giving individuals control over their data, limiting unauthorized access and improving overall security. Consequently, a well-designed biometric system can achieve a synergy between security and privacy, ensuring that both features work in tandem to protect users and their data.

Security Vs Usability

Biometric authentication systems often face a trade-off between security and usability, as measures designed to enhance protection can reduce user convenience. Strengthening security frequently requires additional authentication steps, such as multi-factor authentication or advanced liveness detection, which make the process longer and more demanding for users. For instance, systems requiring precise positioning during iris recognition provide robust security but can frustrate users due to the high degree of precision required. Similarly, measures designed to prevent spoofing, like requiring users to interact with sensors in specific ways, improve security at the expense of usability, leading to slower and more error-prone interactions.

However, when thoughtfully designed, security and usability can complement each other. Systems that integrate user-friendly interfaces with secure protocols can achieve both goals simultaneously. Fingerprint authentication is a prime example, offering a high level of security alongside ease of use. Adaptive systems that vary authentication requirements based on the context of use can also strike a balance—demanding stricter measures for sensitive actions while allowing quicker methods for routine tasks enhances both user satisfaction and protection. These strategies demonstrate that, under the right conditions, security can coexist with usability.

In some implementations, security and usability not only complement each other but also support one another. A system that is easy to use encourages consistent and proper engagement from users, ensuring that security protocols are adhered to more frequently. For example, a well-designed face recognition system that functions reliably across different environments fosters habitual use, reducing the likelihood of incorrect authentications and missed verifications. Furthermore, continuous authentication systems operate in the background, maintaining security without active user input, thereby maximizing both usability and protection. This synergy between security and usability ensures a seamless, efficient, and secure user experience.

5.1. Challenges and Difficulties of Building the Trade-offs or balances Between

Accuracy and Efficiency

Balancing accuracy and efficiency in biometric authentication systems presents a significant challenge due to the inherent trade-offs between these two objectives. High accuracy requires advanced algorithms, detailed data collection, and precise analysis, all of which increase computational time and reduce efficiency. For example, face recognition systems that aim for high precision rely on high-resolution images and advanced matching techniques, resulting in slower processing. Similarly, prioritizing efficiency often involves simplifying data collection and algorithmic complexity, which can lead to reduced accuracy and increased error rates. In resource-constrained environments, such as mobile devices, this trade-off becomes particularly pronounced due to limited processing power and energy consumption.

Technological advancements, such as deep learning models, offer a potential solution to this dilemma by improving accuracy across various biometric methods. However, these models demand significant computational resources, delaying authentication and consuming power. Simplified algorithms, while faster and more energy-efficient, may struggle to handle variability in biometric traits, such as lighting or aging effects, resulting in compromised reliability. Multi-modal biometric systems, which integrate multiple traits like fingerprint and face recognition, provide enhanced accuracy but reduce efficiency due to increased data processing requirements. Thus, balancing the two features remains an ongoing technological challenge.

Hardware limitations further complicate this balance. High-accuracy systems require advanced sensors that capture detailed data but slow down the process, whereas optimized hardware for faster performance often sacrifices detail, reducing accuracy. Dynamic and adaptive systems offer a promising approach by adjusting security levels based on context, ensuring efficient processing for routine tasks while switching to higher-accuracy modes when necessary.

Security and Privacy

The relationship between security and privacy in biometric authentication systems is often conflicting. Security ensures that only legitimate users can gain access, but this typically requires the storage and transmission of sensitive biometric data, which raises privacy concerns. Centralized databases, for instance, enhance security by enabling quick and accurate verification but increase the risk of privacy breaches. Once compromised, biometric data cannot be reset like traditional passwords, making privacy violations particularly harmful. Similarly, advanced security measures, such as multi-modal biometrics that use multiple traits for authentication, improve resistance to attacks but require more personal data, heightening the risk of misuse.

However, security and privacy can complement each other when carefully integrated. Privacy-enhancing technologies, such as anonymization and template protection, help safeguard personal data without compromising security. Encryption techniques, particularly homomorphic encryption, enable secure data processing while preserving privacy by keeping biometric data encrypted throughout its lifecycle. These measures ensure that even if data is intercepted, it remains unusable to attackers, thereby maintaining both privacy and security.

Furthermore, systems designed with user consent and data control in mind reinforce the balance between these two features. User-centric models allow individuals to manage their biometric data, ensuring that privacy is respected while maintaining high security. Template protection methods that transform biometric data into non-reversible forms prevent unauthorized access and data misuse. By integrating privacy-by-design principles, biometric systems can create a framework where both security and privacy are inherent, ensuring robust protection while fostering trust among users.

Security and Usability

Balancing security and usability in biometric authentication systems is a significant design challenge, as improving one often comes at the expense of the other. Security aims to prevent unauthorized access, but high-security measures such as multi-factor authentication (MFA) can create a more cumbersome experience for users. For example, systems requiring both fingerprint and facial recognition improve protection but reduce usability by making the authentication process slower and more difficult. Similarly, liveness detection steps, such as blinking during face recognition, add complexity, potentially leading to user frustration if the system is unresponsive or error-prone.

However, security and usability can complement each other when systems are designed with user convenience in mind. A single biometric model, such as fingerprint recognition, strikes a balance by offering both quick authentication and robust security. While less secure than multi-modal systems, it provides an appropriate level of protection for low-risk scenarios, such as unlocking a smartphone. Adaptive security models can further enhance this balance by adjusting authentication requirements based on context.

Security and usability also support each other by encouraging consistent usage. A user-friendly system promotes trust and compliance, ensuring that users follow security protocols rather than seeking less secure alternatives. Additionally, systems that prioritize usability improve accuracy by reducing user errors, indirectly strengthening security. User training and education can also enhance both features by fostering an understanding of the importance of security without compromising usability.

6.1. Existing and New Possible Solutions for Biometrics for user authentication

Accuracy and Efficiency

Existing solutions for balancing accuracy and efficiency in biometric authentication systems have focused on

optimizing algorithms and system design to achieve a workable trade-off. Techniques like feature extraction and dimensionality reduction, using methods such as Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA), help enhance efficiency by reducing the amount of data processed while preserving key features for high accuracy. In face recognition, for example, PCA-based approaches like Eigenfaces allow for quick processing by focusing on critical facial landmarks, improving real-world applications without significant loss of precision. Similarly, multi-stage classification systems, such as cascade classifiers, increase efficiency by using lightweight models in the initial stages and applying more complex ones only to potential matches, ensuring both speed and accuracy.

Template matching optimization plays a crucial role in fingerprint recognition systems. Minutiae-based techniques focus on key fingerprint features, balancing accuracy with computational efficiency. Advanced hierarchical matching methods further improve performance by breaking down the matching process into smaller steps, ensuring quick yet reliable recognition. In real-time face recognition, deep learning models, particularly Convolutional Neural Networks (CNNs), deliver high accuracy but come with a computational cost. Techniques like quantization and model pruning reduce this burden, enabling efficient operation on mobile and embedded devices without compromising accuracy.

Emerging solutions offer new possibilities for overcoming the accuracy-efficiency trade-off. Edge computing reduces latency by performing initial data processing locally, enhancing efficiency while maintaining accuracy by offloading complex tasks to remote servers. Federated learning further enhances both privacy and efficiency by keeping data on user devices, transmitting only model updates to central servers. Neural Architecture Search (NAS) automates the development of optimal models for specific hardware, balancing performance with resource constraints. Zero-Shot Learning (ZSL) enables systems to recognize new identities without retraining, improving adaptability and reducing the need for frequent updates. Lastly, quantum computing and Vein Pattern, though still developing, holds the potential to revolutionize biometric systems by offering unparalleled speed and accuracy through parallel data processing.

Security and Privacy

Balancing security and privacy in biometric authentication systems has led to the development of several existing solutions aimed at protecting sensitive biometric data. Encryption remains one of the most widely used techniques for securing biometric data during transmission and storage. Symmetric encryption methods like AES and asymmetric encryption methods like RSA ensure that even if the data is intercepted, it remains unreadable. However, encryption alone cannot address all privacy risks, as it does not mitigate concerns related to biometric data storage and reuse. Template protection techniques offer a solution by storing mathematical representations of biometric data rather than raw data. Methods such as fuzzy vaults, cancellable biometrics, and homomorphic encryption prevent direct access to original biometric traits, enhancing privacy by ensuring that compromised templates cannot be reverse-engineered.

Local biometric processing has also emerged as a key strategy to reduce privacy risks by keeping biometric data on the user's device. Edge computing facilitates this approach, enabling fast, secure processing without transmitting sensitive data to centralized servers. Multi-factor authentication (MFA) further strengthens security by requiring multiple forms of verification, such as combining biometrics with a PIN or password, ensuring that even if biometric data is compromised, unauthorized access remains difficult. Additionally, anonymization and de-identification techniques are employed to remove personally identifiable information from stored data, allowing the use of biometric datasets for analytics without compromising user privacy.

New solutions for enhancing both security and privacy are also being explored. Federated learning enables model training on user devices without transmitting raw data, reducing privacy risks while maintaining system accuracy. Zero-knowledge proofs (ZKPs) provide a means of verifying a user’s identity without exposing their biometric data, ensuring secure and private authentication. Differential privacy adds statistical noise to biometric data, making it impossible to isolate individual users while preserving overall system functionality. Blockchain technology offers decentralized data management, enhancing both data integrity and user privacy by allowing users to control access permissions. Finally, secure multi-party computation (SMPC) enables joint biometric computations across multiple parties without exposing the underlying data, ensuring that privacy is maintained even during collaborative processes.

Security and Usability

Biometric authentication systems face a constant challenge in balancing security with usability. Single-factor authentication (SFA), such as fingerprint or facial recognition, offers high usability due to its simplicity and speed. However, it provides only moderate security, as biometric traits can be spoofed. Multi-factor authentication (MFA), by requiring additional verification such as a PIN, improves security but decreases usability, making it less appealing for users who prioritize convenience. Adaptive authentication helps bridge this gap by adjusting security requirements based on context. For instance, low-risk actions may require only a biometric scan, while high-risk transactions demand additional verification, ensuring an optimal balance between ease of use and robust security. Furthermore, the systems rely on optimized algorithms that deliver fast and accurate results. Advances in hardware have made it possible for these algorithms to run efficiently on devices such as smartphones, ensuring minimal delays.

Future solutions focus on achieving seamless integration of security and usability. Continuous authentication, which passively monitors user behaviour, ensures ongoing security without requiring repeated logins. Edge computing enhances real-time authentication by processing biometric data locally, improving both speed and privacy. Privacy-preserving models, such as those using biometric data masking and secure computation, protect sensitive information while maintaining usability by allowing secure remote processing. Behavioural adaptive authentication further enhances security by dynamically adjusting requirements based on user behaviour and risk levels. Optimized neural networks reduce the computational load while maintaining accuracy, ensuring that biometric systems provide secure and user-friendly experiences in real-time scenarios.

References:

[1] Z. Rui and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," in *IEEE Access*, vol. 7, pp. 5994-6009, 2019, doi: 10.1109/ACCESS.2018.2889996. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8590812

[2] B. Chesebro and M. B. A. Oldstone, "Neurological Disease and the Immune System," *Cold Spring Harbor Perspectives in Medicine*, vol. 3, no. 10, p. a010396, Oct. 2013. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC3787579/.

[3] R. Parkavi, K. R. Chandeesh Babu and J. A. Kumar, "Multimodal Biometrics for user authentication," *2017 11th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, India, 2017, pp. 501-505, doi: 10.1109/ISCO.2017.7856044

[4] A. Ricciardi, F. Maisto, A. Saggese, M. F. Ragosta, and V. Moscato, "Towards a Scalable Graph-based Approach for Fake News Detection," *arXiv preprint arXiv:2212.13187*, Dec. 2022. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/2212/2212.13187.pdf.

[5] Q. Wu, P. Mittal, C. Troncoso, and G. Danezis, "An Efficient Framework for Multi-Message PIR with Distributed Trust," in *Proceedings of the 29th USENIX Security Symposium (USENIX Security 20)*, Aug. 2020, pp. 717–734. [Online]. Available: https://www.usenix.org/system/files/sec20-wu.pdf.

[6] "A Survey on Biometric Authentication Toward Secure and Privacy-Preserving Identification," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 3, pp. 123-145, Sept. 2023. [Online]. Available: https://ijisae.org/index.php/IJISAE/article/download/6570/5420/11741.

[7] "Private biometrics," *Wikipedia: The Free Encyclopedia*, Dec. 8, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Private_biometrics.

[8] "Adaptive Authentication," *Silverfort Glossary*, Silverfort, [Online]. Available: https://www.silverfort.com/glossary/adaptive-authentication/.

[9] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125-143, June 2006. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=979d218385030c498416182a346cb5bef28a412b.