**Journal of Computer Science and Technology Studies**
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| **RESEARCH ARTICLE**

# Biometric Authentication-Risks and advancements in biometric security systems

**Gaurav Malik**
*Goldmaan Sachs, United States*

## | ABSTRACT

Biometric authentication is a fast-growing, novel technology that makes the identity verification process secure and user-friendly with unique physiological and behavioral indicators. The paper attempts to meet a theory on biometric systems' development, hazards and constraints by examining various biometric technologies like fingerprint, facial acknowledgement, iris checking, and behavioral biometrics. The integration of machine learning and artificial intelligence has made these systems more accurate and reliable, and hence, they can be used on mobile devices, banks, and border control. Since biometric authentication systems are beneficial, there are many risks, including privacy, data breaches, spoofing attacks and regulatory issues. While these risks are unavoidable as more and more organizations are embracing biometric systems, it is only right that data protection is strong, that legal frameworks are abided by, and that the practice is ethical. The paper explains the need to balance security and user convenience that takes care of the secure storage and transmission of biometric data and maintains compliance with evolving regulations. In addition, it stresses the importance of repeatedly observing and updating the biometric authentication systems to guarantee their integrity and security. Biometric authentication is poised to become a powerful tool for increasing security in many sectors. However, this success depends largely on considering different technological, legal and ethical factors to diminish any risks such a system might present.

## | KEYWORDS

Biometric Authentication, Security, Machine Learning, Data Protection, Privacy Concerns.

## | ARTICLE INFORMATION

**ACCEPTED:** 01 August 2024 **PUBLISHED:** 25 August 2024 **DOI:** 10.32996/jcsts.2024.6.3.14

## 1. Introduction

Biometric authentication describes a method for identifying or identifying an individual based on their unique physiological or behavioral characteristics. Biometrics do not depend on something the user knows but on something the user essentially has. The characteristics can vary from fingerprint patterns, iris scans, and facial recognition to behavior characteristics like typing patterns and vocal recognition. Biometric data has gained much popularity for authentication because it can increase security while improving the user experience. Biometric authentication is an advanced security technology based on the biological and behavioral traits of the person that can be measured to confirm identity. This method uses physiological traits, such as fingerprints, retina scan, face geometry, or behavioral features, such as voice and gait recognition. Physiological biometrics are more likely to be considered by biometrics because they are less susceptible to change over time. Behavioral biometrics are dynamic and can change throughout an individual's system. There are two major phases of interest in a biometric system – enrollment and verification. During enrollment, an individual's biometrics are captured and stored in a secure database specific to this individual. The system compares the captured data with information previously stored once the authentication process begins.

Biometric systems have quickly been developing, and they have been made possible by innovations in sensors, machine learning, and artificial intelligence (AI), which continue to make them more accurate and usable. Due to this, biometric authentication is becoming a viable option for applications such as unlocking smartphones and safe and secure financial transactions, and it is already being utilized in border control at airports. Cyber threats have become rampant, and securing valuable information is not taken for granted. While passwords and PINs are still good conventional security practices, many related attacks, including phishing, brute force, and social engineering, could undermine traditional security measures. Thus, these methods have come to be considered inadequate to protect high-value assets. Biometric authentication can serve as a much-needed solution, offering a more secure alternative with considerably greater convenience.

Biometric systems are just one of the main reasons they are good, thanks to which they can use two-factor authentication (2FA) without additional devices and tokens. For instance, facial recognition incorporated into a smartphone or laptop might automatically open it without pressing the 'Remember me' button. In addition, biometric identifiers are more difficult to copy or steal than traditional credentials. One thing cannot be guessed or phished; fingerprints or iris scans, for example, are a biometric characteristic unique to the individual and cannot be easily replicated. Thus, it significantly reduces the risk of identity theft, unauthorized access, and fraud. In addition, the expansion in the usage of frictionless security solutions in industries such as banking, healthcare, and government services is fueling the acceptance rate of biometric authentication. Organizations will be able to make their security more robust and the user experience better by using biometric technologies, which will reduce the need for passwords and PINs, which can be inconvenient and hard to control.

This paper provides a comprehensive study of biometric authentication and risk risks, as well as advancements and possible future developments of biometric security systems. The technologies of biometric systems will be considered and examined, and the technical, ethical, and legal challenges will also be addressed. In addition, this article will uncover some of the risks that come with this, such as privacy, spoofing attacks, and data breaches, which may defeat the effectiveness of these systems. Since biometric systems are increasingly used, it is important for both users and organizations that depend on these technologies to understand these risks and how to protect against them. The article will delve into the inroads in biometric security, including advanced AI Machine learning, and multi-factor authentication, which put these systems at increasingly greater accuracy and dependability. This article adopts the approach of providing real-world case studies and best practices so businesses and individuals can use this as a starting point when securely implementing biometric authentication. Biometrics is the path to the future of security with better protection, faster convenience for the end user, and a strong need to fight against the growing threat of cybercrime. However, its implementation will come; for that, you have to comprehend the technologies, problems, and the best approaches that will determine the future of digital security.

## 2. Overview of Biometric Authentication Technologies

In the modern world, biometric authentication has become the center of modern security systems. It offers a much more robust identity verification than the traditional password-based approach. Biometrics utilizes distinctive human attributes, such as physical and behavioral features, for authentication purposes, making it a more secure system for personal and organizational use. Today, the various biometric technologies available range from the application to the accuracy and complexity.

*Table 1: Overview of Biometric Authentication Technologies*

| Biometric Technology | Description | Pros | Cons | Common Applications |
|---|---|---|---|---|
| **Fingerprint Recognition** | Scans unique ridges and valleys on the fingertips | Fast, cheap, accurate | Vulnerable to spoofing, damaged fingers | Smartphones, law enforcement |
| **Facial Recognition** | Uses facial features (eyes, nose, jawline) to identify | Non-invasive, convenient | Privacy concerns, lighting-dependent | Mobile phones, security systems |
| **Iris and Retina Scanning** | Identifies based on iris color or retina blood vessels | High accuracy, stable over time | Expensive, uncomfortable | High-security areas, banking |
| **Voice Recognition** | Identifies based on voice features (pitch, tone) | Accessible, user-friendly | Susceptible to background noise, impersonation | Virtual assistants, customer service |
| **Behavioral Biometrics** | Analyzes behavior patterns like typing or mouse movement | Hard to replicate, real-time monitoring | Changes over time, health/behavior factors | Fraud detection, online banking |
| **DNA-based Authentication** | Uses unique genetic material for verification | Extremely secure | Expensive, privacy concerns | Forensic applications, high-security areas |

### *2.1 Fingerprint Recognition*

Fingerprint recognition is a very old and widely used biometric technology. Each person's unique pattern of ridges and valleys on his fingertip is taken, and it is then matched against a stored database of fingerprints to verify identity. Scanning the fingerprint using any of the optical, capacitive, or ultrasound sensors, each has its level of accuracy and speed (Iula, 2019). The fingerprint is created with a digital image with optical sensors or with the electrical properties of the skin with capacitive sensors. However, ultrasound sensors produce a 3D map of the print using sound waves.

Being fast, cheap, and relatively accurate, fingerprint recognition is commonly used in smartphones, security systems, and law enforcement applications. However, its limitations include vulnerability to spoofing using fake fingerprints and challenges for identification in cases when the person's fingerprints are damaged and worn. Despite these challenges, fingerprint recognition continues to be an important biometric technology in both the commercial and security sectors.

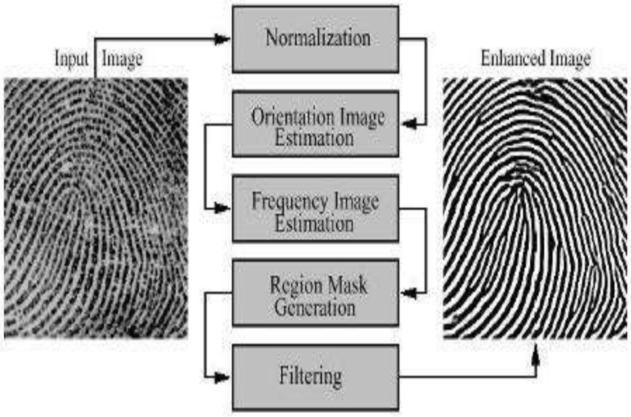

*Figure 1: Different Steps of Image Enhancement*

### *2.2 Facial Recognition*

Facial recognition technology uses facial features to uniquely identify a person – the distance between the eyes, the nose shape, and other jawline shapes. This technology uses high-performing algorithms to map these facial features and generate a biometric template to compare it with a stored database. The facial image is captured, and then it analyzes a distinguishing characteristic of the face and compares it against the database to verify identity.

Based on its non-invasive nature and convenience, facial recognition has become very popular because it does not need direct contact or intervention with the user (Jeon et al., 2019). This is also used in mobile and public surveillance security systems. However, the advantages of facial recognition have also been critiqued for violating privacy and exposing data security, as well as potentially misidentifying people not only in conditions of low lighting but also when individuals have similar facial features. Additionally, photographs and videos are susceptible to spoofing the technology. However, advancements in 3D facial recognition and liveness detection have helped alleviate some of the technology's vulnerabilities.

### *2.3 Iris and Retina Scanning*

Iris recognition and retina scanning are biometric authentication methods based on the eye that are extremely accurate in identifying people. Iris recognition analyzes the colored ring (iris) around the pupil. In contrast, retina scanning looks at the special pattern of blood vessels in the retina on the back side of the eye. The patterns of the iris and retina are unique to every person and do not change over a person's life, making both techniques very precise.

The iris and retina scanning technologies store biometric data–a high-resolution eye image captured by infrared light–and compare it with previously stored data to ensure the security and authentication processes. While fairly accurate, iris recognition is one of the most reliable biometric methods, as the patterns can be complex and unique. Nevertheless, the main limitation of iris and retina scanning is the requirement for sophisticated, costly hardware and entrepreneurial development, which may limit their reach and applicability (Ankerman, 2016). Also, some will have trouble with or experience discomfort while taking iris or retina scans.

### *2.4 Voice Recognition*

The main idea of voice recognition is to identify the identity based on the unique characteristics of an individual's voice. It goes through many voice features such as pitch, cadence, accent, and dynamics of speech, including rhythm and tone (Raju, 2017). All these factors lead to a unique vocal signature that can be used to verify the speaker. Phone systems, virtual assistants, and customer service applications are typical applications that use voice recognition (Kepuska & Bohouta, 2018).

The main benefit of voice recognition is that it is accessible for users who need to speak, and their identity is authenticated. However, voice recognition systems are not impossible to have problems with, as they are susceptible to environmental factors like background noise or poor audio quality, which can lower the technology's accuracy. Furthermore, voice recognition is prone to impersonation attacks wherein the malicious actor can provide a fake voice to another person. Voice biometrics is undergoing recent developments in liveness detection and deep learning algorithms, aiming to reduce risks and increase system reliability (Khade et al., 2021).

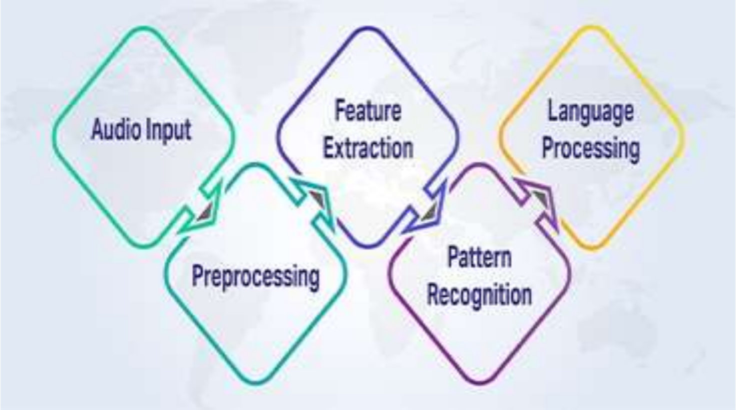

*Figure 2:* ***How Does Voice Recognition Work***

### *2.5 Behavioral Biometrics*

Behavioral biometrics is a subtype of biometric authentication in which the pattern in human behavior is analyzed to verify identity. These include how people type on a keyboard (keystroke dynamics), use a mouse (mouse dynamics), and move around mobile devices. Behavioral biometrics watch out for characteristics like typing speed, pressure, rhythm, and movement patterns to generate a particular profile of the user.

Unlike physical biometrics based on physiological traits, behavioral biometrics are actions and habits that are difficult to replicate. This form of authentication is very useful for continuous monitoring in real-time, for example, in controlling access to systems in fraud detection for online banking. The downside of behavioral biometrics is that these patterns change over time, and as a result, so does the technology's accuracy because of fatigue, stress, or health conditions (Greene et al., 2016).

### *2.6 DNA-based Authentication (Emerging)*

DNA-based authentication is an emerging biometric technology that uses a person's genetic material to verify identity. An analysis of the unusual sequences of DNA in the cells of an individual, sequences that are very specific to each person, allows for this method. DNA analysis can provide incomparable levels of security in that there is simply no way to replicate genetic patterns.

DNA-based authentication is very promising but still in its early stages and is not presently widespread in general applications. Problems faced by DNA authentication are the time and cost of analyzing genetic material, as well as related concerns about privacy and ethics of collecting and storing sensitive genetic samples (Clayton et al., 2019). However, DNA-based authentication's role in securing important information can be furthered by the advancements in DNA sequencing technology and forensic applications. Several biometric authentication technologies can be used for identity verification but have different pros and cons. These technologies are becoming so precise, secure, and practical, and they keep advancing, that they are the ideal security device for controlling physical and digital access.

## 3. Advancements in Biometric Security Systems

In recent years, there have been huge advancements in the field of biometric security systems, driven by technological advancements and the increased urgency of having a more secure and convenient authentication measure. The improvements here are mainly focused on improving accuracy, robustness, and user experience and handling the emerging threats in the cybersecurity space.

*Table 2: Key Advancements in Biometric Security Systems*

| Advancement | Description | Impact on Biometric Systems |
|---|---|---|
| **AI and Machine Learning Integration** | Use of AI algorithms to improve accuracy and adapt to new data | Improves accuracy, reduces spoofing, adapts to user behavior |
| **Multi-factor Biometric Systems** | Combining multiple biometric traits (e.g., fingerprint + facial recognition) | Enhances security, reduces vulnerability to spoofing |
| **Blockchain Integration** | Biometric data stored on decentralized blockchain systems | Secure storage, tamper-resistant, transparency |
| **Advancements in Sensor Technologies** | Improved sensors for capturing more detailed biometric data (e.g., 3D facial recognition) | Higher accuracy, more resistant to spoofing |
| **Biometric Authentication in Mobile Devices** | Integration of biometric systems in smartphones, tablets, and wearable devices | Enhanced security, user convenience, faster access |

### *3.1 AI and Machine Learning in Biometric Systems*

There has been a revolution in the field of biometric authentication systems by artificial intelligence (AI) and machine learning (ML), resulting in more accurate and efficient operations. More sophisticated than traditional methods, biometric data, such as fingerprints, facial recognition, and iris scans, is being analyzed with the help of AI algorithms. In particular, machine learning allows biometric systems to adapt to new data and make their system more and better with time. For example, facial recognition systems can now more accurately identify people in complicated conditions, such as low light or when people are wearing accessories like glasses or hats.

One of the main reasons AI and ML integration will greatly impact biometric systems is fraud detection and prevention. For example, AI can be used to distinguish between a spoofing attempt when someone sends a photo or a video performing like a genuine user (Fletcher, 2018). AI algorithms can analyze many factors, such as the movement of a person's face, to prove authenticity (Nyati, 2018). Furthermore, the ML models can help the system make the right decision by decreasing false positives and false negatives so that only valid users are given access.

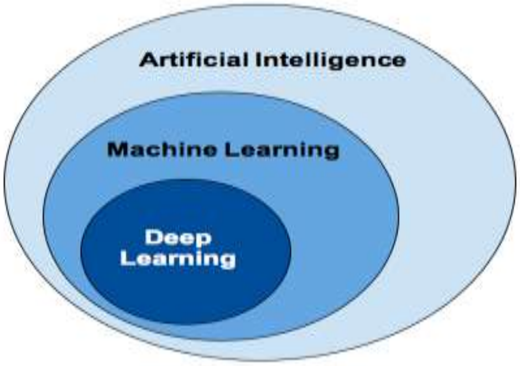

*Figure 3:* ***Predictive Biometric Systems***

### *3.2 Multi-factor Biometric Systems*

The rapid adoption of multi-factor biometric authentication (MFBA) for more secure use cases is growing. MFBA systems offer an extra layer of security by combining multiple biometric traits, like facial recognition, fingerprint scanning, and voice authentication, in a single system to make unauthorized persons face the difficult task of breaking into the system. The systems involve analyzing many characteristics of a single user and matching them to data that's already pre-registered.

For example, in high-security systems used by the government or financial institutions, multi-factor biometric authentication systems may demand that it involve scanning fingerprints and facial recognition to be a hard pill to crack an attack for an attacker (Ducray, 2017). Additionally, multi-modality reduces the probability that a system can be compromised by spoofing (such as using a polytomous produced image of a person's face) or environmental factors that degrade a single trait like poor brights for facial recognition or wear on a fingerprint sensor. A layered approach is superior to traditional password-based systems or any other single biometric trait.

### 3.3 Integration with Blockchain for Enhanced Security

There is no better advancement in cybersecurity than the integration of biometric authentication systems with blockchain technology. As a decentralized and tamper-resistant blockchain, it can safely store biometric data without any single centralized database, becoming a prime target for hackers. With blockchain technology, biometric data (fingerprint or facial scan) is encrypted and then stored on multiple nodes in a distributed ledger (Fu, 2020). The decentralization increases the difficulty in which attackers can manipulate or steal sensitive biometric information, as there is no single point of failure. Moreover, the immutability of blockchain records implies that once biometric data is recorded, it cannot be altered unless it is discovered. This gives additional transparency and accountability, which is very handy in domains like banking and healthcare, as it concerns data integrity.

In the future, blockchain may allow users to continue using biometric data on a need-to-know basis and grant or revoke access. For instance, instead of slavishly relying on a central server to ascertain identity, biometric data could be recorded to a user's blockchain, where users could employ their biometrics to check in without exposing their biometrics to third parties unless required.

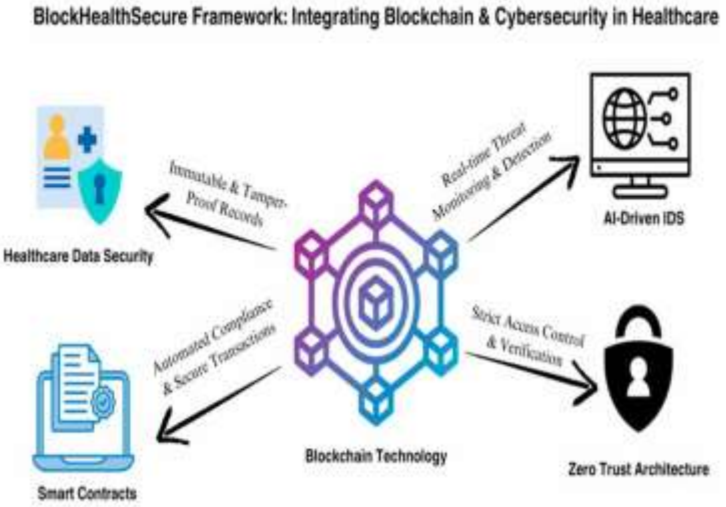
BlockHealthSecure Framework: Integrating Blockchain & Cybersecurity in Healthcare
Healthcare Data Security
Immutable & Tamper-Proof Records
Real-time Threat Monitoring & Detection
AI-Driven IDS
Automated Compliance & Secure Transactions
Strict Access Control & Verification
Smart Contracts
Blockchain Technology
Zero Trust Architecture

*Figure 4:* ***blockHealthSecure***

### 3.4 Advancements in Sensor Technologies

With the continuous improvement in sensor technologies, the quality of biometric authentication systems is getting enhanced with each passing day. Innovations in sensor design and capabilities have achieved more accurate, faster, and more secure systems. For example, fingerprint recognition uses new sensors, such as those that use advanced optical and capacitive technology to capture a more detailed image of a fingerprint and thus are less error-prone and more difficult to spoof.

Similar to this, new 3D sensors are being used to capture the depth and elevation of the face instead of using 2D images. Facial recognition systems using this method are more accurate and less vulnerable to spoofing attempts (attempting to 'spoof' or fake an image or video of a person to defeat a system) using photos or videos (Chingovska et al., 2016). However, these 3D sensors greatly improve the system's ability to identify users from different angles and under various lighting conditions, and such a solution is more secure. Advances in iris and retina scanning use infrared or near-infrared sensors that speed up these technologies and make them more accurate. Today's sensors allow instantaneously scanning of a person's iris, even as the individual moves, for seamless and efficient identification.

### 3.5 Biometric Authentication in Mobile Devices

Biometric authentication has become a standard feature in mobile devices due to the growing demand for convenient and secure access to mobile phones and other personal devices. Integrating biometric technology, such as fingerprint sensors, facial recognition, and voice recognition, on mobile devices has enabled a faster, more secure, and user-friendly authentication system. For example, fingerprint scanners are installed on the power button or under the screen, allowing users to access quickly without user interaction (Kaur et al., 2017). Newer facial recognition technology systems have also improved, and they can scan users' faces in real-time with lighting issues and clothing such as glasses. Voice recognition on mobile devices is also getting more elaborate, and there is another layer of authentication for such mobile banking apps and voice-activated assistance.

Machine learning algorithms are also used to improve the accuracy and security of biometric systems and the service of the biometric system on mobile devices. Since mobile biometric systems can, over time, learn from user behavior and interaction and adjust and also improve their accuracy, there is less chance of unauthorized access and an easy-to-use experience. Biometric security systems advances are becoming more reliable, efficient, and secure. All of this is helping bring you to highly secure systems that are harder to get past by using AI and machine learning, multi-factor authentication, blockchain technology, new and advanced sensor designs, and mobile integration (Kebande et al., 2021). These developments in software and hardware will enhance biometrics and make them a dominant player in protecting digital and photo environments with a more convenient user experience.

## 4. Risks Associated with Biometric Authentication

With an increase in the use of biometric authentication systems, they have become an essential point of access to secure sensitive data, financial accounts, and physical locations. While these systems have become popular, several risks associated with such systems must be addressed to meet both security and privacy concerns. Biometric data can be used to leverage other risks (privacy concerns, data breaches, spoofing attacks, accuracy, ethical implications, and legal risks) and can be compared with any other authentication technology.

*Table 3: Risks Associated with Biometric Authentication*

| Risk Category | Description | Potential Consequences |
|---|---|---|
| **Privacy Concerns** | Unauthorized collection and storage of biometric data | Permanent breach of privacy, government surveillance |
| **Data Breaches and Hacking Vulnerabilities** | Hacking of centralized biometric databases | Irreversible data leaks, identity theft |
| **Impersonation and Spoofing Attacks** | Attacks using fake biometric data to bypass authentication | Unauthorized access, fraud |
| **False Positives/Negatives and Accuracy Issues** | Errors in identifying authorized/unauthorized users | Loss of security, user frustration |
| **Ethical Implications and Government Surveillance** | Governments using biometric data for surveillance without consent | Infringement on privacy, social control |
| **Legal and Regulatory Risks** | Inadequate laws or compliance issues regarding biometric data | Legal penalties, difficulty in implementation |

### *4.1 Privacy Concerns*

The threat to users' privacy is one of the major concerns related to biometric authentication. Biometric data like fingerprints, facial scans, or eye scans are unlike passwords and PINs, which can easily be changed if the password or PIN is compromised. It does not matter how often; if biometric data is leaked, it is a permanent breach, and people cannot change their biometric traits. In addition, storing data regarding biometric information in centralized databases is a high-value target for cybercriminals. Besides collecting biometric data without user consent, in particular, when government agencies or private corporations collect such data with uses other than the original purpose (Zimmerman, 2017). This can complicate other offenses to the unauthorized investigation of people, thus reducing individual autonomy and chilling effect on free expression.

### *4.2 Data Breaches and Hacking Vulnerabilities*

With that, the risk of personal data breaches increases through biometric authentication. The big issue is the storage and management of biometric data, generally in big databases. The hacking of a database containing biometric information may have dire consequences. A compromised password is something that can be reset, while biometric data is something that, once exposed, can never be changed (Siddique et al., 2017). For instance, this could happen when a hacker uses an entry to a government or corporate biometric database and misuses the information for identity theft, fraudulent transactions, or unauthorized access to secured areas. In addition, biometric systems are also very prone to vulnerabilities in implementing such systems, like weak encryption methods or unsafe data transmission, which make it easier for cybercriminals to take advantage of these systems and obtain sensitive biometric data.

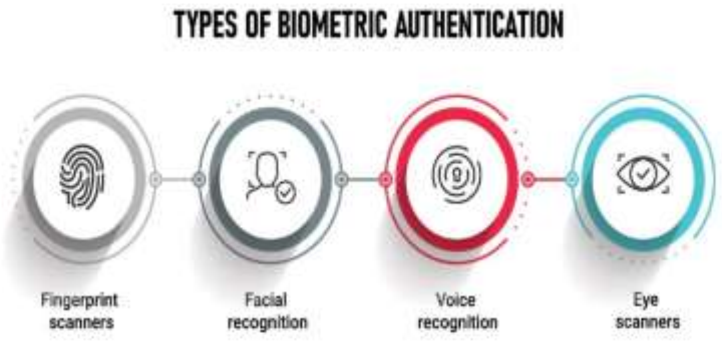

Figure 5: **Biometric Authentication**

### 4.3 Impersonation and Spoofing Attacks

Biometric systems are susceptible to impersonation and spoofing attacks that greatly impact the system's integrity. Recent developments in biometric recognition technology have made the systems vulnerable to attacks that electronically trick the biometric scanners. For example, fingerprint scanners can be fooled using high-quality replicas from materials such as gelatin or silicone. Facial recognition systems also use photographs, videos, or 3D models of a person's face to spoof them (Chingovska et al., 2016). Indeed, while more sophisticated biometric systems, such as multi-factor authentication, mix biometrics with other verification forms, they do not completely remove this risk. A system's reliability and security are undermined if an attacker bypasses a biometric system using a counterfeit biometric trait.

### 4.4 False Positives/Negatives and Accuracy Issues

The accuracy problem is another challenge of biometric authentication. No system is perfect because biometric systems exist to identify people from unique physical attributes. The risk of false positives, incorrectly allowing an unauthorized individual access, and false negatives, denying access to an authorized individual, are significant. As with many things, there are things that affect the accuracy of biometric systems: environmental conditions, user behavior, and even the quality of the biometric sensor. For example, a facial recognition system will perform less well if the person wearing the glasses or the lighting is not optimal (Neto et al., 2016). Likewise, a fingerprint scanner may misidentify a fingerprint if the user's hands are dirty or wet. Such accuracy issues can result in loss of security and user frustration in the biometric authentication system.

### 4.5 Ethical Implications and Government Surveillance

Given that biometric authentication systems have considerable ethical issues, particularly concerning giving the government access, a balance between the need for personal security and the threats posed by government surveillance must be worked out post haste. However, when implemented by governments, biometric systems can form the grounds for tracking citizens' movements, behaviors, and activities in public and private spaces. For example, facial recognition technology in public spaces like traffic intersections may be used without individuals' consent to identify individuals with the threat of mass surveillance and losing privacy rights. In addition, biometric systems can be used in criminal justice or border control operations to profile and target certain groups using biased data (Stenum, 2017). Biometric data may also infringe individual freedoms, thus threatening the risk that they will be exploited for political oppression or social control. However, several ethical dilemmas related to using biometric technologies, particularly in high-impact settings like law enforcement and government surveillance, require clear guidelines and ethical frameworks to be followed.

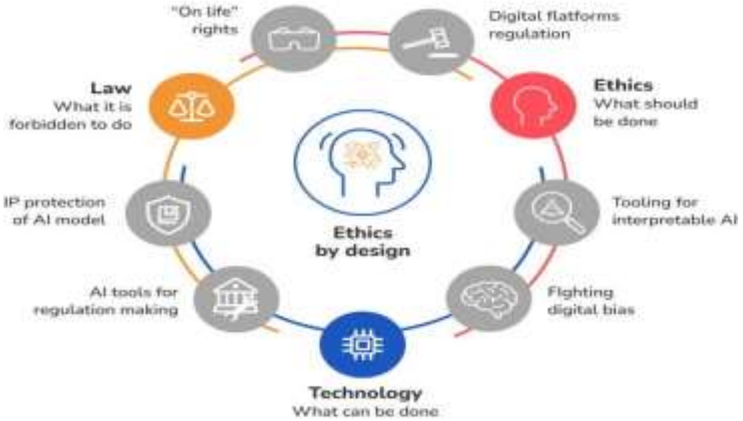
"On life" rights
Digital flatforms regulation
Law
What it is forbidden to do
Ethics
What should be done
Ethics by design
IP protection of AI model
Tooling for interpretable AI
AI tools for regulation making
Fighting digital bias
Technology
What can be done

*Figure 6:* ***Ethical Considerations in The Age Of Artificial Intelligence***

### *4.6 Legal and Regulatory Risks*

The legal and regulatory environment space with biometric authentication is very complex and ever-changing. However, most countries do not know how to make laws encompassing biometric data collection, storage, and usage. It leaves legal uncertainty for the organization to implement the biometric system, which can lead to a legal challenge or a penalty for non-compliance. For example, the European Union's General Data Protection Regulation (GDPR) imposes strict requirements for collecting and processing personal data (personal and biometric) (Hoofnagle et al., 2019). As per GDPR, individuals may not be able to background the use of their biometric data unless they give explicit consent, and the organization must secure and guard the data. However, in the US, state-level laws, such as the Illinois Biometric Information Privacy Act (BIPA), regulate biometric data but not federal laws, demonstrating a holistic manner. Businesses implementing a biometric system often find themselves bound by a fractured legal framework that can make implementing a biometric system complicated, and that can also create increased risk for a lawsuit or penalty if the business does not meet regulatory standards.

Biometric authentication systems have many benefits in terms of security and convenience, but they also yield several risks, which also need to be considered. These problems include privacy concerns, data breaches, spoofing attacks, accuracy problems, ethical dilemmas, and legal vagueness regarding the adoption of biometric technologies (Shaw, 2015). The evolution of such systems will continue, and businesses, governments, and regulators will work together to develop frameworks that reduce these risks while maintaining the effectiveness and security of biometric authentication.

## 5. Legal and Regulatory Frameworks for Biometric Authentication

Since biometric authentication systems are inherently highly sensitive, they are subject to strong legal and regulatory frameworks worldwide. The regulations protect an individual's privacy and ensure that biometric data is handled securely and responsibly. One must be aware of the legal landscape for implementing compliant and safe biometric systems.

*Table 4: Legal and Regulatory Frameworks for Biometric Authentication*

| Regulatory Framework | Region | Key Provisions | Impact on Biometric Systems |
|---|---|---|---|
| **General Data Protection Regulation (GDPR)** | European Union | Requires explicit consent, secure storage, right to access and delete data | High compliance requirements, fines for non-compliance |
| **California Consumer Privacy Act (CCPA)** | United States | Right to access, delete, and opt out of data sales | Requires transparency, user consent, and access control |
| **Brazil's LGPD** | Brazil | Data collection only with explicit consent, purpose limitation | Similar to GDPR, region-specific provisions |
| **China's PIPL** | China | Requires clear consent, prohibits international data transfer | Strong privacy provisions, stringent data export laws |

### *5.1 Global Regulations and Standards*

Global data protection regulations such as biometric authentication implementation are mainly concerned with high data security, transparency, and individual rights standards. The General Data Protection Regulation (GDPR) is the most influential global data protection framework passed by the European Union (EU) in 2018 (Dove, 2018). It considers biometric data as sensitive personal data and is thus subject to strict conditions for collecting, processing, and storing such data. For any biometric authentication system of an organization to be GDPR compliant, it must obtain explicit consent before collecting any biometrics and store them securely only in encrypted form or in a form that cannot be de-anonymized. As a result, data protection measures are imperative for organizations to comply with the regulation, which, in turn, carries heavy penalties for noncompliance.

Similar to the GDPR, the California Consumer Privacy Act (CCPA) serves similar purposes in the United States, with some differences. Under the CCPA, companies must tell consumers how they are collecting and processing, including biometric data, and give them the right to access, delete, and opt out of the sale of their data (Harris, 2020). In addition, it lays out how biometric data should be secured from unauthorized access. Therefore, companies conducting business using biometric authentication systems must comply with CCPA provisions to avoid fines and legal issues.

Comparison
Accuracy
01
Security
04
02
Speed
03
User Convenience

*Figure 7:* ***Biometric Technologies***

### *5.2 Country-Specific Rules and Guidelines*

Biometric authentication also comes under country-specific rules and guidelines apart from global regulations. For instance, the LGPD, a law in Brazil recently passed in 2020, resembles the GDPR in many regards but with some details that are unique to Brazil. It requires that individuals' biometric data are collected only with clear consent from organizations and only for the specific purpose for which the data will be used. Along the same lines, other countries like Canada, India, and Australia have data protection regulations and attached laws for biometric data under specific regulatory provisions. Normally, there are such regulations that organizations should establish technical and organizational measures to prevent biometric data breaches or misuse.

Some additional laws govern how biometric data can be collected and used in some places. For example, the Personal Information Protection Law (PIPL) of China, which has been in force since 2021, lays down the entire set of rules about the processing of biometric data (Czarnocki et al., 2021). This regulation demands that the companies acquire explicit consent from the person, how biometric data would be handled, and when the person's rights to access and request deletion of his/ her data would be upheld. In conjunction with this, PIPL prohibits the export of biometric data to protect individuals' data from abuse internationally.

### 5.3 Data Protection Laws Impacting Biometric Systems

Biometric authentication systems comply with data protection laws as laws that govern the collection, processing, and storing of personal data, including biometric data. Biometric data is also often considered highly sensitive, and in such jurisdictions, it is subject to additional protection under data protection laws (Carmona, 2018). These laws include assuring data accuracy, crypto protection to take the data away from any evil intent, and only allowing data to be accessed by those whom the authority has duly authorized.

The risk posed by biometric data is due to its uniqueness, and exposing or misusing such data often has severe consequences on compromised individuals. Consequently, data protection laws demand well-grounded safeguards, like encryption and anonymization techniques, to prevent it. Data cannot be returned to the person even if it is compromised. Many jurisdictions provide data protection authorities with the power to look at organizations to ensure compliance and investigate possible breaches.

There are also data retention policies that the organization should implement in addition to technical security measures. The GDPR states that biometric data should be stored for no longer than needed to meet the purpose for which it was collected and should then be erasable when no longer needed. The CCPA and other regulations also require rules on the period for which personal, biometric data, and for that matter, any data related to an individual, does not have to be retained before it is erased (Raimondi, 2021).

### 5.4 Challenges in Legal Compliance

Whilst the regulatory frameworks governing biometric authentication are deep and wide, the organizations struggle to comply fully. The biometric data collection problem is global, and there is often a requirement to meet various and sometimes conflicting jurisdictions in the regulation of biometrics. When an organization is active in the EU and the US, European GDPR and California CCPA will have their requirements on consent and how to enforce them (Thomas, 2020). However, this complexity makes compliance a never-ending fever in which you cannot stop sweating. It requires constant auditing, updating of internal policies, and knowing the legal saga from top to bottom.

Since data protection laws constantly update, organizations have to be alert and prepared to make quick changes when the law changes. Because biometric technologies develop so quickly, lawmakers frequently address new risks in the form of new regulations, such as the unfair invocation of biometric data in artificial intelligence and surveillance technology. As much as this creates an ongoing challenge for businesses to stay compliant and avoid legal pitfalls, it is also appreciated by almost every employee across the globe, which makes it a win-win situation for everyone.

The second issue is that organizations must educate employees and consumers (stakeholders) about their rights and responsibilities regarding biometric data. When dealing with complex biometric technologies, transparency in data collection and thorough and necessary consent can be difficult to ensure. Additionally, organizations must periodically define the response to data breaches, including how to communicate a breach to customers. There are various legal and regulatory frameworks for using biometric authentication systems whose aim is data protection and privacy. Countries, such as the US and European Union, through the GDPR and beyond, have established strict requirements for organizations regarding the security of biometric data , and global regulations like the GDPR and CCPA are following suit (Voss & Houser, 2019). Nevertheless, international laws are intricate, and the regulatory landscape can change anytime, making legal compliance challenging. Continuous monitoring, updating of policies, and open communication with stakeholders should be key parts of today's organizations' efforts to ensure compliance.

## 6. Security Threats and Vulnerabilities in Biometric Systems

Although considered one of the most secure ways of authentication, biometric systems are not always secure, which is something to consider. The more biometric technologies take to become integrated into daily life, the more important it is to understand the risks they present. Spoofing and fake biometrics, compromise to the database, system attack invariance, and the user's privacy are the biometric system's major threats and vulnerabilities below.

*Table 5: Security Threats and Vulnerabilities in Biometric Systems*

| Threat | Description | Example | Mitigation Strategies |
|---|---|---|---|
| **Spoofing and Fake Biometrics** | Use of fake biometric data to trick the system | Fake fingerprints, photos used for facial recognition | Use multi-layer security, liveness detection |
| **Database Compromise and Breaches** | Hacking of biometric data stored in databases | Breach of government or corporate biometric databases | Strong encryption, decentralized storage (e.g., blockchain) |
| **Lack of System Robustness against Attacks** | Vulnerability of biometric systems to cyber-attacks | Denial of Service (DoS), malware attacks | Continuous software updates, intrusion detection systems |
| **User Privacy Issues with Stored Data** | Risks of unauthorized access to personal biometric data | Identity theft, unauthorized surveillance | Encrypt data, provide user consent and transparency |

### *6.1 Spoofing and Fake Biometrics*

Spoofing is one of the primary security threats to biometric systems if someone can somehow provide counterfeit biometric data to trick a system into authenticating a fraudulent individual. There are several ways of spoofing, including fake fingerprints, facial masks, or voice recordings. For example, attackers will have silicone fingerprints or high-resolution photos of a person's biometric features. Deepfake technology has helped simplify the creation of such images and videos that can get past facial recognition systems (Westerlund, 2019).

Biometric systems employ various detection methods of spoofing attempts (liveness detection); however, an ideal way to stop such attempts is impossible. Although these countermeasures have proven successful in some instances, attackers have been able to exploit them in advanced ways to avoid these spoof detection techniques that require continuous improvement. Thus, to mitigate this risk, biometric systems should be complemented with multi-layered security protocols, including other authentication factors.

### *6.2 Database Compromise and Breaches*

Storing biometric data in centralized databases for easy access and wrangling makes it a well-suited target for cyberattacks. For instance, a biometric database breach is successfully exposed to sensitive personal information such as fingerprint patterns, facial scans, or retinal scans, typically irreversible. Since biometric data is permanent, it is a significant risk to expose, unlike passwords.

Our biometrics database has recently been involved in several high-profile data breaches, where hackers access the biometric information. For instance, in 2019, a biometric database of security company Suprema opened to millions of people, including their fingerprints and facial recognition data (Neace, 2020). There should be robust data protection strategies for such incidents. Data encryption or secure data storage processes can help increase the data breach risk reduction. Also, access controls and monitoring systems that log unauthorized access to the biometric data to avoid such compromises are necessary.

### *6.3 Lack of System Robustness against Attacks*

Another problem common to biometric procedures is the sensitivity of the systems to a range of kinds of cyber-attacks. For instance, many biometric authentication systems, such as facial recognition and fingerprint scanning, may not resist cyber-attacks. Some systems are vulnerable to Denial of Service (DoS) attacks, whereby an attacker floods the system with false data and denies legitimate users access (Yan et al., 2015).

Also, biometric systems are open to malware-seeking attacks on the software that processes biometric data. Phishing campaigns, unpatched vulnerabilities in the system's code, and malicious software can be introduced. Suppose the system processing software is exposed to an attacker. In that case, they may manipulate the biometric data to cause unauthorized access or disrupt the system's operation. This raises the imperative significance of continuous software upgrades, vulnerability testing, and intrusion detection mechanisms in securing biometric systems from attacks. In addition, the physical security of biometric capture devices like fingerprint scanners or cameras is usually ignored. Since these devices can be tampered with or hacked, attackers can manipulate biometric data at the source. Securing the hardware and software components is important to prevent such attacks on biometric systems.

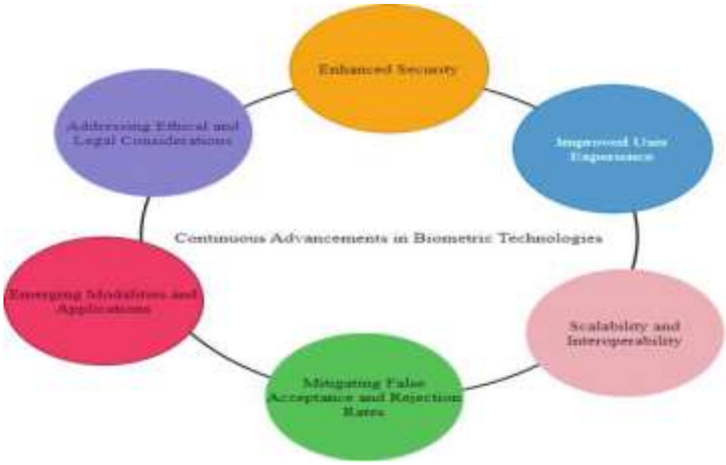
Enhanced Security
Improved User Experience
Scalability and Interoperability
Mitigating False Acceptance and Rejection Rates
Emerging Modalities and Applications
Addressing Ethical and Legal Considerations
Continuous Advancements in Biometric Technologies

*Figure 8: Continuous advancements in biometric technologies.*

### *6.4 User Privacy Issues with Stored Data*

Biometric authentication is one of the most predominant authentications using location data, and the main concern around this is user privacy. Unlike standard passwords, biometric information is naturally personal and distinct to each individual, making misusing or unauthorized use a serious privacy risk. The great problem with biometric data is that it tends to be held in centralized databases that open up a risk of misuse by authorized personnel and malicious actors. This data can also be used for unauthorized surveillance or profiling and constitute privacy violations.

Data collection and storage of personal details raise public concerns when the government or large corporation uses such data (Hardy & Maurushat, 2017). If anyone attacks biometric data for a malicious purpose (blackmail, identity theft), it can lead to unauthorized access and misuse of the biometric data. In addition, many users do not know how their biometric data is stored, processed, and even shared, a condition where users do not provide informed consent in some cases.

For instance, organizations need to adopt strict data governance policies to mitigate privacy concerns, and these policies have to be guarded with transparency, security, and accountability. This includes notifying users about the data collection process, obtaining consent, and offering the opt-out option whenever possible. Another way in which a data breach can be made less damaging with a minimal impact on the privacy of the data subject is through anonymization techniques like the use of hash functions to store biometric data in non-reversible form.

Despite this security enhancement, biometric authentication systems are not invulnerable. Technological advancements and rigorous security practices are needed to address the risks caused by spoofing, database breaches, system robustness, and user privacy, which are necessary for effective security and practice (Ogbonna, 2020). For biometric technologies to be accepted within the population and within different industries, it will become increasingly important to protect their security and reliability.

## 7. The Role of Artificial Intelligence in Enhancing Biometric Authentication

Artificial intelligence (AI) in biometric authentication systems has made them capable, more secure, and more reliable than before. At the same time, integrating AI in biometric authentication technologies has been key in tackling the problems of accuracy, fraud prevention, and maintaining high security in the overall system. The rest is about how AI has affected and influenced these Biometric Security Systems.

### *7.1 AI-Powered Biometric Recognition Systems*

Machine learning algorithms used by AI-powered biometric recognition systems help to enhance the accuracy and dependability of biometric locating systems. Fingerprints and facial recognition are typical and traditional approaches in which biometric systems make templates fixed and compare them using a simple algorithm. However, with AI coupling, these systems can now dynamically and accurately process the biometrics data by learning from big amounts of data (Galla et al., 2021). Using machine learning models, we train the models to detect subtle patterns in biometric features such as unique ridges of fingerprints and the fiddley details of the person's facial structure. This allows it to handle variations (such as lighting, angle, and sensor quality) in environmental conditions and thus provide consistent results. It is particularly useful for applying biometric data in real-world scenarios that may not be presented in ideal conditions.

AI models, especially deep learning networks, obtain thousands of facial attributes, allowing facial recognition systems to utilize such attributes to reach human-like recognition capabilities. As a result, it results in fewer false positives or even negatives than older, rule-based methods. In addition, because AI algorithms can be trained and improved over time, the more data they are exposed to, the more their ability to recognize that data will also improve (Benke, & Benke, 2018).

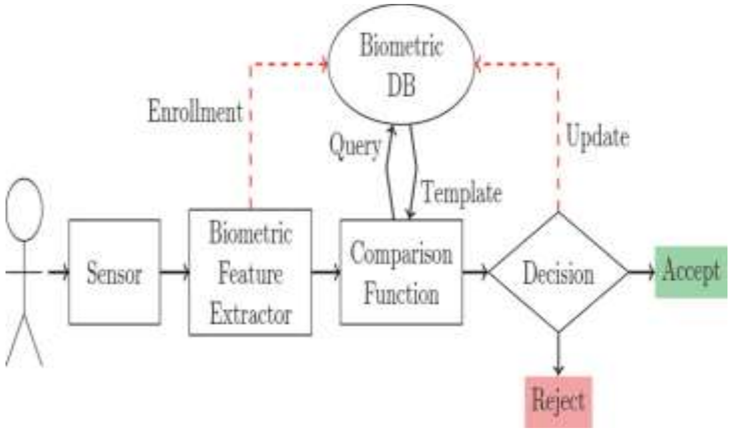

*Figure 9: **AI for Biometric Authentication Systems***

### 7.2 AI for Improving Accuracy and Reducing Fraud

The major advantage of AI in biometric authentication lies in the fact that it can enhance the accuracy of the system while minimizing the scope for Fraud. The other is to use photos or fake fingerprints to spoof biometric systems, such as faking a fingerprint to pretend to be someone else. Advanced techniques for AI-based systems, like convolutional neural networks (CNNs) and recurrent neural networks (RNNs), discriminate between the actual biometric data and the work of counterfeiting (Ali et al., 2021). For example, in facial recognition, AI can take stock of facial features and recognize if a picture is forged, for instance, if a 3D mask or a high-definition picture was used. The human eye is unable to detect some simple discrepancies that a machine learning model can be trained to identify by analyzing features such as lighting inconsistencies, texture, and depth information that the human eye cannot notice.

AI can also help increase the accuracy of biometric authentication through the reduction of false positives and false negatives. In particular, there is a problem with these errors since they happen when the identification or rejection of a person is incorrect. The system can continuously learn from new data to adjust or rework the threshold to adapt to different users and environments (Ditzler et al., 2015). This means that as the AI improves, it helps increase the reliability of biometric authentication systems and makes them less prone to errors and harder to attack by fraudsters.

### 7.3 AI-Driven Multi-layer Security Systems

The potential of AI to supplement biometric security lies in better individual recognition systems and in the development of layered security protocols. MFA systems connect several biometric techniques and other security measures, such as facial recognition, fingerprint, PIN code, and behavioral biometrics. AI enables such an arrangement, agreeing to run these multi-layer systems optimally and to protect the system as a whole.

AI analyses data from all of the sources handling requests to cross-validate the biometric input to determine whether the person is actually the person they say they are. In fact, facial recognition and voice recognition are analyzed by AI-driven systems at the same time, and the user identity is checked using two independent modalities (Vel, 2021). In this way, the possibility of a fraudster attempting to breach security is diminished since the same fraudster would have to get at several biometric identifiers. AI is applied to make multi-layer systems more efficient by automating the decision-making process. With traditional systems, manual intervention or verification slows down security layers and can even require manual intervention in each layer. The system uses this ability to autonomously determine when and how to employ each security layer based on that risk context and the context within which it is deployed, meaning a faster and more responsive user experience while providing great security.

### 7.4 AI in Predictive Threat Analysis

One of the other major uses of AI in biometric authentication is predictive threat analysis. Because AI systems can analyze vast amounts of data in real time, they can easily detect unusual patterns or behaviors that may indicate future security threats. For instance, if an AI detects multiple failed logins on different places or gadgets, it will categorize the behavior as suspicious and ask for additional verification steps like another biometric scan or inform security people (Habibu, 2020). It can also use historical data to predict future threats of Fraud or attack. This predictive capability helps organizations respond before committing any security breach. For high-security environments such as financial institutions and government agencies, threat analysis driven by AI can be especially necessary. Their cost is high, and if something happens, it's critical.

AI can always learn from new threats and update the systems predictive models so that it can detect and lessen risks as time passes (Kumar, 2019). AI can extract threat information from various sources, such as user behaviors, device details, and environment factors, to build a holistic security model that not only recognizes the threat but anticipates future vulnerabilities so that businesses can be ahead of potential attackers. Biometric authentication systems have greatly improved with AI, improving recognition accuracy, reducing Fraud, providing multi-layer security, and providing predictive threat analysis (Iyer et al., 2020). The application of AI in biometric systems will be crucial as the system keeps evolving and addresses the forthcoming challenges while maintaining security, efficiency, and reliability in the face of more advanced security threats (Nyati, 2018).

## 8. Future Considerations and Trends in Biometric Authentication

In recent years, biometric authentication technologies have significantly developed, and in the future, the situation is set to become even more advanced. As biometric systems gain popularity in industries globally to protect digital and physical spaces, several future considerations and trends must be anticipated. Specifically, these trends aim to improve usability, security, and integration with other technologies.

### *8.1 The Rise of Contactless and Remote Biometric Systems*

The development of contactless biometric authentication systems is one of the most important trends in the biometric space. Fingerprint and iris scanners, for example, are traditional biometric systems that can only be facilitated by physical interaction between the user and the device. In addition, since these systems are so low contact, they are gaining large traction. Face recognition, behavioral biometrics, and voice recognition systems have the advantage that the user does not need to touch any sensors there, which makes them well-suited for use in healthcare, airports, and public spaces.

The contactless biometric system is coming about due to increased demand for secure yet frictionless user experiences. For example, in the world after the pandemic, especially in the world after the pandemic, touchless systems are highly interesting because they provide as much security as possible, and, at the same time, they reduce the possibility of transmission of diseases. Furthermore, remote biometric systems enable users to authenticate themselves at a distance by an employee of voice recognition software or smartphone camera (Iyer et al., 2020). They are also forecasted to fill consumer-facing spaces like online bank facilities and mobile device security. These developments will make biometric systems more secure and convenient to use and, as a result, totally change the landscape of personal security.

### *8.2 Biometric Authentication in IoT (Internet of Things)*

One pivotal trend responsible for the future of biometric authentication is integration with the Internet of Things (IoT). As more IoT devices appear in homes, offices, and businesses, there is an ever-greater demand for secure authentication. While we must admit that biometric authentication is very effective in securing IoT networks and devices, it also presents great convenience.

For instance, biometric features, like voice recognition or facial recognition, can be integrated into a smart home system like a voice-controlled assistant to limit the information or devices a connection with can be accessed by only an authorized user. Similarly, wearable devices, like fitness trackers or smart watches, can have biometric sensors for monitoring health metrics while also providing the integration of authentication features for only the owner to permit the operation of the device (Seneviratne et al., 2017). Due to billions of IoT devices being deployed globally, biometric authentication will be necessary to secure access to such systems and protect them from misuse or data breaches. Additionally, more and more IoT systems will use biometric data to create more personalized and context-aware experiences. For example, when a user is identified, the home settings can be adjusted based on that, for instance, by lighting, temperature, or security. As the demand for seamless and secure IoT-enabled experiences continues to grow, this trend will evolve further.

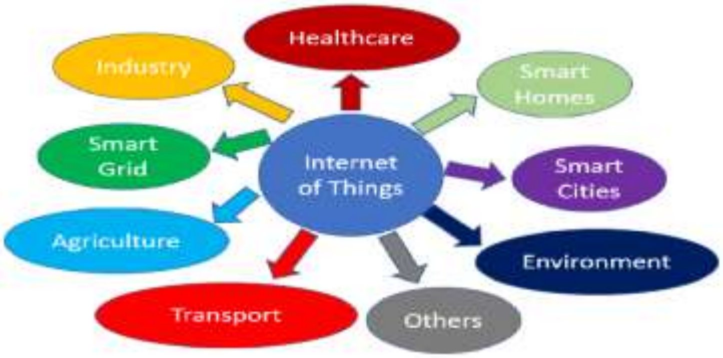

*Figure 10: Application domains of the IoT*

### *8.3 Integration with Emerging Technologies*

The estimation of biometric authentication and their integration with emerging technologies like Augmented Reality and Virtual Reality will be widely used. However, AR and VR technologies are becoming increasingly advanced and widespread and will eventually seek secure, seamless, frictionless authentication methods (Corcoran & Costache, 2018). These demands are well served by biometric systems, which combine high security with the cost of authentication methods such as passwords or Pins. For instance, in VR environments, users will soon be able to identify themselves with the system simply through facial recognition or iris scanning, allowing only authorized parties to enter the system.

In AR, biometric authentication can verify a user's identity before entering its features or virtual objects, especially in crucial industries like healthcare or finance. The potential of the biometrics fused in with AR and VR can help gain better user experiences by allowing for seamless, context-aware authentication, which won't disrupt the experience of the immersive nature of AR and VR, respectively. In addition, biometric authentication has been identified for use in AR and VR to promote more personal and secure interactions. For example, facial and voice biometrics might be used to tint user avatars based on special events such as games or virtual meetings (Mandryk & Nacke, 2016). With the prevalence of AR and VR technologies increasing, biometrics will only become more important for secure and easy interaction.

### *8.4 Ethical and Social Implications of Widespread Adoption*

By all means, the proliferation of biometric authentication systems continues, but it carries many ethical and social difficulties that must also be dealt with. Privacy is one of the main problems. The inherent nature of personal biometric data is that it is inherently personal; therefore, if it is mishandled, it can lead to significant breaches in the individual's privacy (Harper, 2021). An example is that biometric data collected and stored by government or private companies for large-scale collection could result in abuse of personal data, causing worries about surveillance and security of such data.

Biometric systems could also be biased. Face recognition is compared to other biometric systems, and it has been shown that other biometric systems, such as face recognition, have higher error rates for some demographic groups, particularly for people of color and women. The more biometric systems are used, the more important it will be to organizations that the systems are accurate and fair for all users and that they are fair without discriminating or causing unequal treatment (Stewart, 2019). One of these concerns is consent. There are cases when a person is required to provide biometric data to use services or to join some activities, but the procedure is opaque, and it is unclear what kind of data will be used and shared. Rules and guidelines will be needed to safeguard users' rights and ensure that biometric systems work properly without abuse.

01
Biometric Data
02
The Importance of Biometric Data in Security
03
Tips for Implementing Biometric Data in Security Systems
04
Case Studies Highlighting the Effectiveness of Biometric Data

*Figure 11: Introduction to Biometric Data and its Importance in Security Measures - Biometric Data: Enhancing Security Measures with EIDV*

### *8.5 Regulation Evolution for Biometric Technology*

As biometric authentication systems become more common tools, the regulatory landscape for their technologies will continue to change. Frameworks for governing the collection, storage, and usage of two of the many authorized forms of biometrics under way at the government and regulatory body level include processing data, fingerprints as used notary-wise, and iris scans are increasingly present. For example, in the European Union, the General Data Protection Regulation (GDPR) is currently starting to shape how biometric data is collected and handled, how organizations have to make it transparent, and how users have to give their consent to it (Tikkinen-Piri 2018).

More comprehensive regulatory frameworks will be needed to cover the increasing use of biometric technology in different sectors. Issues such as cross-border data flow, data retention policies, and strong security measures that will have to be taken into account by these frameworks are the data retention policy, cross-border flow of data, and strong security measures to protect biometric data. With the integration of these technologies into everyday life, it would be necessary for governments to balance the benefits of such technology with the protection of individual rights and freedom. The more biometric authentication grows, the more it will be overlaid, and its blurring edge will continue to appear with emerging technologies like IoT, AR, or VR, which will create new solutions and problems. The growth of touchless systems and the increased possibility of more secure, personal experiences will evolve biometric security in the future. However, these technologies must be implemented in an ethical, regulatory, sensitive, responsible, and transparent way.

## 9. Real-World Successful Case Study

### *9.1 Biometric Authentication in Banking*

One of the most adopted areas where biometric authentication has been adopted has been the banking sector, which has the potential to increase security and improve the customer experience as much as possible. The fingerprint and facial recognition examples are the most striking examples of leveraging fingerprint and facial recognition technologies for mobile banking and ATM access (Agidi, 2018). For example, some banks have introduced biometric features to their mobile banking apps. Customers may use a fingerprint or facial recognition to log in to their accounts or authorize transactions. The biggest benefit of this method is that it provides better security than a traditional password-based system and is more user-friendly.

Biometric authentication of customers was also incorporated into ATMs that allow customers to withdraw cash or perform transactions without providing a PIN (Taralekar et al., 2017). Fingerprint-based authentication has already been used by some banks worldwide, such as Indian ICICI Bank, which has undertaken such particular steps to secure ATM access and minimize corruptive efforts to gain access to stolen or hacked PINs. The advancements in sensor technologies have made this shift into biometric security both fast and accurate, so the shift also supports leaning towards biometric security.

*Table 6: Real-World Successful Case Studies in Biometric Authentication*

| Industry | Use Case | Technology Implemented | Outcome |
|---|---|---|---|
| **Banking** | Mobile banking and ATM access | Fingerprint and facial recognition | Increased security, better user experience |
| **Airports** | Airport security and check-ins | Facial recognition | Reduced wait times, improved security |
| **Corporations** | Access control in high-security areas | Fingerprint, iris, and facial recognition | Prevented unauthorized access, enhanced security |
| **Healthcare** | Patient identity verification | Fingerprint and facial recognition | Reduced medical errors, improved patient safety |

### *9.2 Biometric Systems in Airports*

It is no wonder that airports have increasingly adopted biometric authentication to secure these areas better and enhance passengers' experience. The TSA PreCheck program in the United States pre-screens travelers for security, and they can speed by the baggage. Biometric systems like facial recognition can help travelers be checked without manual scans, and the process can be much quicker, while TSA can verify the identity of the travelers.

Facial recognition systems are used at international airports, such as Miami International Airport (MIA) and Dubai International Airport (DXB), whereby travelers' faces are scanned when checking in, at security screening, and during boarding (Al Ameri, S2019). These systems also expedite passenger flow by reducing human errors and identity fraud and speeding up passenger flow. For instance, the implementation of biometric authentication in these airports is one of the ways the aviation industry has adapted technology to make passenger travel safer and more efficient. Airlines such as Delta and American Airlines are even using biometric check-ins, which are linking passenger travel data with the passengers' facial features, among other things. This integration also provides a seamless experience and reduces the amount of dependency on physical boarding passes to some extent, ultimately making the travel process paperless and more efficient.

### *9.3 Biometric Access Control in Corporations*

Several corporations, particularly those that deal with sensitive data or require high physical security, have been leaning on biometric systems for access control. Biometric authentication technologies like fingerprints, iris scans, and facial recognition are being used to prevent unauthorized personnel from accessing restricted areas in office buildings, laboratories, and data centers.

For example, companies like Google or Apple use biometric authentication in their employee access systems. Facial recognition and fingerprint scanners replace access cards and PINs to access secure areas in these organizations (Dragerengen, 2018). This method greatly reduces the risk of unauthorized access since the biometric traits are unique to each person and cannot easily be replicated or stolen. Additionally, biometric access control systems are more efficient than most security measures. Passwords are a thing of the past, and employees no longer have to remember them or carry access cards that can be lost or stolen. The centralized databases are integrated with the systems for real-time monitoring and logging of access attempts. This provides better security and enables fast detection of possible security breaches.

### *9.4 Use of Biometric Authentication in Healthcare*

Biometric authentication is an important aspect within the healthcare industry for patient safety and administrative processes. Patient identification is one of the most crucial applications of RFID tags. By ensuring that the proper person receives appropriate treatment, fingerprint or facial recognition can assist healthcare providers in accurately verifying patients' identities. Hospitals like the Cleveland Clinic have addressed problems associated with patient identity mistakes by installing biometric patient identification systems to reduce the chances of medical errors.

In these systems, patients enroll using their biometrics, and healthcare providers can authenticate them at every visit—including emergent situations when time is of the essence. Biometric records are then integrated with electronic health records (EHR) so that the patient's information is accurate and available when others need to see it (Ogbodo, 2020). Biometric authentication also can help speed up check-in processes at healthcare facilities. Patients do not have to wait in long queues, nor do they need to fill in paper forms, as patients need to check in using fingerprint or facial recognition. It frees up much of the administration burden and frees healthcare providers to spend more time with their patients rather than administration.

Additionally, biometric systems have a positive role in reducing fraud in healthcare as they can ensure that insurance claims and billing are attached to the correct patient. This technology has been the best way to respond to identity theft in medical systems, which are becoming increasingly prominent in the digital health ecosystem today. In many ways, biometric authentication systems have already proven themselves in use in a variety of industries, such as banking, air travel, business security, and even healthcare. The development also goes beyond improving security as it boosts website efficiency and user experience. Biometric systems will evolve increasingly in real life and become more secure, convenient, and effective in business and private efforts (Hamidi, 2019).

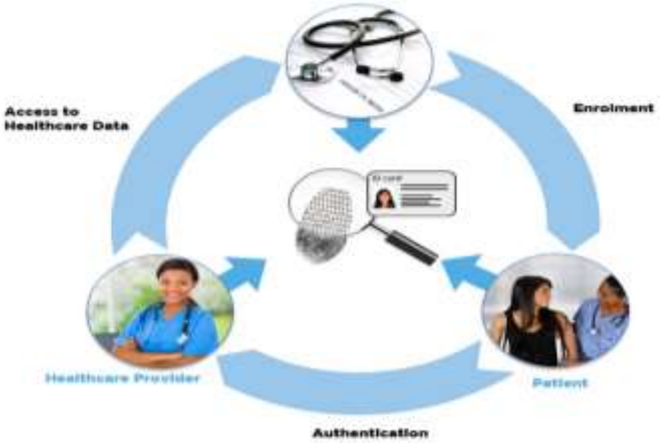

*Figure 12:* ***Biometrics in healthcare***

**10. Best Practices for Implementing Biometric Authentication**

Multiple considerations are essential for effective biometric authentication system implementation: securing the system, making it convenient for a user to use, and maintaining legal compliance.

***10.1 Choosing the Right Biometric Technology for Your Business***

Choosing the proper biometric technology is crucial to satisfy the needs of the particular business and defeat the risks to security with authentication. Depending on the industry or application, there can be different biometric systems. For instance, since iris or facial recognition systems are more expensive but more accurate, they are used more in high-security environments such as airports, metro stations or data centers. In contrast, fingerprint recognition is usually used in affordable consumer devices.

Businesses will have to evaluate operational context and decide on factors like accuracy, reliability, and speed of technology to make an informed decision. Another issue of interest is Scalability and ease of integration with existing infrastructure (Maqsood et al., 2016). For example, a use case of biometric authentication for finance (banking) applications requires financial institutions to evaluate if the particular technology will be able to work with a large number of users in a way that will not hamper performance. Additionally, the technology should be selected according to user expectations and regulatory requirements. For example, the region might require stricter regulations on facial recognition systems in public spaces, whereas they may be preferred for contactless authentication based on facial recognition in public spaces. However, when it comes to implementing a biometric, the biggest barrier is that businesses must find a balance between security, user preferences, and legal requirements.

***10.2 Balancing Security with User Convenience***

Researchers need to find the right balance between robust security, which defeats attackers at any cost, and User Convenience, which is the ability for users to quickly and easily authenticate. Biometric systems are highly associated with security based on the uniqueness of bodily traits and man's propensity to resist things he perceives as inconvenient, so they are threatened by user resistance. To do this, businesses should design systems for users to have a smooth experience using them. As a case study, researchers provide multi-modal biometric systems that merge two or more biometric identifiers (such as fingerprint and facial recognition) to improve both security and user convenience (Dargan & Kumar, 2020). Biometrics MFA, which combines with other methods of authentication (PINs or passwords, for example), puts a layer of security over existing authentication methods but is not over-burdening to the user. The role of user education is equally important regarding user acceptance and usage. However, businesses should also explain the benefits of biometric authentication; it is clearly a more secure solution than passwords and has faster authentication times. A higher adoption rate and less user frustration can be ensured if systems are made user-friendly in design and all systems are designed with a focus on accessibility.

### *10.3 Data Protection and Encryption*

Since biometric data is confidential, companies must take privacy and data encryption seriously when deploying biometric authentication systems. Encryption protocols are used to safely and securely store and transmit biometric data, like fingerprints or iris scans. To further secure the data on the device and in the cloud, data should be stored in encrypted formats to prevent a data breach or unauthorized access.

According to this, biometric systems should also have robust access control mechanisms barring the people who can access the stored data. To avoid unauthorized access to retrieve or manage biometric data, role-based access controls (RBAC) can be used (Kanth, 2019). Businesses must maintain routine data storage and handling audits to detect security weaknesses and close gaps. Suppose biometric data is used in compliance with industry standards and regulations (including the EU's General Data Protection Regulation or the California Consumer Privacy Act). In that case, it happens because of privacy laws. This would include obtaining explicit consent from users to collect their biometric information and allowing users to delete their data when requested.

### *10.4 Regulatory Compliance and Ethical Considerations*

In other words, it is essential to implement biometric authentication systems to comply with data privacy laws and ethical standards. Biometric data is regulated worldwide, both legally and ethically, and organizations should take care not to contravene these codes and attract legal consequences. Apart from the GDPR and the CCPA, businesses need to be aware of regional differences in privacy laws (Newman et al., 2020). For example, the way that biometric data is collected in China may be regulated differently from that of the United States or the European Union. Keeping in touch with ever-changing laws will help organizations remain compliant.

These considerations toward biometric authentication are all ethical. It is worrying that biometric data is being used for surveillance in such areas as facial recognition. Businesses must ensure the correct use of a biometric system for a legitimate purpose and guarantee that a biometric system protects users' privacy. Additionally, businesses should communicate to their users how their biometric data will be used and how and where it will be stored and protected using clear and transparent communication (Huszti-Orbán & Aoláin, 2020). A key practice to maintaining ethical standards is implementing opt-in consent processes, where users consent to provide their biometric information voluntarily. In addition, a data minimization principle should ensure that data collected is reduced to the bare minimum necessary.

### *10.5 Continuous System Monitoring and Updates*

After a biometric authentication system has been developed, it will be important to continuously monitor and update it to ensure its integrity and security. The business must always be aware of new threats and try to counter new vulnerabilities. System security is enhanced through regular updates, either software patches or hardware upgrades (Vaniea & Rashidi, 2016). In addition, businesses need to set up a system that can trace the biometric system's performance and usage patterns. This system can detect anomalies or suspicious activities, such as failed login attempts (s) or unauthorized access attempts (s), which can suggest a security breach.

Businesses should also perform security audits to examine the viability of their biometric frameworks. It entails evaluating technological infrastructure on the one hand and processes of data collection, storage and transmission on the other hand. Regular assessments help identify weaknesses in the system and give the chance to remedy those weaknesses. Investing in employee training for employees in charge of operating or managing biometric systems ensures that these employees have the necessary skills and means to react swiftly to any security situation or incident. This also ensures that staff members are properly trained to know the value of safeguarding user data and complying with regulatory requirements.

## 11. Conclusion

Using biometric authentication is an important change in how digital and physical spaces are secured using unique physical and behavioural traits. As provided throughout the paper, biometric technology, such as fingerprint recognition, facial, scan, iris, retina scanning and voice, is an integral component of modern security systems. These technologies have several advantages compared with traditional password-based systems, such as higher security, more user convenience, and less risk of fraud and identity theft. Biometric authentication is a unique and hard-to-replicate trait that solves the growing problem of cyber threats, unauthorized access and data breaches. However, the adoption of biometric systems comes with considerations and risks. In addition to the privacy concerns, biometric data is personal and ideally cannot be changed if compromised. In addition, there are threats to the effectiveness of biometric authentication regarding the possibility of data breaches, spoofing attacks, and system vulnerabilities. When biometrics become more common, the possibility of marital misuse (to watch or to perve on) or loss of unbidden access to protected data presses ethical considerations.

The development of biometric technology has speeded up with artificial intelligence (AI) and machine learning, which has rapidly increased the accuracy and reliability of biometric authentication systems simultaneously. With AI-driven solutions, the systems have become better at adapting new data, increasing the layer of security, decreasing false positives, and increasing fraud detection. Given the integration capabilities with such leading-edge technologies as the blockchain, the Internet of Things (IoT), and augmented and virtual reality (AR/VR), biometric systems will seamlessly continue to be improved in all areas to offer highly secure and user seamless experiences of all kinds in different industries. As biometric systems continue to develop, organizations must stay abreast in safeguarding against potential risks and difficulties connected with the systems. This includes being GDPR- and CCPA-compliant, ensuring that you have all the right privacy policies and that they are required, that the privacy language is in the right form, and that they are applied correctly. The ethical considerations must guide the implementation of the biometric systems; user consent must be collected, and the users' privacy must be respected. Additionally, businesses should pay adequate attention to the safety of stored biometric data through effective encryption and proper access controls to prevent unauthorized access and eliminate any possibility of a breach.

Researchers can say that biometric authentication's future is positive and will be further improved with continuous improvements in sensor technologies and AI-driven algorithms. With more industries like banking, healthcare, and government services adding biometric authentication to their security frameworks, the technology will only continue to play a key role in providing crucial data security and a pleasant user experience. Increasingly, contactless biometric systems are developing, and biometrics is being added to everyday devices such as smartphones, wearables, and IoT devices, which will speed up the process of security, making authentication faster and simpler for users. However, companies aiming to embed biometric authentication into their projects should consider which technology to use, depending on the corporate needs. Security versus user convenience should be balanced since user acceptance of a biometric system is key to its success. Risk mitigation and the reliability of biometric authentication can be achieved through continuous monitoring, regular updates, and adopting best practices related to data protection and security systems.

Biometric authentication systems, however, represent a fantastic way to protect information with access to the system and identify oneself without a lot of legal or moral baggage attached. To remain a business that utilizes biometric systems safely and effectively, adherence to best practices, maintaining user transparency, keeping up with technological advancements, and legislation changes are necessary. With biometric authentication evolving and expanding into more and more organizations, its future as a way of defining security will become that much bigger for more secure sensitive information and more streamlined use of access across industries, becoming an essential and commonplace feature.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

**Publisher's Note**: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

## References

[1] Agidi, R. C. (2018). Biometrics: The future of banking and financial service industry in Nigeria. *International Journal of Electronics and Information Engineering*, *9*(2), 91-105.

[2] Al Ameri, S. A. S. H. (2019). *The Role of Religious and Cultural Dynamics in the Implementation of Security Measures in the Selected International Airports in the UAE: An Empirical Case Study* (Doctoral dissertation, University of Gloucestershire).

[3] Ali, M. H., Ibrahim, A., Wahbah, H., & Al_Barazanchi, I. (2021). Survey on encode biometric data for transmission in wireless communication networks. *Periodicals of Engineering and Natural Sciences (PEN)*, *9*(4), 1038-1055.

[4] Ankerman, C. D. (2016). A Closer Look: Iris Recognition, Forensics, and the Future of Privacy. *Conn. L. Rev.*, *49*, 1357.

[5] Benke, K., & Benke, G. (2018). Artificial intelligence and big data in public health. *International journal of environmental research and public health*, *15*(12), 2796.

[6] Carmona, M. M. S. (2018). *Is Biometric Technology in Social Protection Programmes Illegal Or Arbitrary?: An Analysis of Privacy and Data Protection*. ILO.

[7] Chingovska, I., Erdogmus, N., Anjos, A., & Marcel, S. (2016). Face recognition systems under spoofing attacks. *Face Recognition Across the Imaging Spectrum*, 165-194.

[8] Chingovska, I., Erdogmus, N., Anjos, A., & Marcel, S. (2016). Face recognition systems under spoofing attacks. *Face Recognition Across the Imaging Spectrum*, 165-194.

[9] Clayton, E. W., Evans, B. J., Hazel, J. W., & Rothstein, M. A. (2019). The law of genetic privacy: applications, implications, and limitations. *Journal of Law and the Biosciences*, *6*(1), 1-36.

[10] Corcoran, P. M., & Costache, C. (2018, August). A privacy framework for games & interactive media. In *2018 IEEE Games, Entertainment, Media Conference (GEM)* (pp. 1-9). IEEE.

[11] Czarnocki, J., Kun, E., Giglio, F., Royer, S., & Petik, M. (2021). Legal study on Government access to data in third countries. *Legal study on Government access to data in third countries*.

[12] 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.

[13] Ditzler, G., Roveri, M., Alippi, C., & Polikar, R. (2015). Learning in nonstationary environments: A survey. *IEEE Computational Intelligence Magazine*, *10*(4), 12-25.

[14] Dove, E. S. (2018). The EU general data protection regulation: implications for international scientific research in the digital era. *Journal of Law, Medicine & Ethics*, *46*(4), 1013-1030.

[15] Dragerengen, K. (2018). *Access control in critical infrastructure control rooms using continuous authentication and face recognition* (Master's thesis, NTNU).

[16] Ducray, B. (2017). *Authentication by gesture recognition: A dynamic biometric application* (Doctoral dissertation, Royal Holloway, University of London).

[17] Fletcher, J. (2018). Deepfakes, artificial intelligence, and some kind of dystopia: The new faces of online post-fact performance. *Theatre Journal*, *70*(4), 455-471.

[18] Fu, M. H. (2020). Integrated technologies of blockchain and biometrics based on wireless sensor network for library management. *Information Technology and Libraries*, *39*(3).

[19] Galla, E. P., Madhavaram, C. R., & Boddapati, V. N. (2021). Big Data And AI Innovations In Biometric Authentication For Secure Digital Transactions. *Available at SSRN 4980653*.

[20] Greene, S., Thapliyal, H., & Caban-Holt, A. (2016). A survey of affective computing for stress detection: Evaluating technologies in stress detection for better health. *IEEE Consumer Electronics Magazine*, *5*(4), 44-56.

[21] Habibu, T. (2020). *Development of secured algorithm to enhance the privacy and security template of biometric technology* (Doctoral dissertation, NM-AIST).

[22] Hamidi, H. (2019). An approach to develop the smart health using Internet of Things and authentication based on biometric technology. *Future generation computer systems*, *91*, 434-449.

[23] Hardy, K., & Maurushat, A. (2017). Opening up government data for Big Data analysis and public benefit. *Computer law & security review*, *33*(1), 30-37.

[24] Harper, H. (2021). Your Body, Your Data, But Not Your Right of Action: Seeking Balance in Federal Biometric Privacy Legislation. *Nat'l Sec. LJ*, *8*, 86.

[25] Harris, R. (2020). Forging a path towards meaningful digital privacy: Data monetization and the CCPA. *Loy. LAL Rev.*, *54*, 197.

[26] Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65-98.

[27] Huszti-Orbán, K., & Aoláin, F. N. (2020). *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?*. Minneapolis: Human Rights Center, University of Minnesota.

[28] Iula, A. (2019). Ultrasound systems for biometric recognition. *Sensors*, *19*(10), 2317.

[29] Iyer, A. P., Karthikeyan, J., Khan, R. H., & Binu, P. M. (2020). An analysis of artificial intelligence in biometrics-the next level of security. *J Crit Rev*, *7*(1), 571-576.

[30] Jeon, B., Jeong, B., Jee, S., Huang, Y., Kim, Y., Park, G. H., ... & Choi, T. H. (2019). A facial recognition mobile app for patient safety and biometric identification: design, development, and validation. *JMIR mHealth and uHealth*, *7*(4), e11472.

[31] kanth Mandru, S. (2019). Role-Based Access Control (RBAC) in Modern IAM Systems: A study on the effectiveness and challenges of RBAC in managing access to resources in large organizations. *European Journal of Advances in Engineering and Technology*, *6*(4), 57-64.

[32] Kaur, N., Azam, S., Kannoorpatti, K., Yeo, K. C., & Shanmugam, B. (2017, January). Browser fingerprinting as user tracking technology. In *2017 11th International Conference on Intelligent Systems and Control (ISCO)* (pp. 103-111). IEEE.

[33] Kebande, V. R., Awaysheh, F. M., Ikuesan, R. A., Alawadi, S. A., & Alshehri, M. D. (2021). A blockchain-based multi-factor authentication model for a cloud-enabled internet of vehicles. *Sensors*, *21*(18), 6018.

[34] Kepuska, V., & Bohouta, G. (2018, January). Next-generation of virtual personal assistants (microsoft cortana, apple siri, amazon alexa and google home). In *2018 IEEE 8th annual computing and communication workshop and conference (CCWC)* (pp. 99-103). IEEE.

[35] Khade, S., Ahirrao, S., Phansalkar, S., Kotecha, K., Gite, S., & Thepade, S. D. (2021). Iris liveness detection for biometric authentication: A systematic literature review and future directions. *Inventions*, *6*(4), 65.

[36] Kumar, A. (2019). The convergence of predictive analytics in driving business intelligence and enhancing DevOps efficiency. International Journal of Computational Engineering and Management, 6(6), 118-142. Retrieved from https://ijcem.in/wp-content/uploads/THE-CONVERGENCE-OF-PREDICTIVE-ANALYTICS-IN-DRIVING-BUSINESS-INTELLIGENCE-AND-ENHANCING-DEVOPS-EFFICIENCY.pdf

[37] Mandryk, R. L., & Nacke, L. E. (2016). ▪ Biometrics in Gaming and Entertainment Technologies. In *Biometrics in a Data Driven World* (pp. 215-248). Chapman and Hall/CRC.

[38] Maqsood, T., Khalid, O., Irfan, R., Madani, S. A., & Khan, S. U. (2016). Scalability issues in online social networks. *ACM Computing Surveys (CSUR)*, *49*(2), 1-42.

[39] Neace, G. (2020). Biometric Privacy: Blending Employment Law with the Growth of Technology, 53 UIC J. Marshall L. Rev. 73 (2020). *UIC Law Review*, *53*(1), 3.

[40] Neto, L. B., Grijalva, F., Maike, V. R. M. L., Martini, L. C., Florencio, D., Baranauskas, M. C. C., ... & Goldenstein, S. (2016). A kinect-based wearable face recognition system to aid visually impaired users. *IEEE Transactions on Human-Machine Systems*, *47*(1), 52-64.

[41] Newman, M., Swift, M., & Gladicheva, V. (2020). GDPR and CCPA Start to Bare Teeth as Privacy Protection Goes Global. *Bus. L. Int'l*, *21*, 267.

[42] Nyati, S. (2018). Revolutionizing LTL carrier operations: A comprehensive analysis of an algorithm-driven pickup and delivery dispatching solution. International Journal of Science and Research (IJSR), 7(2), 1659-1666. Retrieved from https://www.ijsr.net/getabstract.php?paperid=SR24203183637

[43] Nyati, S. (2018). Transforming telematics in fleet management: Innovations in asset tracking, efficiency, and communication. International Journal of Science and Research (IJSR), 7(10), 1804-1810. Retrieved from https://www.ijsr.net/getabstract.php?paperid=SR24203184230

[44] Ogbodo, I. A. (2020). Exploring access to EHR by emergency patients using multimodal biometrics. *Int. J. Latest Technol. Eng. Manag. Appl. Sci*, *9*, 44-50.

[45] Ogbonna, L. (2020). *Technical strategies database managers use to protect systems from security breaches* (Doctoral dissertation, Walden University).

[46] Raimondi, L. (2021). Biometric Data Regulation and the Right of Publicity: A Path to Regaining Autonomy Over Our Commodified Identity. *U. Mass. L. Rev.*, *16*, 198.

[47] Raju, R. K. (2017). Dynamic memory inference network for natural language inference. International Journal of Science and Research (IJSR), 6(2). https://www.ijsr.net/archive/v6i2/SR24926091431.pdf

[48] Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., ... & Seneviratne, A. (2017). A survey of wearable devices and challenges. *IEEE Communications Surveys & Tutorials*, *19*(4), 2573-2620.

[49] Shaw III, S. (2015). *A business integration model for the adaptation of biometrics technology in the 21st century* (Doctoral dissertation, Capella University).

[50] Siddique, K., Akhtar, Z., & Kim, Y. (2017). Biometrics vs passwords: a modern version of the tortoise and the hare. *Computer Fraud & Security*, *2017*(1), 13-17.

[51] Stenum, H. (2017). The body-border. Governing irregular migration through biometric technology.

[52] Stewart, L. (2019). Big data discrimination: Maintaining protection of individual privacy without disincentivizing businesses' use of biometric data to enhance security. *BCL Rev.*, *60*, 349.

[53] Taralekar, A., Chouhan, G., Tangade, R., & Shardoor, N. (2017, December). One touch multi-banking transaction ATM system using biometric and GSM authentication. In *2017 International Conference on Big Data, IoT and Data Science (BID)* (pp. 60-64). IEEE.

[54] Thomas, I. (2020). Getting ready for the California consumer privacy act: Building on general data protection regulation preparedness. *Applied Marketing Analytics*, *5*(3), 210-222.

[55] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134-153.

[56] Vaniea, K., & Rashidi, Y. (2016, May). Tales of software updates: The process of updating software. In *Proceedings of the 2016 chi conference on human factors in computing systems* (pp. 3215-3226).

[57] Vel, T. (2021). AI-Driven Adaptive Authentication for Multi-Modal Biometric Systems. *J. Electrical Systems*, *17*(1), 75-88.

[58] Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: providing a competitive advantage for US companies. *American Business Law Journal*, *56*(2), 287-344.

[59] Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology innovation management review*, *9*(11).

[60] Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2015). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE communications surveys & tutorials*, *18*(1), 602-622.

[61] Zimmerman, H. (2017). The data of you: regulating private Industry's collection of biometric information. *U. Kan. L. Rev.*, *66*, 637.